Proiect

GUVERNUL REPUBLICII MOLDOVA

H O T Ă R Î R E nr. _____
din „___” _____ 2014
Chişinău

cu privire la aprobarea Reglementării tehnice ”Infrastructura informaţională internă a autorităţilor administraţiei publice”

I. DISPOZIŢII GENERALE

1. Prezenta Reglementare are următoarele obiective de bază:

a) asigurarea introducerii tehnologiilor moderne în activitatea autorităţilor administraţiei publice pentru perfecţionarea procedurilor de luare a deciziilor;

b) asigurarea utilizării eficiente la nivel optim a tuturor resurselor existente în sistem (hardware, software, dispozitive de comunicaţii, personal tehnic de specialitate etc.);

c) perfecţionarea organizării schimbului de informaţii dintre autorităţile administraţiei publice, inclusiv cele de peste hotare, dezvoltarea colaborării cu instituţiile domeniului dat de activitate;

d) asigurarea sistemului unic de securitate informaţională a autorităţilor administraţiei publice ale Republicii Moldova.

II. Noţiuni şi abrevieri

2.În sensul prezentei Reglementări, următoarele noţiuni se definesc astfel:

sistem informaţional – totalitatea resurselor informaţionale interdependente, tehnologiilor, metodelor şi personalului, destinată păstrării, prelucrării şi furnizării informaţiei;

resursă informaţională – totalitatea informaţiei documentate în sistemele informaţionale automatizate, organizată în conformitate cu cerinţele stabilite şi legislaţia în vigoare;

tehnologie informaţională – totalitateametodelor, procedeelor şi mijloacelor de prelucrare şi transmitere a informaţiei, precum şi regulile de aplicare ale acestora;

date - fapte, idei, fenomene, procese, proprietăţi, indicii, instrucţii ş.a. prezentate într-o formă convenţională, care permite transmiterea sau schimbul acestora, precum şi prelucrarea lor în mod manual sau automat;

bază de date - totalitate de date corelate între ele, organizate conform unei structuri conceptuale, care descriu caracteristicile şi relaţiile esenţiale dintre principii, destinată unui sau mai multor domenii de aplicare;

bancă de date - sistem tehnico - informaţional ce include una sau mai multe baze de date şi un sistem de administrare a acestora;

complex de mijloace tehnice şi de program - totalitate de mijloace tehnice şi de program care asigură realizarea proceselor informaţionale;

obiect informaţional – reprezentarevirtuală a principiilor real existente, atît ale celor materiale cît şi celor nemateriale;

punct de acces la Internet – echipament telecomunicaţional tehnologic compus din Sistem de Operare (SO) şi alte diverse interfeţe fizice (router), care la rîndul său îndeplineşte nu doar funcţia de interconectare a reţelelor dar datorită nivelului soft al sistemei de operare cu care operează, poate îndeplini şi funcţia de delimitator de viteze, clasificator de priorităţi a pachetelor, tipului de trafic, limitator de acces a traficului în diferite medii/sisteme informaţionale şi alte funcţii de trafic engineering (QoS).

serviciu informaţional – activitate de furnizare a produselor informaţionale;

SCS – sistem de cablare structurat;

ÎC – începerea de crosare;

CME – cameră de comutare a magistralei externe.

III. Clasificarea sistemelor informaţionale interne

3. Clasificarea resurselor informaţionale este efectuată conform aspectului cantitativ şi de extindere a infrastructurii informaţionale interne, precum şi conform principiilor de funcţionalitate a elementelor infrastructurii interne.

4. Astfel, definim trei clase de sisteme informaţionale interne şi trei tipuri de extensii de funcţionalitate:

a) Clasa 1 – Infrastructuri informaţionale interne cu numărul de echipamente terminale (staţii de muncă, PDA, Servere) nu mai mare de 50 unităţi;

b) Clasa 2 – Infrastructuri informaţionale interne cu numărul de echipamente terminale între 50 şi 100 unităţi;

c) Clasa 3 – Infrastructuri informaţionale interne cu numărul de echipamente terminale mai mare de 100 unităţi;

d) Extensii de tipul 1 – Activităţi de accesare a resurselor informaţionale, ce nu sunt clasificate drept resurse informaţionale de importanţă statală şi sunt reglementate prin acordurile de interconectare între autoritate şi entitatea terţă (altă autoritate, instituţie publică/comercială).

e) Extensii de tipul 2 – Activităţi de accesare a resurselor informaţionale, clasificate prin Legea Republicii Moldova nr. 467 din 21.11.2003 drept resurse informaţionale de importanţă statală.

f) Extensii de tipul 3 – Activităţi de creare, procesare, stocare, schimb de informaţii între două sau mai multe autorităţi ale administraţiei publice, clasificată drept informaţie de importanţă statală şi, totodată, ca informaţie necesară pentru realizarea sarcinilor autorităţii administraţiei publice, al căror reglementare este efectuată în baza acordurilor de interconectare şi a politicilor de securitate existente sau celor adiţionale.

5. Clasele de sisteme informaţionale interne şi tipurile de extensii de funcţionalitate sunt prezentate în tabelul nr. 1.

Tabelul 1. Clase de sisteme informaţionale interne şi tipuri de extensii de funcţionalitate

Clase de infrastructuri	*Echipamente Terminale*	*Extensii de tipul 1*	*Extensii de tipul 2*	*Extensii de tipul 3*
Clasa 1	*<50*	*Cu accesarea altor resurse informaţionale externe*	*Cu accesarea resurselor informaţionale de bază*	*Cu crearea resurselor informaţionale de bază*
Clasa 2	*50-100*	*Cu accesarea altor resurse informaţionale externe*	*Cu accesarea resurselor informaţionale de bază*	*Cu crearea resurselor informaţionale de bază*
Clasa 3	*>100*	*Cu accesarea altor resurse informaţionale externe*	*Cu accesarea resurselor informaţionale de bază*	*Cu crearea resurselor informaţionale de bază*

IV. Arhitectura şi cerinţele faţă de infrastructura informaţională internă

4.1. Arhitectura şi cerinţele faţă de infrastructura de reţea internă

6. Sistemul de cablare structurat (SCS) este temelia infrastructurii informaţionale şi de telecomunicaţii a oricărei organizaţii moderne, indiferent de dimensiunea acesteia.

7. Reţelele interne în oficii trebuie să deţină, cel puţin, următoarele caracteristici:

a) Universalitate, ce va permite utilizarea sistemului de cablaj în transmisiunea diferitor semnale digitale, precum şi va permite conectarea diferitor tipuri de echipamente de reţea pentru oferirea serviciilor de reţea internă;

b) vor permite organizarea noilor locuri de muncă rapid şi eficient, precum şi schimbarea topologiei fizice de interconectare, fără pozarea liniilor de cablu suplimentare;

c) va permite organizarea serviciului unic de exploatare;

d) va avea termen de exploatare de 10 sau mai mulţi ani, dacă va fi creată pe parcursul perioadei de construcţie a unei clădiri sau reutilării acesteia.

8. Sistemul de cablare structurat (SCS) corespunde tuturor cerinţelor prezentate mai sus.

9. Se subînţelege că SCS este sistemul de cablare, la baza căruia stau trei principii:

a) **Structurare** – admite secţionarea reţelei de cablare, a accesoriilor sau a subsistemelor în părţi separate, fiecare dintre care îndeplineşte anumite funcţii; este echipat cu o interfaţă standard pentru comunicarea cu alte subsisteme, precum şi

echipamente de reţea. În componenţa oricărui subsistem neapărat se includ instrumente de comutare, care asigură flexibilitatea înaltă şi permite de a crea structuri complexe cu modificarea uşoară a configurării şi adaptarea la cerinţele aplicaţiilor concrete. La construirea sistemului trebuie să fie aplicată abordarea generalizată pentru orice tip de cablaj sau echipament de comutare, care oferă oportunitatea de a utiliza tehnologii de transmitere a semnalului electric, optic şi fără fir de la orice nivel, alegerea fiind determinată de condiţiile interne şi de eficienţa economico-tehnică maximă a acestui proiect special.

b) **Flexibilitate** – crearea unui sistem de cablu pe principii de arhitectură deschisă, cu specificaţii tehnice de bază, menite să asigure funcţionarea oricărei tehnologii. Acest lucru vă permite utilizarea sistemului de cablu pentru transmiterea semnalelor diferitor aplicaţii.

c) **Redundanţă** – introducerea în SCS a punctelor de acces suplimentare (prize informaţionale), cantitatea şi locul cărora sunt stabilite de topologia zonei şi a spaţiului de lucru, dar nu de planurile plasării personalului sau a mobilierului de birou. Aplicarea acestui principiu permite o adaptare rapidă a sistemelor de cablu pentru nevoile specifice de producţie.

10. Pentru crearea SCS şi exploatarea în viitor a acesteia este necesară întrunirea unei serii de condiţii, şi anume – SCS ar trebui să deţină:

a) catalogul produselor;

b) standarde şi metode de proiectare care permit executarea cerinţelor standardelor existente;

c) posibilitatea gestionării (administrării), în conformitate cu procedurile standard;

d) sistemul de pregătire a personalului şi asigurare a garanţiei pentru producător.

11. Utilizarea reţelei locale permite SCS:

a) de a oferi reduceri de cost, prin durata lungă de exploatare şi cheltuieli mici de exploatare;

b) de a creşte gradul de fiabilitate a sistemelor de cablu;

c) de a schimba configuraţia şi construirea reţelelor fără influenţă asupra resurselor existente;

d) de a utiliza simultan diferite protocoale de reţea şi arhitecturi de reţea, într-un singur sistem;

e) de a combina într-un sistem unic canalele de transmitere a semnalelor optice şi electrice;

f) de a elimina confuzia şi de a sistematiza firele din traseele de cablu;

g) de a crea serviciul unic de exploatare;

h) de a asigura cu transfer de informaţii principala parte a echipamentului de reţea actual şi cel de perspectivă de diferite clase, în caz de disponibilitate a unei interfeţe standardizate;

i) de a asigura localizarea rapidă a deranjamentului, recuperarea legăturii sau trecerea la linii de rezervă în baza principiului modular de construcţie.

4.1.1. Structura SCS

1) Topologie SCS

12. La baza oricărui sistem de cablare structurat este pusă topologia arborescentă, care uneori este denumită structură ierarhică a stelei.

13. Nodurile structurii sunt considerate încăperi tehnice (de crosare şi de aparate), care sunt conectate între ele cu locuri de muncă, cabluri electrice şi optice.

14. Toate cablurile de intrare în încăperile tehnice, se introduc obligatoriu în echipamente de comutare pe care se desfăşoară comutarea în procesul exploatării curente a sistemului de cablaj. Acest lucru oferă flexibilitate SCS, posibilitate uşoară de reconfigurare şi de adaptare sub o aplicaţie concretă, pentru susţinerea funcţionării tuturor aplicaţiilor principale de reţea (vezi tabelul nr.2).

Tabelul 2. Topologia logică şi fizică a reţelelor moderne de date

Protocol	Topologia logică	Topologia fizică
Ethernet	Magistrală de date	Magistrală de date, stea
Fast Ethernet	Magistrală de date	Stea
Gigabit Ethernet	Magistrală de date	Stea

15. Din tabelul nr. 2 se constată că topologia analizată este considerată acea platformă care asigură suportul lucrărilor moderne ale mijloacelor de transfer de date.

2) Încăperi tehnice

16. Pentru a construi un SCS şi un sistem informaţional al unei întreprinderi în ansamblu sunt necesare încăperi tehnice de două tipuri: de aparataj şi de crosare. **17.** Camera de aparataj în continuare va fi denumită încăpere tehnică, în care se aranjează echipamentul de reţea (CTA, servere, concentratori).

18. În cazul în care volumul de bază al echipamentelor tehnice instalate în încăpere constituie echipamentul reţelei interne, atunci această încăpere se numeşte cameră de servere, iar dacă echipamentul constituie CTA intern şi sisteme de telecomunicaţii externe – atunci încăperea se numeşte nod telecomunicaţional.

19.Încăperile de aparataj se amenajează cu podele false, sisteme antiincendiare, sisteme de aer condiţionat şi sisteme de control al accesului.

20. Camera de crosare este o încăpere, în care se amplasează echipamentul de comutare al SCS, de reţea şi alte echipamente auxiliare. Se recomandă ca încăperea să se afle în apropierea coloanelor verticale, să fie amenajată cu aparat telefonic şi sistem de control al accesului. Cu toate acestea, nivelul de echipare al încăperii de crosare cu echipament ingineresc, asigurarea funcţionării acestuia, în ansamblu sunt indicatori mai mici decât cele ale camerei de aparataj. Camera de crosare, în practică, este adesea numită pur şi simplu încăpere tehnică (de etaje).

21. Sala de aparate poate fi compatibilă cu încăperea de crosare (ÎC). În acest caz, echipamentul de reţea poate fi conectat direct la echipamentul de comutare al SCS.

22. Dacă camera de aparate este situată separat, atunci echipamentul de reţea se conectează la echipamentul de comutare local sau la prize simple.

23. În camera de comutare a magistralei externe (CME) se aduc cablurile magistrale externe, la care se conectează ÎC.

24. În ÎC se introduc cablurile magistrale interne, la care se conectează camerele de crosare pe etaj. Cablurile orizontale din camerele de crosare pe etaj sunt , la rândul lor, conectate la prizele informaţionale de la locurile de muncă.

25. În calitate de conexiuni suplimentare, care majorează flexibilitatea şi funcţionalitatea sistemului, se permite trasarea cablurilor magistrale externe între ÎC şi cablurile magistrale interne între CME.

26. În toate SCS poate exissta doar cîte o CME, şi în fiecare clădire poate fi prezentă nu mai mult de o ÎC.

27. Se permite consolidarea CME cu ÎC, atunci cînd acestea sunt situate în aceeaşi clădire. În mod similar, ÎC ar putea fi unită cu CME, în cazul în care sunt amplasate pe un etaj.

28. Dacă densitatea locurilor de muncă este mică, o excepţie este de a permite să se conecteze la CME cablurile orizontale ale etajelor conexe.

3) Subsisteme SCS

29. În general, SCS include trei subsisteme:

a) subsistemul magistralelor externe, sau (subsistemul primar) constă din cabluri magistrale interne între CME şi ÎC, echipamente de comutaţie în CME şi ÎC, la care se conectează cabluri magistrale externe şi link-uri de comutare şi / sau de conectare în CME. Subsistemul magistralelor externe se consideră temelia pentru construirea unei conexiuni de reţea la una dintre clădiri (campus) între două clădiri situate alături. În practică, acest subsistem are, adesea , o topologie fizică de inel, care în mod suplimentar asigură majorarea fiabilităţii din contul existenţei traseelor de cabluri de rezervă. Din aceleaşi considerente, subsistemul magistralelor externe uneori se realizează după topologia dublă de inel. În cazul în care este setat la SCAS în mod autonom, numai într-o singură clădire, atunci subsistemul magistralelor externe este absent;

b) subsistemul magistralelor interne, (vertical, sau secundar) conţine între CP şi CE cabluri magistrale interne, la care este conectat echipamentul de comutare în CP şi CE şi link-urile de comutare şi / sau de conectare în CP. Cablurile subsistemului prezentat, de fapt, conectează între ele etaje separate ale clădirii şi / sau încăperile dintr-un spaţiu al clădirii. Dacă SCS deserveşte un etaj, atunci subsistemul magistralelor interne poate lipsi;

c) subsistemul orizontal(terţiar), este creat de cabluri orizontale interne între etajele de crosare şi prizele informaţionale de la locurile de muncă, prizele informaţionale în sine, echipamentul de comutare în etajele de crosare, la care se conectează cablurile orizontale, şi link-urile de comutare şi / sau de conectare în CP. În componenţa cablajului orizontal se permite utilizarea unui singur punct de tranziţie, în care se petrece o modificare a tipului de cablu pozat (de exemplu, trecerea de la cablu plat pentru trasarea lui sub covor cu caracteristici de transmisie echivalente).

30. Divizarea SCS pe subsisteme izolate se aplică indiferent de tipul sau forma de punere în aplicare a reţelei, el va fi identic, atît pentru birou, cît şi pentru reţea.

31. Uneori, din motive de comoditate a proiectării şi exploatării se utilizează echipamentul de zdrobire mai mic al SCS pentru subsisteme despărţite. Astfel, , elementele de conectare a echipamentelor de reţea din camera de crosare a SCS se separă într-un subsistem administrativ separat, cabluri, adaptoare, precum şi alte elemente necesare la locul de muncă, formează un subsistem separat al locului de muncă, etc.

32. În majoritatea cazurilor ce ţin de conectarea echipamentului de reţea la SCS, aceasta se realizează cu ajutorul link-ului de comutare. În unele situaţii, în afară de link poate fi necesar un adaptor pentru a asigura coordonarea de semnalizare şi parametrii mecanici ai interfeţelor (conectorilor) optice sau electrice ale SCS şi echipamentului de reţea. De exemplu, adaptoarele se aplică pentru a se conecta la echipamentul de reţea al SCS cu interfeţe V.24 (RS-232), la dispozitivele sistemului de televiziune prin cablu, sistemele IBM AS/400 cu terminale 5250, controlorul de terminal IBM 3274 şi terminalele 3270, precum şi la alte aplicaţii, care au fost elaborate pentru alte sisteme de cablu.

33. Subsistemul locurilor de muncă oferă conectarea echipamentului de reţea, la locurile de muncă. Echipamentul aplicat pentru realizarea conectării este în întregime dependent de cererile de aplicare. Subsistemul nu este parte a SCS, şi nu intră în sfera de aplicare a standardelor SMV ISO/CEI 11801:2009, cu toate că aceste documente normative suprapun pe ea parametrii şi caracteristicile de delimitare.

4) Comutarea în SCS

34. Principala caracteristică a oricărei SCS este că trecerea la ea, spre deosebire de CTA electronice şi a echipamentului de reţea, se face întotdeauna manual cu cabluri de comutare şi/sau conectare. Cea mai importantă consecinţă a acestei abordări este că funcţionarea unei SCS nu depinde de starea reţelei de alimentare cu energie.

35. Introducerea în SCS a componentelor electronice sau electromecanice, precum şi trecerea imediată, presupune utilizarea obligatorie a echipamentului sursei de putere. Această decizie este absolut nejustificată din punct de vedere economic şi tehnic pentru etapa de dezvoltare a tehnicii. Aceasta se datorează faptului că în mediu comutarea unui port în sistemul actual se poate efectua o dată pe an, iar sursa de alimentare reduce semnificativ fiabilitatea operaţională în comparaţie cu componentele pasive, care formează un sistem de cablu.

36. Cealaltă parte a refuzului de la sursa standard de alimentare cu energie electrică se consideră:

a) necesitatea utilizării cablurilor de comutare, care în mod semnificativ ar înrăutăţi indicatorii de masă şi gabarite a echipamentului de comutare şi necesită aplicarea măsurilor speciale pentru a face faţă sarcinilor administrative;

b) imposibilitatea introducerii în componenţa SCS a comutatoarelor standarde, de control, senzori şi alte echipamente similare, care reduc uşurinţa de exploatare, majorează timpul de căutare a deranjamentului, complică diagnostica curentă etc.

37. Există doar câteva lucrări în producţie de serie, care au ca scop introducerea componentelor în unele subsisteme ale SCS. Cu toate acestea, ele au un caracter auxiliar (un studiu al stării porturilor, comutarea semnalelor aplicaţiilor lente), nu ating procesul de transmitere a semnalelor informaţionale şi nu sunt standardizate sau nu conţin sugestii pentru ediţiile viitoare.

5) Principiile de administrare a SCS

38. Principiile de administrare sau de management al SCS sunt totalmente determinate de structura sa. Există modul unipunct şi modul multipunct de administrare.

39. Administrarea de multipunct este administrarea SCS, care a fost construită pe arhitectura clasica a stelei ierarhice. Principalele criterii ale acestei versiuni, este nevoia de a schimba minim două cabluri şi în general modificarea configuraţiei. Utilizarea acestui principiu asigură flexibilitate în ceea ce priveşte gestionarea şi dă posibilitatea de adaptare a SCS pentru susţinerea noilor aplicaţii.

40. Arhitectura unică de administrare este utilizată în situaţiile în care se doreşte de a facilita gestionarea sistemelor de cablu. Principiile acesteia pot fi utilizate numai pentru SCS amplasate într-o clădire şi lipsite de subsisteme magistrale. Principala sa caracteristică este legătura directă la toate prizele informaţionale ale locurilor de muncă cu camera tehnică.

41. Administrarea unipunct poate fi utilizată numai în reţele mici şi simplifică procesul de administrare a sistemului de cablu din contul necesităţii de punere în aplicare a tuturor cablurilor care trec printr-un singur loc.

6) Cablurile SCS

42. O modalitate de îmbunătăţire a eficienţei tehnice şi economice de cablu a sistemelor de birou este de a minimaliza tipurile de cabluri aplicate la construcţia lor.

43.În SCS, în conformitate cu standardul internaţional SMV ISO/CEI 11801:2009, pot fi utilizate doar:

a) cabluri simetrice electrice pe baza cablului torsadat cu val de rezistenţă de 100, 120 şi 150 ohm în performanţă ecranată şi neecranată;

b) cabluri optice singlemode şi multimode.

44. Cablurile electrice sunt utilizate, de obicei, pentru crearea branşamentului orizontal. Ele sunt transmise ca semnale de telefon cu viteză redusă şi de date de mare viteză pentru aplicaţii de date.

45. Utilizarea soluţiilor optice în subsistemul orizontal este acum găsit rareori, deşi ponderea lor este în creştere foarte rapidă (în contextul fibrelor to the desk).

46. În subsistemele magistralelor interne, cablurile electrice şi optice sunt folosite la fel de des, dar cablurile electrice sunt destinate în principal pentru transferul semnalelor de telefon şi a datelor cu frecvenţe de până la 1 MHz, în timp ce cablurile optice furnizează transfer de mare viteză pentru aplicaţiile de date. Pe magistrale cablurile optice joacă un rol dominant.

47. Pentru a trece de la cabluri electrice în optice, în procesul transmisiei datelor la viteze de 10 Mbps sau mai mare, în încăperi tehnice se instalează echipamentul de reţea corespunzător (media convertoare, sau transivere), care servesc de obicei,

aparatajul de grup (un hub al sistemului transport de date, modul de PBX controler al sistemului ingineresc al clădirii, etc.)

48. Utilizarea directă a cablurilor de fibră-optică pentru transmiterea semnalelor de telefon şi de încetinire a transmiterii datelor, în perioada modernă a tehnologiilor, este imposibilă din punct de vedere economic şi foarte rar folosită, cu excepţia situaţiilor în care celelalte soluţii nu sunt posibile sau sunt cerinţe specifice de protecţie a informaţiilor de la acces nesancţionat. Prin urmare, în scopul îmbunătăţirii eficienţei tehnice şi economice a reţelei în ansamblul este, necesar procesul de transformare a semnalului electric lin în optică, combinat cu multiplexare.

49. Pentru a construi un subsistem orizontal, se permite utilizarea ecranată şi neecranată a cablurilor.

50. Cablul ecranat simetric potenţial are cele mai bune caracteristici, comparativ cu cel neecranat. Cu toate acestea, acest cablu este foarte critic la calitatea de instalare şi de împământare, costul acestuia fiind mai mare şi indicatorii de greutate mai mici.

51. Cablurile multimode de fibră optică sunt utilizate, de obicei, ca bază pentru subsistemul magistralelor interne. Cablurile multimode se recomandă a fi aplicate numai în cazul construirii magistralelor de dimensiuni mari.

52. Cablurile coaxiale nu sunt permise pentru utilizare. Acest fapt se datorează fiabilităţii mai mici a reţelelor care sunt construite pe această bază, tehnologiei mici şi costului mai mare în comparaţie cu cablurile pe baza cablului torsadat.

53. Pentru asigurarea capacităţii de lucru, pe SCS al echipamentelor de reţea pentru interfaţă coaxială şi triaxială se utilizează nomenclatorul larg de adaptere de diferite tipuri.

4.1.2. Clase şi categorii. Legătura lor cu lungimile traseelor

1) Clasele aplicaţiilor, categoriile cablurilor şi conectoarelor SCS

54. Toate tipurile de aplicaţii, ce pot executa schimb de date în baza cablului torsadat, sunt împărţite în 4 clase — A, B, C şi D (vezi tabelul nr. 3). Clasa A se consideră inferioară, D - superioară.

55. Pentru protocoalele fiecărei clase, se alocă categoria necesară a liniilor de transmitere de date, care determină caracteristicile electronice limită, necesare pentru lucrul normal al protocolului specificat şi al protocoalelor inferioare.

56. La protocoalele optice se referă cele ce utilizează ca mediu de transmitere a datelor fibra optică. Pentru acest tip de protocol, mărimea benzii de transmitere a datelor nu este o limită.

Tabelul 3. Clasele aplicaţiilor ISO/IEC 11801

Clasa liniei şi a protocolului	Definire
A	Canal de telefonie, linie cu frecvenţă redusă de transmitere a datelor. Frecvenţă maximă a semnalului – 100 KHz
B	Aplicaţie cu viteză medie de transmitere a datelor. Frecvenţă maximă – 1 MHz

C	Aplicaţie de schimb de date la viteză înaltă. Frecvenţă maximă – 16 MHz
D	Aplicaţie cu viteză ultra-înaltă de transmitere a datelor. Frecvenţă maximă – 100 MHz
FO	Aplicaţie de transmitere a datelor prin fibră optică

57. Este important faptul că standardul ISO/IEC 11801 nu presupune aplicaţii şi linii cu frecvenţă maximă de transmitere a datelor 20 MHz, care corespund categoriei 4 a conectoarelor şi cablurilor, ceea ce se datorează răspîndirii scunde a aplicaţiilor de transmitere a datelor la frecvenţe de 16-20 MHz.

Tabelul 4. Corespunderea categoriei cablurilor şi conectoarelor claselor aplicaţiilor

TIA/EIA-568-A	**ISO/IEC 11801**	**ISO/IEC 11801**
	Cabluri şi conectoare	Aplicaţii
-		A
-	-	B
Categoria3	Categoria 3	C
Categoria4	Categoria 4	-
Categoria5	Categoria 5	D
-	Categoria 6	E
-	Categoria 7	F

58. La fel se practică şi introducerea unor derivări de standarde. Spre exemplu în unele ţări vorbitoare de limbă germană, categoria aplicaţiilor ce activează la 200 MHz cîteodată este denumită D+, iar cea ce ajunge la 300 mHz - D++.

59. În afară de cablaj, după categorii se specifică şi conectoarele. Categoria se determină prin frecvenţa maximă, specifică anumitor tipuri de conectoare şi cabluri. Cablurile şi conectoarele de categorii înalte suportă toate tipurile de aplicaţii specifice cablurilor şi conectoarelor de nivel mai inferior.

Tabelul 5. Categoriile cablurilor şi conectoarelor

Categoriile cablu-conector	**Frecvenţa maximă**	**Protocoale tipice**
Categoria 3	Pînă la 16 mHz	Reţele interne Token Ring şi Ethernet 10Base-T, canale voice,

		şi alte canale de viteză mică
Categoria 4	Pînă la 20 mHz	Reţele interne Token Ring şi Ethernet 10Base-T
Categoria 5	Pînă la 100 mHz	Reţele interne pînă la 100 mbps
Categoria 6	Pînă la 200 mHz	Reţele interne cu viteză pînă la 155 mbps
Categoria 7	Pînă la 600 mHz	Reţele interne cu viteză pînă la 1000 mbps

2) Limitările lungimilor cablurilor şi link-urilor SCS

60. Limitele pe lungimile maxime ale cablajului şi a cablurilor de interconectare (link) ale subsistemelor orizontale şi magistralesunt descrise în tabelul 6.

61. Lungimile maxime ale liniilor electrice de transmitere a semnalului de clasă menţionată sunt date, ţinînd cont de structura simetrică a cablajului şi a altor componente, cu categoria nu mai joasă decît cea stipulată.

A+B+E5 10 mC şi D <, 20 mF şi G < 30 m

a) Lungimea sumară a tuturor cablurilor şi link-urilor subsistemului

b) Lungimea cablurilor comutaţionale (link-uri) în camera de comutare şi camera de crosare a magistralelor interne (CCME);

c) Lungimea cablajului terminal în camera de comutare şi CCME.

62. Specificare:

a) Toate lungimile sunt lungimi fizice.

b) Lungimile 10 m (A+B+E) şi 30 m (F şi G) sunt recomandate.

63. Lungimea cablului subsistemului orizontal este stabilită la 90 m (+ 10m pentru link-uri). Alegerea respectivă se datorează posibilităţii cablului torsadat (ca sistem ghidant de variaţii electromagnetice) de a transmite semnalul celor mai răspîndite protocoale de tip Fast Ethernet.

64. În determinarea distanţei se ia în consideraţie posibilităţile şi nivelul tehnic al echipamentelor de reţea, la momentul scrierii standardelor. Nu în ultimul rînd se iau în cosideraţie şi cele mai răspîndite tipuri arhitecturale a încăperilor de oficiu.

Tabelul 6. Lungimile maximale ale cablajului, în dependenţă de tipurile de cabluri şi aplicaţii

Clasa aplicaţiei	**A**	**B**	**C**	**D**	**F O**
Mediul de transmitere a semnalului					
Cablu simetric categoria 3	2km	200 m	100 m		
Cablu simetric categoria 4	3km	260 m	150 m		
Cablu simetric categoria 5	3km	260 m	160 m	100 м	
Cablu simetric categoria 150 Ом	3km	400 m	250 m	150 м	
Fibră optică Multimod	-	-	-	-	2km

Fibră optică Monomod	-	-	-	-	3km

65. Specificaţie:

a) Lungimea de 100 m este lungimea sumară a cablajului orizontal (90m) şi a cablurilor de interconect.

b) 3 km — limită formală. Nu este o limită fizică pentru dioda monomodă.

66. În cazul creării subsistemului orizontal pe bază de fibră optică, lungimea traseului este stabilită la 90 m din considerente că ea garantează efectuarea limitărilor la nivel de protocol în reţelele FastEthernet pe diametrul maxim al domeniului de colizii.

67. Subsistemul magistralelor interne se foloseşte pentru interconectarea într-un tot întreg a facilităţilor tehnice în cadrul unui edificiu. Reieşind din aceasta, lungimea maximă se stabileşte la 500 m.

68. Subsistemul magistralelor externe, cel ce interconectează diferite edificii, poate fi constituit din cabluri cu lungimea maximă de 2 sau 3 km, în dependenţă de tip, iar prin intermediul echipamentului de reţea aceasta poate fi extinsă la sute de kilometri. La transmiterea de date pe distanţe lungi se pot folosi liniile de transmitere de date a diferitor operatori telecomunicaţionali.

4.1.3. Variante suplimentare ale topologiei SCS

69.În continuare sunt descrise variante suplimentare de creare a subsistemului orizontal de cablaj, a subsistemului de magistrala internă. Prezenţa acestor variante măreşte considerabil libertatea de alegere a proiectantului şi permite sporirea eficienţei tehnico-economice a sistemului de cablaj în majoritatea SCS întîlnite.

1) Modele de creare a reţelelor SCS

70. Subsistemul orizontal SCS, creat în baza cablului torsadat poate fi executat în 4 modele diferite.

71. Primul model este cel mai răspîndit şi este caracterizat prin folosirea cablului direct (cu lungimea maximă de 90m) ce interconectează priza informaţională şi panelul de comutare în facilitatea de crosare.

72. Modelul doi se caracterizează prin formarea tractului de transmitere din două cabluri de tip diferit, dar cu caracteristici echivalente de transmitere a datelor.

73. Conform normativelor, sunt descrise două posibilităţi de combinare cablurilor de acest tip: cablul cu multiple perechi + cablul cu 4 perechi şi cablul de formă plată + cilindrul cu acelaşi număr de perechi (în practică se folosesc cabluri cu 4 perechi). Ele se interconectează în aşa numitul punct de interconectare PI.

74.PI se realizează pe echipamentul comutaţional, însă este interzisă folosirea lui în administrarea SCS şi pentru conectarea echipamentului de reţea activ. În conformitate cu cele expuse, în punctul de trecere, niciodată nu poate fi aplicat echipament comutaţional sau link-uri terminale.

75. Ultimele două modele de creare a subsistemului orizontal SCS se folosesc pe scară largă în aşa numitele oficii deschise (open offices), adică încăperi de metraj mare, împărţite în secţii prin intermediul mobilierului specializat sau a pereţilor uşori, necapitali.

76. O proprietate comună a acestui tip de oficii este fluxul sporit al angajaţilor, şi schimbările dese ale locurilor de muncă, precum şi prezenţa zonelor de grupare a locurilor de muncă şi a tehnicii de calcul. În tipul respectiv de oficii se pot utiliza prizele telecomunicaţionale cu acces multiplu MUTO (Multi-User Telecommunication outlet) şi punctele de consolidare CP (consolidation point). Ambele varianteadaptează exemplele de SCS descrise mai sus (tabelul nr. 7).

Tabelul 7. Analogiile între diferitele modele de organizare a subsistemului orizontal.

Tipul de	Conexiune directă	Conexiune multi-utilizator
Oficiu	Link simplu	Punct de trecere
Open	Priză multi-acces	Punct de consolidare

77. Termenul MUTO se aplică la priza care deserveşte cîţiva utilizatori. Acest tip de priză se clasifică aparte (par. 3.3.3.2.2) şi se instalează pe coloanele şi pereţii încăperii, sub podeaua falsă, în boxe specializate.

78. Lungimea maximă W a link-ului terminal, ce conectează priza MUTO cu echipamentul telecomunicaţional nu trebuie să fie mai mare de 20 m şi se calculează prin formula:

$$W= (102-H)/1,2-7 \text{ m}, W<20 \text{ m}, (1)$$

unde H — lungimea cablajului orizontal;

1,2 - Coeficient ce specifică mărimea sporită de atenuare a semnalului în cablul de interconectare din conductor din fibre multiple.

7 - Coeficient constant ce denotă mărimea maximă a cablurilor de interconectare a echipamentului în camerele de crosare.

79. Formula (1) demonstrează că la lungimea maximală de 20 m a cablurilor terminale, lungimea cablajului orizontal nu trebuie să depăşească 70 m.

80. În aşa fel, lungimea totală a terminalului şi a link-ului comunicaţional în oficiul de tip deschis poate ajunge la 27 m în loc de 10 m în cazul oficiului simplu, ceea ce duce la mărirea flexibilităţii sistemului de cablare.

81. Punctul de consolidare CP în oficiul deschis este analogul direct al punctului de trecere în topologia standard. De la el, la prizele de lîngă locurile de muncă se trag porţiuni scurte de cablu orizontal care sunt prelungiri a cablului de bază.

82. SCS bazată pe CP se recomandă în cazurile cînd frecvenţa schimbării locurilor de muncă este mai mică decît în cazul aplicării prizelor MUTO.

83. La fel ca şi în cazul cablării tradiţionale, în oricare linie orizontală a oficiilor de tip deschis se interzice utilizarea a mai mult de un punct de trecere (MUTO şi CP), iar în punctul de consolidare nu se permite conectarea echipamentului activ şi executarea operaţiilor de administrare.

2) Topologia cu administrare centralizată

84. Sistemele cu administrare centralizată se referă la crearea reţelei prin cablaj optic. Ideea de bazăconstă în prezentarea proiectantului SCS a posibilităţii dezicerii în situaţia dată de împărţirea strictă a cablajului în subsistem orizontal şi subsistem al magistralelor interne, cu comasarea acestora într-un tot întreg, trecînd de la topologia stea de doua nivele la una simplă cu un nivel.

85. Aplicarea principiului administrării centralizate permite:

a) mărire considerabilă a administrării reţelei interne din contul noilor posibilităţi de creare (pe viitor) a diferitor grupuri de lucru la nivel fizic fără folosirea conexiunilor virtuale;

b) acumularea echipamentului activ într-un singur loc, ceea ce determină sporirea nivelului de securizare şi apără de la accesul nesancţionat la informaţie, diminuează necesitatea în canale de viteză înaltă şi simplifică procesul de luare a măsurărilor exploataţionale; diminuarea semnificativă şi chiar totală (în unele cazuri) a spaţiului dedicat camerelor de crosare pe etaje.

86. Actualitatea folosirii în practică a metodei de administrare centralizată s-a mărit brusc odată cu implementarea în masă a tehnicii de transmitere a semnalelor prin fibră optică, care nu impune limitări pe lungimile canalelor de viteză înaltă precum ar fi cea de 90 metri pentru canalul de transfer de date în baza cablului torsadat.

87. Sistemele de cablare examinate, pot fi construite în baza următoarelor variante: cu folosirea unei interconexiuni şi fără aceasta.

88. Folosirea unei interconexiuni permite păstrarea infrastructurii existente a edificiului, cauza fiind amplasarea aparatajului de crosare în camerele de crosare rezervate de proiectul iniţial.

89. Această variantă la rîndul său poate fi executată în 2 scheme diferite; prima poate fi numită schemade ramificare. Conform acesteia, pînă la aparatajul de crosare se aduce cablul de magistrală, iar următoarea multiplicare se efectuează de către cablul abonatului care se aplică pe cablul magistrală cu un interconector.

90. A doua schemă a primit denumirea de panel pasiv de comutare. Conform acestei scheme se exercită procesul de comutare prin intermediul cablului comutaţional.

91. Distanţa maximă de la priza informaţională şi pînă la dulapul de comutare nu poate depăşi 90m, ceea ce se conformează cerinţelor în privinţa cablajului orizontal şi permite revenirea uşoară la topologia generală binivel.

92. Lungimea maximă a canalului cu interconectare se alege 300 m, din considerentele primirii unui canal de transfer de date de 1 Gbit/s într-un cablu de fibră optică de tip 62,5/125, ceea ce acoperă necesităţile aplicaţiilor de viteză înaltă de tipulGigabit Ethernet şi Fibre Channel.

93. Prin analogie cu structurile pe cablu electric, în care se folosesc puncte de trecere de tip diferit, în locul amplasării crosului nu se instalează echipament activ de orice fel.

94. Limitările protocoalelor reţelelor Fast Ethernet, în cazul dat se consideră neprincipiale, posibil din cauza unei folosiri pe scară mică a aparatajului de fibră optică de standardul 100Base-FX, care lucrează în regim de împărţire a benzii.

95. La crearea SCS fără interconexiune, lungimea oricărui cablaj nu poate depăşi 90 m, pentru a se încadra în standardele existente. Acest fapt considerabil reduce posibilitatea organizării sistemului cu administrare centralizată într-un şir de încăperi de oficiu, însă permite dezicerea de etaje de crosare dedicate. În cazul cînd acestea sunt prevăzute de proiect, se aplică schema de tranzit şi atunci în sălile de crosare se propune păstrarea cablului de rezervă şi a echipamentului comutaţional.

96. Limitări şi recomandărisuplimentare:

a) în punctul interconectării nu se recomandă aplicarea diferitor tipuri de conectoare a fibrelor optice;

b) tipul de bază al conectoarelor optice se consideră SC, în varianta simplex sau duplex;

c) conexiunea neflexibilă poate fi efectuată prin intermediul sudurii sau cu ajutorul splice-lor mecanice;

d) în varianta cu o interconectare, în cazul aplicării unei conexiuni neflexibile a fibrelor, se permite utilizarea diferitor tipuri de cablaj în subsistemele de cablaj orizontal şi magistral;

e) identificarea şi marcarea fibrelor şi conexiunilor trebuie efectuate în conformitate cu cerinţele şi normele în vigoare.

4.1.4. Principiul cable sharing

97. Tipul de bază al cablajului folosit în subsistemul modern orizontal al SCS este cablul simetric torsadat (4 perechi, care la rîndul lor au patru variante diferite de executare).

98. Cele mai răspîndite aplicaţii de viteză medie (Ethernet 10Base-T, Token Ring) şi de viteză mare Fast Ethernet 100Base-TX, TP-PMD, ATM) necesită pentru funcţionare doar două perechi. Celelalte două perechi nu se utilizează în transmiterea datelor, iar în unele plăci de reţea sunt împământate, ceea ce înseamnă că sunt inutile.

99. Nivelul caracteristicilor tehnice ale cablajului orizontal permite transmiterea prin cablu, în acelaşi interval de timp pînă la două, iar în unele cazuri trei sau patru aplicaţii fără un impact observabil unora asupra altora. O astfel de soluţie de aplicare a cablajului orizontal are denumirea de cable sharing (împărţirea sau disocierea cablului).

100. Pentru realizarea practică a principiului cable sharing sunt elaborate şi implementate în producerea de serie un şir vast de elemente specializate care pot fi clasificate în următoarele grupe:

a) Y-adaptor, balun dublu şi triplu;
b) Priză dubla adaptabilă;
c) Cordon bifocar;
d) Cordon de montare de tip special;
e) Module duble pentru prize, ce permit bifocarea cablurilor.

101. Grupele enumerate la alineatul 100, în afară de ultimele două, permit o întoarcere uşoară la standardul de 4 perechi pentru organizarea reţelei orizontale de transmitere a semnalului electric, ceea ce înseamnă că nu afectează universalitatea sistemului de cablare.

102. Pentru aparatajul folosit în realizarea principiului cable sharingnu sunt necesare cerinţe adăugătoare, în afară de marcarea diferită a prizelor.

103. Cele mai adaptate cabluri pentru transmiterea concomitentă a doua semnale sunt cele cu torsiunea pătratică, care, în temei, reprezintă 2 elemente plasate sub un ambalaj.

104. Folosirea principiului de organizare a SCS este binevenit în reţelele mici şi mijlocii şi este determinat de două premise:

a) în acest tip de reţele, cheltuielile de creare a cablajului orizontal sunt relativ mari, iar transmiterea într-un singur cablu a două semnale micşorează considerabil cheltuielile capitale de organizare a reţelei;

b) necesitatea de folosire a conexiunilor de viteză înaltă (Gigabit Ethernet) este

joasă datorită volumului mai mic de informaţie transmisă: în astfel de condiţii problema neajunsului de bandă de transport de date trece printr-o perspectivă îndelungată.

4.2. Arhitectura şi cerinţele faţă de infrastructura de acces Internet

105. Serviciile *de acces Internet oferă posibilitatea de conectare la reţeaua globală Internet, constituită din* calculatoarele şi reţele de calculatoare interconectate între ele, care la rîndul lor sunt deţinute de alte sisteme tehnico-organizatorice (agenţii guvernamentale, societăţi, instituţii academice, Internet Service Providere).

106. Arhitectura infrastructurii de acces la Internet este reprezentată de un şir de echipamente de telecomunicaţii de nivelul 3 al modelului OSI (Network Layer) ce pot garanta transportarea pachetelor de la sursă la destinaţie, determinînd calea cea mai scurtă. Astfel se definesc *puncte de acces la Internet*ce sunt reprezentate prin aceste echipamente telecomunicaţionale (routere).

107. Principii şi metode de organizare a infrastructurii de acces Internet:

a) Principiul accesibilităţii
b) Principiul accesului unic
c) Principiul transparenţei
d) Principiul partajării resurselor
e) Principiul securităţii

108. Punctul de acces la Internet, după nivelul de complexitate al reţelei interne (vezi capitolul Clasele de sisteme informaţionale interne) se clasifică în:

a) Punct de acces de Clasa 1 – routere Software;
b) Punct de acces de Clasa 2 – routere Low-end;
c) Punct de acces de Clasa 3 – routere Low-end flexible
d) Punct de acces de Clasa 4 – routere Midrange
e) Punct de acces de Clasa 5 – routere High-End

109. Punctul de acces de clasa 1este echipamentul ce include posibilitatea de rutare a traficului dintre reţeaua internă LAN şi WAN. La fel poate fi atît echipament computaţional fizic cît şi un produs software cu funcţia de router instalat pe SO mamă. Sistemul computaţional asigurînd funcţionalitatea operaţiilor de bază pe cînd funcţia de router (funcţia de rutare) este procesată în fundal (engl. background). Astfel de tip de router asigură accesul la Internet a unui grup mic de calculatoare (<5). Performanţa lor fiind redusă din cauza faptului că procesul de rutare, ne fiind primordial, este direct orientat spre procesarea operaţiilor de rutare.

110. Performanţa şi stabilitateaunui astfel de router este direct dependentă de capacităţile fizice ale calculatorului, ce are funcţia de software router.Astfel de routere sunt benefice în caz de realizare a accesului la Internet a unui număr mic de calculatoare, cerinţele faţă de acces WAN fiind minime (în cazul în care nu este necesară aplicarea regulilor de trafic engineering).

111. Tabelul 8 sumează posibilităţile tehnice ale acestui tip de router:

Tabelul 8. Posibilităţile tehnice ale *routerelor Software*

Posibilităţi tehnice
Router în Regim de aplicaţii soft
Simplu în configurare
Posibilitatea de transformare a adreselor IP (NAT) inclusă

Lipsa protocoalelor de rutare
Independent faţă de tipul de OS selectat (Windows, Linux etc.)

112. Punct de acces de clasa 2este echipamentul de telecomunicaţii L3 cu posibilităţi tehnice de bază ale SO, care este limitat în posibilităţi tehnice şi fizice atît de procesare a operaţiilor de rutare şi altor tipuri, cît şi în posibilităţi de expansiune.

113. Aceste clase de routere sunt destinate rutării traficului dintre reţelele LAN în WAN. Routerul de această clasă are inclus în sine modulul de HUB sau Switch, la fel dispune şi de posibilităţi de bază ale firewall-ului.

114. Configurarea routerului de clasa 2 este realizată pe un Sistem de Operare cu fişier de configurare personalizat, astfel evitînd utilizatorului modificarea involuntară, persistă nivel de autentificare.

115. Acest tip de routere nu dispun de posibilităţi de redundanţă, dar sunt echipamente dedicate cu o configuraţie hardware predefinită, fără posibilitatea de extindere şi instalare adiţională a modulelor telecomunicaţionale. În vederea realizării redundanţei este benefică instalarea, configurarea unui al doilea router.

116. Sunt utilizate protocoalele de rutare de bază: RIP OSPF, la fel dispun şi de posibilitatea de translare NAT în scop de asigurare a accesului la WAN a utilizatorilor din LAN.

117. Performanţa este limitată, dar mai benefică decît în cazul routerelor de Clasa 1, deoarece în activitatea de procesare a operaţiilor de rutare sunt concentrate modulele fizice strict orientate spre rutare şi nicidecum a altor operaţii.

118. Această clasă de routere este destinată pentru reţele mici (<20 în dependenţă de posibilităţile fizice ale echipamentului ex. RAM, CPU, Ethernet Module), parte integră a Clasei I de infrastructură.

119. Tabelul 9 sumează posibilităţile tehnice ale acestui tip de router:

Tabelul 9. Posibilităţi tehnice ale *routerelor Low-end*

Posibilităţi tehnice
Inexistenţa majorării fizice a capacităţii echipamentului
Protocoale de rutare RIP şi OSPF
Performanţa limitată
Simplitate în configurare a echipamentului
Modul de HUB, Switch inclus
Existenţa firewall-ului, configuraţie de bază
Posibilitatea de transformare a adreselor IP (NAT) inclusă

120. Punct de acces de clasa 3reprezintă echipamente de telecomunicaţii similare echipamentelor de clasa 2, dar există posibilitatea de majorare a capacităţilor fizice şi respectiv a eficacităţii, în dependenţă de necesitate şi modelul producătorului.

121. În cadrul acestei clase de routere există posibilitatea conectării diferitor tipuri de WAN conexiuni sau interfeţe la fel şi prin intermediul interfeţelor Ethernet, FastEthernet. Dau dovadă de o performanţă mai avansată decît clasele anterioare, datorită posibilităţii de expansiune a interfeţelor, modulelor adiţionale fără modificarea procesorului de bază.

122. Tabelul 10 sumează posibilităţile tehnice ale acestui tip de router:

Tabelul 10. Posibilităţile tehnice ale Punctului de acces de clasa 3

Posibilităţi tehnice
Posibilitatea majorării fizice a capacităţii echipamentului
Varietate largă de conexiuni şi interfeţe WAN
Protocoale de rutare RIP şi OSPF
Suport de VLAN (802.1q)
Performanţa limitată
Simplitate în configurare a echipamentului
Modul de HUB, Switch inclus
Existenţa firewall-ului, configuraţie de bază
Posibilitatea de transformare a adreselor IP (NAT) inclusă

123. Punct de acces de clasa 4reprezintăroutere de gamă medie (engl. Midrange), sunt clasificate la un nivel mai înalt decît routerele de clasa 3.

124. Se manifestă prin multiplele interfeţe WAN, LAN şi prezenţa porturilor Ethernet, FastEthernet, Gigabit Ethernet (10/100/1000Mbps), utilizînd mediul de transport cupruşi/sau fibră-optică.

125. Prezenţa protocoalelor adiţionale în cadrul sistemului de operare, permite ca routerele Midrange să ofere o gamă largă de funcţionalităţi tehnice. Apare posibilitatea de utilizare a protocolului SIP (VoIP), ce permit transmiterea datelor şi vocii simultan. De asemenea, redundanţa fizică a routerelor midrange este realizată prin dublarea fizică a lor.

126. Routerele de această clasă pot fi utilizate ca echipamente de nivel *Core* ce au ca funcţie rutarea pachetelor din diferite medii de reţele LAN WAN şi realizarea serviciilor de acces.

127. Este posibilă realizarea redundanţei prin intermediul protocolului VRRP, ceea ce oferă majorarea calităţii serviciului. Destinat pentru asigurarea funcţionalităţii reţelelor clasei 3 de infrastructură.

128. Tabelul 11 sumează posibilităţile tehnice ale acestui tip de router:

Tabelul 11. Posibilităţile tehnice ale punctului de acces de clasa 4

Posibilităţi tehnice
Posibilitatea majorării fizice a capacităţii echipamentului
Varietate largă de conexiuni şi interfeţe WAN
Protocoale de rutare RIP, OSPF, BGP
Suport de VLAN (802.1q)
Performanţa limitată
Protocol de redundanţă VRRP
Suport de VPN protocol
Existenţa firewall-ului, configuraţie avansată
Posibilitatea de transformare a adreselor IP (NAT) inclusă

129. Punct de acces de clasa 5(engl. High-End) sunt clasificate ca cele mai performante tipuri de routere după productivitate.

130. Se manifestă prin multiplele interfeţe WAN, LAN, Ethernet, FastEthernet, GigabitEthernet (10/100/1000Mbps), utilizînd mediul de transport cupru şi/sau fibră-optică.

131. Prezenţa protocoalelor adiţionale în cadrul sistemei de operare, permite ca routerele High-End să ofere o gamă largă de funcţionalităţi tehnice. Apare posibilitatea de utilizare a protocolului SIP (VoIP), ce permite transmiterea datelor şi vocii simultan.

132. Este integrat protocolul de redundanţă şi lărgit spectrul de posibilităţi de redundare a interfeţelor, şasiului, blocurilor de alimentare, canalelor logice, fizice etc.

133. Routerele de această clasă pot fi utilizate ca echipamente de nivel *Core* ce au ca funcţie rutarea pachetelor din diferite medii de reţele LAN WAN MAN şi realizarea serviciilor de acces.

134. Tabelul 12 sumează posibilităţile tehnice ale acestui tip de router:

Tabelul 12. Posibilităţile tehnice ale punctului de acces de clasa 5

Posibilităţi tehnice
Posibilitatea majorării fizice a capacităţii echipamentului
Varietate largă de conexiuni şi interfeţe WAN
Protocoale de rutare RIP, OSPF, BGP
Suport de VLAN (802.1q)
Performanţa scalabilă
Protocol de redundanţă VRRP, GLBP etc.
Suport de VPN protocol
Existenţa firewall-ului, configuraţie avansată
Posibilitatea de transformare a adreselor IP (NAT) inclusă, DHCP

4.3. Arhitectura şi cerinţele faţă de infrastructura de servere şi servicii

135.În capitolul 4.3. sunt descrise procedurile administrative de realizare a serviciilor bazate pe Internet/Intranet şi prestarea acestora utilizatorului final. Acestea includ descrierea etapelor şi acţiunilor necesare pentru determinarea arhitecturii sistemelor, topologia reţelei, alocarea spaţiului de adresare, rutare şi înregistrarea numelor de domen, securitatea şi administrarea resurselor informaţionale.

4.3.1. Identificarea serviciilor

136. Spectrul de servicii fiind foarte larg se încadrează în următoarele categorii:

a) Serviciul Internet/Intranet Moldova Exchange (MD-IX);
b) Transfer de date (FTP, SFTP, SMB Sharing);
c) Prezenţă şi acces Internet (web-hosting, name-service DNS);
d) Servicii multimedia (VoIP, difuzare video on-line, video-conferinţă etc.).

137. Serviciile rulate în cadrul autorităţii includ în sine o multitudine de activităţi şi procese tehnologice ce necesită a fi executate în scop de menţinere şi asigurare a funcţionalităţii lui, şi anume:

a) *Proces tehnologic de distribuire a resurselor Internet*. Organizarea distribuţiei resursei Internet utilizatorilor acestui serviciu prin crearea listelor de acces şi setarea limitărilor de viteză pe bandă (IN/OUT), distribuţia fiind organizată static la nivel central pentru fiecare utilizator sau grup de utilizatori;

b) *Proces tehnologic de evidenţă şi monitoring a serviciului Internet*; Monitorizarea şi alarmă în caz de apariţie a problemelor, prin intermediul soluţiilor soft, hard;

c) *Proces tehnologic de redundanţă şi balansare a canalelor Internet existente*; Redundanţă, balansare prin intermediul organizării canalelor fizico-logice şi legăturilor de back-up dintre operatorii existenţi. Setarea parametrilor dinamici de automatizare a procesului de redundanţă;

d) *Proces tehnologic de rutare dinamică, statică şi distribuire a IP adreselor*; Organizarea IP adresării publice şi private. Organizarea rutării IP adreselor în extranet şi intranet, metodologia selectată fiind dinamică şi statică. Distribuirea şi evidenţa IP adreselor publice şi private în registrul de evidenţă.

e) *Proces tehnologic de organizare şi evidenţă a listelor de acces*; Crearea listelor de acces şi evidenţa lor orientate în asigurarea securităţii.

4.3.2. Resursele umane implicate în procesul de mentenanţă a serviciului

138. În capitolul 4.3.2. vor fi definite funcţiile şi atribuţiile personalului tehnic implicat în mentenanţă. Resursele implicate în procesul de mentenanţă, gestionare a serviciilor reprezintă un factor major în asigurarea funcţionalităţii lui. De nivelul cunoştinţelor posedate de către specialiştii implicaţi în acest proces rezultă buna funcţionare a serviciului.

139. La îndeplinirea procesului ciclului de viaţă al serviciului se determină următoarele roluri de bază:

a) *Managerul procesului de mentenanţă* - organizează procesele şi sub-procesele serviciului, creează infrastructura procesului şi îl adaptează la cerinţele respective înaintate;

b) *Administrator al serviciilor de reţea* - dirijează, gestionează şi modernizează serviciile ce ţin de funcţionalitatea mediului de transport comunicaţional, telecomunicaţional. În responsabilitatea sa intră funcţionalitatea echipamentelor de reţea;

c) *Administrator al serviciilor VoIP şi multimedia* este responsabil de asigurarea transportului de date tip voce şi video în cadrul sistemului, respectiv funcţionarea serviciilor bazate pe protocolul de iniţiere a sesiunilor SIP, H323 atît prin intermediul mediul de transport IP cît şi PSTN, ISDN. La fel şi asigurarea funcţionării sistemelor de on-line video streaming, sistemelor de videoconferinţă;

d) *Administrator al serviciilor web-hosting, DNS* - efectuează lucrări de mentenanţă a serviciului, prin crearea, modificarea sau eliminarea site-urilor clientului. Realizarea lucrărilor de instalare şi configurare a serviciilor se efectuează conform normelor tehnice de funcţionare a serviciului WEB-Hosting şi DNS. Înregistrarea zonelor DNS, configurarea web serverelor, aplicarea politicilor de

securitate se face conform cerinţelor utilizatorului reieşind din posibilităţile platformei. Administratorul realizează periodic lucrări de audit al serviciului, monitorizează în timp real funcţionalitatea şi efectuează actualizări ale platformei software. Securitatea serviciilor WEB-hosting şi DNS este asigurată de soluţii IPS, WAF la nivel centralizat şi în baza firewall-ului, modulelor integrate (suhosin, mod_security), listelor de acces realizate de administrator;

e) *Administratorull serviciului mail, antispam, antivirus* este responsabil de funcţionarea serverelor SMTP, POP/IMAP, WEBMAIL şi de autentificare. Instalarea şi configurarea iniţială a serviciului se efectuează conform normelor tehnice de funcţionare a serviciului email. Actualizarea filtrelor antispam şi antivirus se efectuează automatizat în fiecare zi. Analiza mesajelor false pozitive şi mesajelor spam nedetectate este efectuată de administrator pentru a putea realiza sau modifica politicile şi regulile de filtrare. Accounting-ul şi mentenanţa serviciului se efectuează prin instrumente web specializate. Realizarea lucrărilor de actualizare a softurilor este efectuată prin aplicarea modulelor integrate în cazul soluţiilor hardware-software complexe, în celelalte cazuri actualizarea se face manual. Monitorizarea serviciului este efectuată de către administrator online prin instrumente grafice, şi de notificare;

f) *Administrator al serviciului back-up şi storage* - controlează funcţia de rezervare şi restabilire a datelor de importanţă majoră pentru întreprindere. In funcţiile administratorului intră procedurile de efectuare a copiilor de rezervă; controlul copiilor de rezervă; stocarea şi păstrarea copiilor de rezervă; restabilirea deplină sau parţială a datelor, informaţiei şi aplicaţiilor. Administratorul utilizează utilitare specifice de monitorizare a proceselor de backup şi a resurselor hardware implicate, analizează regulat logurile de efectuare a backup-ului. Securitatea şi integritatea datelor rezervate reprezintă momente importante şi necesită atenţie deosebită din partea administratorului. De aceea, administratorul verifică periodic integritatea datelor rezervate şi locurile de accesare a acestora;

g) *Specialistul de gestionare a produselor software de mentenanţă.* Rolul de specialist de gestionare a produselor software de mentenanţă constă în urmărirea, analiza şi raportarea datelor statistice pentru evaluarea ulterioară a evenimentelor şi anomaliilor ce au avut loc, sau care pot avea loc. De asemenea, să aplice careva acţiuni în cazul mesajelor de alarmă, pentru a soluţiona problema. În funcţia sa, se indică şi actualizarea permanentă a obiectelor monitorizate cu lista echipamentului activ, astfel încît să existe posibilitatea colectării datelor maxime de statistică, alarmă etc., care ulterior vor avea un rol important în luarea deciziilor de activitate.

140. În scopul realizării procesului de mentenanţă, se admite completarea componenţei rolurilor, menţionate în prezenta reglementare tehnică, precum şi îndeplinirea a cîtorva roluri de către un singur executant.

4.3.3. Infrastructura de servere

141. Scopul acestei subclauze este de a descrie factorii ce trebuie luaţi în consideraţie la planificarea şi designul infrastructurii de servere. Informaţiile şi recomandările sunt destinate pentru implementarea efectivă a serviciului prin identificarea acţiunilor necesare la fiecare etapă a procesului de design al sistemului informaţional. Determinarea tipului de servere necesare pentru realizarea platformei

este efectuată ca rezultat al identificării serviciului prin numărul de utilizatori, amplasarea acestora, cost.

142. Pentru realizarea arhitecturii respective este necesar de a evalua diferite aspecte ale activităţii autorităţii, înainte de a alege echipamentul necesar pentru infrastructura serviciului.

143. Este necesar de a defini cerinţele în domeniile ce ţin de stocarea, administrarea, transmiterea şi procesarea datelor în cadrul reţelei după cum urmează:

a) Cerinţe faţă de soluţia însăşi;
b) Platforma software;
c) Date;
d) Utilizatori;
e) Cerinţe speciale;

144. Alegerea unei soluţii complexe pentru satisfacerea cerinţelor faţă de serviciul dezvoltat este condiţionată de cerinţele şi condiţiile iniţiale. Detalierea acestor cerinţe permite de a alege capacitatea şi volumul de echipamente necesar.

145. Platforma software aleasă este esenţială în estimarea costului, resurselor hardware şi performanţele serviciului.

146. Este necesar de a determina tehnologia de funcţionare a serviciului (Embedded, Java, .Net, Linux), sistemul de operare (Proprietar - Microsoft, sau Open Source – Linux,), platforma software a serviciului (IIS sau Apache pentru Web server, şi SQL Server sau Oracle ca sistem de gestiune a bazelor de date), tipul de licenţiere (Proprietară, GNU GPL etc.).

147. Tipul datelor cu care se operează în cadrul autorităţii pot fi de diferite categorii, cele mai dese ori acestea pot fi documente (Word, Excel, PDF, PPT, TXT), date multimedia (fotografii, video, audio), arhive (NRG, ISO, RAR, ZIP, DAT etc.), specifice aplicaţiilor utilizate (xml, cer, rtf).

148. Volumul acestor date este direct proporţional cu numărul de utilizatori şi implică resurse de procesare diferite în dependenţă de tip. Asigurarea securităţii datelor necesită resurse tehnologice suplimentare cum ar fi metode criptografice, software sau hardware de criptare etc.

149. Conform celor trei clase de sisteme informaţionale interne descrise la începutul acestui capitol, performanţele serverelor utilizate trebuie să asigure accesibilitatea serviciului pentru numărul respectiv de utilizatori.

150. În cazul serviciilor web, performanţa şi banda de acces a serverelor trebuie să ofere un nivel constant de stabilitate şi accesibilitate a resurselor.

151. Serviciile back-up şi storage necesită resurse de stocare a informaţiilor în dependenţă de necesităţile reale a autorităţii.

152. Performanţele unui sistem de gestiune a bazelor de date stau la baza măsurii eficacităţii modului în care resursele oferite de mediul unei baze de date sunt utilizate.

153. În continuare sunt definite roluri ale serverelor după cum urmează:

a) Serviciile de streaming - acces la serviciile de online-translare a întrunirilor, conferinţelor sau ale altor evenimente după solicitare necesită servere de stocare, echipament de encodare şi server web;

b) Serviciile de Web-hosting, servicii DNS - găzduirea paginilor web şi crearea/păstrarea/editarea zonelor DNS, necesită servere de stocare;

c) Serviciul de poşta electronică de nivel 1- schimbul de mesaje e-mail folosind metode de criptare preventivă a informaţiei, care garantează livrarea, autenticitatea mesajului electronic (identifică recipientul şi expeditorul) şi asigură principiul de non-repudiere;

d) Serviciul de poştă electronică de nivel 2 - schimbul de mesaje e-mail folosind tehnologii şi protocoale tradiţionale (POP3/SMTP) cu filtrarea anti-spam/phishing;

e) Serviciile de telefonie multifuncţională – VoIP şi multimedia (conferinţe telefonice, videoconferinţe, voicemail,);

f) Serviciul Directory Service oferă securizarea accesului la resurse, standardizarea numelor, un mediu unificat pentru servicii şi aplicaţii, precum şi managementul centralizat al utilizatorilor, calculatoarelor, imprimantelor şi aplicaţiilor. Topologia soluţiei de Directory Service implementată în cadrul autorităţii trebuie să fie foarte flexibilă, să asigure posibilitatea de extensie în viitor, atât la nivel de adăugare de noi site-uri, cât şi de adăugare de noi domenii. Organizarea ierarhică a site-urilor, a utilizatorilor şi a resurselor permite simplificarea managementului la nivelul întregii organizaţii.

154. Infrastructura de sistem este predestinată pentru asigurarea funcţionării fiabile şi fără întrerupere a componentelor platformei de sistem şi trebuie să asigure integrarea deplină a alimentării cu energie electrică, răcirii, dirijării şi mentenanţei.

155. Infrastructura de sistem include următoarele elemente:

a) alimentare continuă – sursa (sau blocul) de alimentare fără întrerupere de tipul ”on-line” şi protejat de la întreruperi în funcţionare după principiul ”N+1 Redundancy”

b) rack – dulap comunicaţional, pentru montarea utilajului activ şi sistemului de cabluri.

c) condiţionare – ventilatoare active (cu senzori de temperatură) şi mijloace de răcire (aparate de condiţionare).

d) dirijare – sistemul de control a mediului înconjurător şi a alimentării cu energie electrică.

156. Elementele infrastructurii descrise mai sus oferă siguranţă şi fiabilitate sistemului de comunicaţii. Lipsa unuia din elementele de mai sus reduce uptime-ul serviciului, stabilitatea şi securitatea acestuia.

157. Pentru lansarea serviciului sunt necesare următoarele acţiuni:

a) Pregătirea serverelor şi planificarea topologiei de reţea. Arhitectura şi topologia infrastructurii de servere trebuie să fie realizată în baza specificaţiilor OSI, în baza comunicaţiilor deja existente. Documentarea procesului de realizare a reţelei trebuie abilitat cu scheme, indexări, tabele, specificaţii la fiecare etapă.

b) Alocarea IP adreselor. Obţinerea spaţiului de IP adrese de la ISP care oferă servicii internet pentru serverele publice şi setarea acestora

c) Înregistrarea numelui de domen. Pentru organizarea accesului public la resursele informaţionale ale autorităţii este necesară înregistrarea numelui de domen (DNS) propriu în spaţiul de adrese global de nivelul superior (TLD - Top Level Domain, ex.: .com, .net, .org, .gov, ccTLDs - country codes Top Level Domain , ex.: .md, .ro, .ru) sau de nivele inferioare (ca subdomen al domenelor de nivel superior) în mod ierarhic (ex.: nume.gov.md, nume.host.md).

d) Delegarea domeniului în IN-ADDR.ARPA este necesară pentru transformarea IP adresei în nume de domeniu. IP adresa publică obţinută de la ISP trebuie să aibă înregistrată componenta opusă (inversă) în spaţiul de domene IN-ADDR (ex.: spaţiul de IP adresa 123.45.67.8 este reprezentată de 8.67.45.123.in-addr.arpa). Pentru serviciile publice, cum ar fi web-hosting, mail-hosting, este necesar ca adresa IP a serverului să aibă în corespundere componenta opusă în spaţiul de domene IN-ADDR, echivalentă cu numele de domeniu DNS.

e) Securitatea infrastructurii de servere. Asigurarea securităţii este definită prin politica de securitate la organizaţie privind regimul de acces fizic la echipament, regimul de parole. Accesul la resursele confidenţiale, informaţii senzitive trebuie realizat prin canale criptate (SSL) garantate prin autentificare viguroasă. ISP-ul trebuie să fie informat privind încercările frauduloase de autentificare.

f) Optimizarea şi managementul reţelei, trebuie efectuat în regim continuu, în regim automat şi transparent pentru utilizatorul final al serviciului. Managementul reţelei trebuie realizat prin instrumente standardizate de monitorizare, notificare şi raportare. În vigoarea utilităţilor oferite de platforma serviciului şi scalabilităţii infrastructurii realizate procesele de management al resurselor informaţionale pot atinge un nivel înalt de automatizare.

4.3.4. Cerinţe şi specificaţii funcţionale

1) Cerinţe faţă de serviciile prestate

158. Serviciile dezvoltate în cadrul autorităţii trebuie să corespundă următoarelor cerinţe:

a) Interoperabilitate - un serviciu trebuie sa ofere interfeţe pentru alte servicii şi aplicaţii.

b) Siguranţă . serviciul trebuie să fie viabil şi să funcţioneze stabil în orice moment de timp.

c) Integrabilitate - utilizarea aceloraşi platforme, sisteme de operare, şi limbaje de programare permite de a integra servicii complexe.

d) Securitate - protecţia platformei cu prevenirea accesului neautorizat la resursele informaţionale trebuie asigurată prin mijloace software, protocoale şi politici de securitate.

e) Scalabilitate şi extensibilitate - modularitatea soluţiilor alese pentru realizarea şi prestarea serviciului

f) Management şi acces.

2) Serviciile Web

159. Serviciile Web reprezintă o modalitate standardizată de distribuţie a resurselor informaţionale, care foloseşte Internetul şi tehnologiile fundamentale ce stau la baza acestei reţele. De asemenea, serviciile Web oferă posibilitatea de interconectare a numeroase aplicaţii disponibile pe diferite platforme şi domenii informaţionale.

160. Un serviciu Web trebuie:

a) Să fie uşor de extins şi refolosit în aplicaţii noi. Această cerinţă trebuie realizată prin adoptarea programării orientate obiect, cît şi prin folosirea

modularizării. Un serviciu poate fi văzut ca un modul, un obiect. Clientul nu trebuie să ştie că serverul se află pe altă maşină, ci doar să apeleze o metodă a serviciului ca şi cînd acesta este un obiect ce aparţine propriului program.

b) Să ofere interoperabilitate indiferent de platformă, sistem de operare şi limbaj de programare. Această problemă a fost rezolvată prin decizia de a folosi XML şi anume protocolul SOAP (Simple Object Access Protocol). În esenţă, acest protocol este bazat pe limbajul XML, avînd următoarele caracteristici funcţionale:

a. controlul transferului de pachete de date între furnizorul de servicii Web şi utilizatorul acestora, folosind protocolul HTTP (metode GET sau POST) pentru transferul pachetelor de date între server şi utilizator;

b. transferul parametrilor stabiliţi de utilizator şi specifici funcţiilor accesibile prin intermediul serviciului Web

c. returnarea rezultatelor rulării funcţiilor pe serverul care furnizează serviciul Web, aceste rezultate reprezintă seturi de date care au fost transpuse în fişiere XML.

c) Să fie transmis prin cît mai multe căi posibile prin reţea. Acest lucru este necesar deoarece multe autorităţi folosesc doar anumite protocoale de transport pentru o mai bună securitate. Cea mai bună soluţie este folosirea protocolului HTTP datorită posibilităţii de a nu fi blocat de firewall.

d) Să fie uşor de descris şi creat programe client. Utilizarea WSDL (Web Services Description Language). WSDL este bazat pe limbajul XML, avînd rolul de a informa potenţialii utilizatori ai serviciului Web în legătură cu elementele specifice acestuia. Astfel, prin intermediul WSDL se pot afla informaţii legate de funcţiile expuse de serviciul Web, precum şi cele legate de parametrii ce pot fi atribuiţi acestora.

e) Să fie accesibil pe Internet. Acest lucru trebuie realizat prin folosirea unor registre UDDI (Universal Discovery Description and Integration). UDDI are o funcţie asemănătoare motoarelor de căutare disponibile pe Web, permiţînd utilizatorilor căutarea serviciilor Web pentru necesităţile proprii. UDDI foloseşte informaţiile de descriere a serviciului Web stabilite prin intermediul limbajului WSDL, în scopul oferirii potenţialilor utilizatori a unei modalităţi eficiente de căutare, completată cu un set de informaţii de utilizare a serviciului Web.

3) Specificaţii funcţionale

161. Funcţionalitatea serviciilor web în reţeaua Intranet/Internet trebuie să fie asigurată în regim autonom continuu, fără intervenţia operatorilor şi administratorilor de sistem, cu condiţia respectării regulamentelor administrative corespunzătoare şi a altor regulamente:

1) Timpul total de întrerupere a funcţionării paginii web, legat de defecţiunile sistemului sau de efectuarea lucrărilor regulamentare de deservire, nu trebuie să depăşească 3-4 ore pe lună.

2) Aplicaţiile ce oferă servicii web trebuie să funcţioneze în reţeaua Internet constant, ţinînd cont de încărcătura de pînă la 50 HTTP- solicitări pe minut, totodată timpul mediu de recepţie a sistemului la solicitare nu trebuie să depăşească 1000 ms, iar timpul maxim - 4000 ms.

3) În timpul proiectării şi elaborării suportului software al aplicaţiilor web, trebuie luate în considerare sarcinile legate de asigurarea securităţii informaţionale, inclusiv:

a. protecţia informaţiei şi a suportului software atît împotriva accesului neautorizat la informaţia cu caracter confidenţial, cît şi împotriva modificării neautorizate a conţinutului obiectelor informaţionale şi a suportului software;

b. protecţia platformei tehnologice a aplicaţiilor web de la DDOS atacuri, "viruşi de computer", "viermi de reţea" etc.

4) Pentru asigurarea securităţii informaţionale a aplicaţiilor web, trebuie întreprinse măsuri de:

a. includere în componenţa structurală a resurselor web, în caz de necesitate, a mecanismelor de autentificare şi autorizare prin intermediul login-ului şi al parolei individuale;

b. asigurare a filtrării accesului la anumite resurse ale web prin adresele/subreţelele de acces, inclusiv Intranet/Internet ("restrict la IP");

c. utilizare pentru întreg sistem a produselor soft testate şi recunoscute pe piaţă, cu toate pachetele de reînnoire recomandate de producători;

d. utilizare a configurărilor protejate ale suportului soft, indicate din timp, create în perioada instalării;

e. utilizare a procedurilor tehnologice de elaborare şi documentare, care trebuie să minimalizeze riscurile creării breşelor incidentale în sistemul de securitate în urma erorilor din codul de program elaborat;

f. monitorizare continuă a ameninţărilor şi riscurilor orientate spre securitatea materialelor publicaţiilor specializate şi resurselor informaţionale;

g. efectuarea copiilor de rezervă, permanente şi neîntrerupte, a modulelor soft informaţionale ale resurselor informaţionale de importanţă cu utilizarea dispozitivelor speciale tehnico-tehnologice şi complexelor software.

162. Proiectarea arhitecturii software pentru o producere sistematică a sistemelor este dificilă. Produsele sistematice trebuie să fie atît flexibile, cît şi cu o durata de viaţă mare. Mai mult, acestea trebuie să susţină o mulţime de cerinţe care sunt cunoscute numai la nivelul domeniului larg – detaliile fiind necognoscibile pînă la crearea produsului actual.

163. Stadiile iniţiale ale proiectării arhitecturii reprezintă punctele în care se iau cele mai importante decizii relativ la arhitectură. Există (este cazul cel mai frecvent) arhitecturi care pot fi foarte greu corectate, în cazul în care aceste decizii de fundamentare sunt eronate.

V. Cerinţe faţă de conţinutul documentaţiei tehnice şi documente de conformitate

5.1. Dispoziţii generale.

164. Cerinţele faţă de conţinutul documentaţiei tehnice, elaborate în momentul proiectării infrastructurii interne a autorităţilor administraţiei publice au fost elaborate în conformitate cu prevederile standarduluiSMV ISO/IEC 11801:2009 „Tehnologia informaţiei. Cablare generică pentru localurile utilizatorilor"şi SM SR EN ISO „Sisteme de management al calităţii. Cerinţe".

165. Conţinutul documentaţiei este comun pentru proiectele tehnice elaborate în oricare dintre scopurile: dezvoltare, extindere, modernizare, optimizare, etc. a infrastructurii interne a autorităţilor administraţiei publice. Este permisă atît introducerea capitolelor noi în documentaţie, eliminarea, cît şi unificarea acestora, în dependenţă de necesitate.

166. În cazul în care este necesar, documentele se reunesc în cărţi, care sunt marcate corespunzător.

5.2. Documentaţia tehnică

167. Documentaţia tehnică (proiectul tehnic de creare a reţelelor locale, proiectul tehnic de prestare a serviciilor, proiectul tehnic de creare a liniilor de cablu optic) trebuie să conţină următoarele capitole:

a) Conţinutul proiectului tehnic – este realizată în vederea indicării numărului de desene tehnice şi a specificaţiei acestora, inclusiv cuprinsul.

b) Informaţii generale – indică scopul şi obiectivele proiectului tehnic. De asemenea, vor fi incluse informaţii teoretice cu privire la tehnologiile ce vor fi utilizate în vederea atingerii scopului şi obiectivelor.

c) Date tehnice şi constructive ale cablurilor utilizate – descrie tipul cablului utilizat (optic sau torsadat), structura şi proprietăţile acestuia, unele caracteristici fizice.

d) Etapele efectuării lucrărilor – sistematizează toate lucrările în cîteva etape generale, în vederea indicării ordinii efectuării de lucrări şi sintetizării principalelor acţiuni şi măsuri care trebuie întreprinse.

e) Schema fizică şi logică – indică traseul de pozare a cablului (torsadat, optic) sau cartograma, modalitatea de amplasare a echipamentelor active şi pasive, modalitatea de conectare a echipamentelor terminale sau intermediare la reţea, reflectarea distanţelor şi unităţilor de măsură, reflectarea principiului de funcţionare.

f) Descrierea tehnică a proiectului – indică tipul serviciului prestat, modul de conectare şi rutare, calitatea serviciului, statistica şi monitorizarea şi securitatea informaţiei.

g) Specificarea materialelor şi lucrărilor – indicarea consecutivă a tututor bunurilor materiale ce vor utilizate şi lucrărilor necesare de a efectua în vederea bunei funcţionări a sistemului proiectat.

h) Evaluarea financiară – reflectă costul lucrărilor efectuate, a echipamentelor şi bunurilor materiale, care necesită a fi utilizate la implementarea proiectului, costul total.

VI. Principiile de asigurare a securităţii infrastructurii informaţionale

168. Proiectarea, crearea şi operarea infrastructurii interne se va baza pe următoarele principii de securitate:

a) Separarea funcţionalităţilor. Funcţionalitatea mecanismelor şi metodelor folosite în asigurarea securităţii resurselor informaţionale interne trebuie să fie divizate funcţional pe nivelele OSI.

b) Principiul separării responsabilităţilor. Pentru efectuarea unei protecţii informaţionale eficace, în cadrul autorităţii publice va fi desemnat personal tehnic,

responsabil de crearea şi administrarea sistemului de securitate, iar la nivel de aplicaţii, măsurile de securitate trebuie să ofere divizare funcţională granulară a subcomponentelor şi atributelor de acces la aceste subcomponente.

c) Pincipiul prezumţiei agresivităţii traficului extern. Implicit, tot traficul care se originează în reţele externe autorităţii publice va fi considerat ca trafic potenţial primejdios, care poate conţine în sine date menite să exploateze vulnerabilităţi ce ţin de confidenţialitatea, integritatea şi accesibilitatea resurselor informaţionale interne.

d) Principiul omogenităţiimecanismelor şi metodelor de protecţie. În crearea sistemului complex de asigurare a securităţii resurselor informaţionale vor fi utilizate metode şi mecanisme omogene din punctul de vedere al asigurării şi managementului protecţiei informaţiei.

e) Principiul filtrării obligatorii a traficului. Tot traficul destinat serverelor de aplicaţii sau serverelor interne de servicii va fi direcţionat spre/prin sistemul de protecţie şi ulterior filtrat, scăzînd posibilitatea de executare a unui cod de program primejdios.

f) Reducerea riscurilor pînă la un nivel rezonabil. Nivelele de aplicare a mecanismelor de protecţie trebuie să corespundă la nivelul de posibilitate de exploatare a unei vulnerabilităţi a sistemului protejat. Astfel protecţia trebuie să fie una modulară, distribuită pe nivelele 2-7 OSI, însă instalarea şi aplicarea mecanismelor de securitate trebuie să fie una transparentă, fără modificări majore în funcţionalitatea resurselor informaţionale interne.

g) Principiul privilegiilor minimale. Componentele infrastructurii informaţionale şi utilizatorii resurselor interne trebuie să poată accesa doar informaţia şi serviciile necesare pentru efectuarea funcţionalităţii proprii.

h) Principiul consolidării mijloacelor software. Sistemele de securitate vor efectua consolidarea din punctul de vedere al asigurării securităţii sistemelor de operare a serverelor de aplicaţii şi echipamentului telecomunicaţional implicat în crearea resurselor informaţionale interne ale autorităţii publice.

i) Principiul integrării transparente. Măsurile de protecţie vor fi instalate transparent pentru serverele de aplicaţii şi utilizatori finali, iar căderea sau ieşirea din funcţiune a sistemelor de protecţie a resurselor informaţionale nu trebuie să afecteze accesibilitatea resurselor informaţionale interne.

j) Principiul existenţei politicilor de securitate internă. În cadrul autorităţii publice vor fi create şi aplicate politici de securitate specializate ce vor reglementa procedura de utilizare şi acces la resursele informaţionale interne şi externe. Politicile de securitate vor fi create pentru orice serviciu sau server de importanţă majoră şi necesar pentru buna funcţionarea a infrastructurii informaţionale interne.

k) Principiul consistenţei politicilor de securitate. Politicile de securitate aplicate în cadrul autorităţii publice vor reglementa procedurile de asigurare a securităţii informaţionale pentru tot ciclul de viaţă a unei resurse informaţionale şi pentru infrastructura informaţională internă.

l) Principiul organizării auditului intern. Pentru a evalua eficienţa politicilor şi mecanismelor de securitate a resurselor informaţionale interne va fi efectuat auditul intern reglementat şi planificat. Auditul va putea fi efectuat prin forţe proprii sau prin instituţii terţe competente şi abilitate, dar cu specificarea clară a

obiectivelor auditului, procedurii de audit, precum şi a rezultatelor aşteptate. Evaluarea va fi efectuată în baza rezultatului auditului care va determina criteriile de conformitate şi actualitate, specifice pentru obiectul audiat.

m) Principiul protecţiei adecvate. Realizarea sistemului de securitate va tinde nu spre realizarea securităţii maxime, ci utilităţii în raport cost/risc acceptabil.

n) Principiul verigii cele mai slabe. Este principiul care determină securitatea sistemului informaţional în întregime.

VII.Riscuri specifice infrastructurii interne a autorităţilor administraţiei publice

7.1.Riscuri în urma calamităţilor naturale

7.1.1 Distrugerea fizică a infrastructurii

169. Infrastructura internă a autorităţilor administraţiei publice, ca şi orice altă infrastructură telecomunicaţională este supusă riscului distrugerii fizice în urma calamităţilor naturale.

170. Cauzele naturale ce pot duce la deteriorarea infrastructurii interne pot fi:

a) Inundaţii;
b) Vînturi cu viteze înalte;
c) Incendii;
d) Cutremure de pămînt;
e) Alunecări de sol, etc.

7.1.2 Întreruperi în suportul infrastructurii

171. Suportul infrastructurii interne a autorităţilor administraţiei publice este asigurat de:

a) reţelele de curent electric;
b) sistema de climatizare;
c) sistema de asigurare cu energie electrică de rezervă (generator).

172. Fiind mai dese decît distrugerea fizică a infrastructurii, întreruperile în suport tind a fi la fel de dăunătoare, acest fapt explicîndu-se prin necesitatea în energie electrică şi în climatizare a echipamentului telecomunicaţional. Din motiv că infrastructura este una modernă este supusă, în cazul calamităţilor, unei probabilităţi mai mici de apariţie a riscului de distrugere. Totodată, reţelele electrice sunt vechi şi prezintă o probabilitate ridicată de defecţiuni în cazul calamităţilor, ceea ce se răsfrînge în mod direct asupra infrastructurii.

173. Sistema de climatizare, în caz de deteriorare, poate duce la funcţionarea incorectă a echipamentului telecomunicaţional sau la incapacitatea totală de funcţionare a acestuia. Riscul deteriorării sistemei de climatizare are un impact mai mic asupra infrasctructurii, însă este necesar de a ţine cont de existenţa acestuia.

174. De obicei, pentru a micşora probabilitatea apariţiei riscului de întrerupere a asigurării infrastructurii cu energie electrică, echipamentul este conectat la o sursă de energie electrică de rezervă. Apariţia riscului deteriorării acestui sistem este determinată de deteriorarea reţelei de asigurare cu energie electrică de bază.

7.1.3 Congestia/supraîncărcarea infrastructurii

175. Una dintre urmările calamităţilor naturale este creşterea cererii populaţiei în sursele de informare. Aceasta duce la creşterea traficului în reţeaua autorităţilor administraţiei publice, care poate avea drept urmare imposibilitatea reţelei de a procesa cantitatea sporită de cereri.

7.1.4 Reabilitarea/reparaţia infrastructurii

176. Activitatea de reabilitare/reparaţie a infrastructurii autorităţilor administraţiei publice include 4 faze:

a. răspuns de urgenţă;
b. restaurare şi reparaţie;
c. resconstrucţia celor distruse pentru înlocuire funcţională;
d. reconstrucţia pentru dezvoltare.

177. În general, durata fazelor succesive creşte cu un factor de 10. În timp ce răspunsurile de urgenţă pot dura de la cîteva zile, la cîteva săptămîni, reconstrucţia pentru dezvoltare durează cîţiva ani.

178. Răspunsurile de urgenţă ţin de înlocuirea cîtorva echipamente, defectarea cărora a dus la funcţionarea incorectă sau întreruperea funcţionării reţelei autorităţilor administraţiei publice.

179. Restaurarea şi reparaţia este efectuată în cazul distrugerii uneia sau cîtorva linii de telecomunicaţii. În dependenţă de numărul liniilor deteriorate, restaurarea poate dura pînă la cîteva săptămîni.

180. Reconstrucţia celor distruse este efectuată atunci cînd linia de telecomunicaţii nu mai poate fi reparată.

181. Reconstrucţia pentru dezvoltare este efectuată în cazul cînd o porţiune întreagă a reţelei (linii de telecomunicaţii şi echipament) este distrusă. Acest caz este cel mai dificil de realizat, deoarece necesită mijloace financiare importante şi o durată îndelungată de timp.

7.1.5 Reducerea probabilităţii apariţiei riscului

182. Reducerea probabilităţii apariţiei riscului în urma calamităţilor naturale specifice infrastructurii autorităţilor administraţiei publice se realizează prin intermediul următoarelor măsuri:

a. construirea liniilor comunicaţionale conform standardelor în vigoare, aplicînd măsuri de rezisenţă în cazul calamităţilor naturale;
b. asigurarea echipamentelor cu sursă de energie electrică de rezervă, în vederea menţinerea funcţionalităţii reţelei în cazul defectării sursei de energie electrică de bază;
c. mărirea în permanenţă a redundanţei reţelei telecomunicaţionale cu scopul de a asigura funcţionalitatea în cazul creşterii bruşte a volumului de trafic.

7.2. Riscuri cauzate de factorul uman

7.2.1 Introducerea sau declanşarea vulnerabilităţilor

183. Introducerea vulnerabilităţilor de către factorul uman este realizată în momentul proiectării sau montării liniei telecomunicaţionale sau a echipamentului.

184. Proiectarea incorectă sau insuficientă, fără luarea în calcul a tuturor elementelor duce la reducerea termenului de exploatare sau la creşterea riscului de funcţionalitate incorectă.

7.2.2 Exploatarea vulnerabilităţilor de către factorul uman

185. Riscurile ce ţin de exploatarea vulnerabilităţile sunt următoarele:

a) riscul de spam - procesul de expediere a mesajelor electronice nesolicitate, de cele mai multe ori cu caracter comercial, de publicitate pentru produse şi servicii dubioase. Spam-ul se distinge prin caracterul agresiv, repetat şi prin privarea de dreptul la opţiune;

b) riscul de phishing - formă de activitate infracţională care constă în obţinerea unor date confidenţiale, cum ar fi date de acces pentru aplicaţii de tip bancar, aplicaţii de comerţ electronic sau informaţii referitoare la carduri de credit, folosind tehnici de manipulare a datelor identităţii unei persoane sau a unei instituţii;

c) accesul neautorizat - include orice tip de acces neautorizat (calitativ) sau extra-contractual (cantitativ). Drept exemplu, poate fi menţionat accesul neautorizat al unei persoane la reţeaua internă a unei întreprinderi, autorităţi, un serviciu non-contractual, etc;

d) spionarea infrastructurală - colectarea, utilizarea, publicarea informaţiei cu privire la infrastructura autorităţilor administraţiei publice sunt riscuri importante, deoarece în baza acestora pot fi bine gîndite atacurile asupra reţelei. Informaţia cu privire la infrastructură este o valoare a deţinătorului;

e) vandalism fizic - deteriorarea intenţionată sau neintenţionată a liniei telecomunicaţionale sau echipamentului. Proiectarea şi montarea incorectă duce la creşterea probabilităţii şi posibilităţii de acces neautorizat, care are drept urmare apariţia riscului de vandalism fizic;

f) terorism şi războaie - distrugerea unei poţiuni a infrastructurii autorităţilor administraţiei publice, cauzată în mod intenţionat sau neintenţionat în moment de forţă majoră de către factorul uman.

7.2.3. Creşterea complexităţii interdependenţei şi unificarea comunicaţiilor

186. În timp ce creşte complexitatea, mai ales la reţelele de management, dependenţa de serviciile telecomunicaţionale vor creşte de asemenea. Astfel, o problemă relativ mică se poate transforma peste cîtva timp în una de proporţii. Cauza problemei este mai puţin importantă decît rezistenţa reţelei.

Capitolul VIII. Politica de acces la resursele informaţionale externe

187. Scopul politicii de acces la resursele informaţionale externe este de a crea o fundaţie pe care vor fi bazate toate activităţile legate de asigurarea securităţii informaţiei, în condiţiile existenţei unor conexiuni externe.

188. Pentru a asigura eficienţa acestei politici, ea trebuie să fie aprobată la nivel de conducători ai autorităţii publice şi conducătorilor autorităţilor din extranet.

189. Politica de securitate trebuie să fie tehnologic actualizată, să se dezvolte în ritm cu tehnologiile informaţionale noi. Cu alte cuvinte, odată cu dezvoltarea

metodelor tehnologice de acces la resursele informaţionale trebuie să fie actualizate politicile de securitate.

190. Politica de securitate a autorităţii publice trebuie să fie una balansată din punct de vedere a necesităţilor autorităţii publice şi tehnologiilor de asigurare a securităţii informaţionale existente. Deoarece ambele sînt în continuă dezvoltare, politica de securitate trebuie să fie actuală şi adecvată.

191. Politica de acces la resursele informaţionale externe, sau oferirea accesului la anumite resurse informaţionale interne din sisteme informaţionale externe se va baza pe următoarele consideraţii:

a)Reţeaua extranet va fi divizată securizat de către reţeaua intranet a autorităţii publice;

b) Conexiunile protejate vor fi create în baza conexiunilor VPN sau în baza liniilor dedicate;

c)Utilizatorii din reţeaua extranet vor fi unic identificaţi prin tehnici adecvate de autentificare şi autorizare;

d) Personalul responsabil pentru asigurarea conexiunilor din /spre extranet, va genera raporturi lunare referitor la numărul de accesări pentru a verifica utilizarea corectă a resurselor informaţionale;

e)Un sistem de monitoring în timp real, audit, alertare trebuie să fie instalat pentru a detecta, anihila şi raporta încercările frauduloase sau abuzive de acces a resurselor informaţionale interne sau externe.

192. Apriori conectării unui segment extranet, trebuie să fie efectuat un audit al vulnerabilităţilor aplicaţiilor şi tuturor elementelor infrastructurii interne şi externe. De preferinţă este auditul şi crearea politicii de risk-management de către o entitate terţă competentă şi autorizată.

193. Totodată va fi efectuată revizuirea politicii de securitate în contextul modificărilor apărute. Revizuirea şi modificările după necesitate a politicilor de securitate vor fi regulate şi cu caracter exhaustiv şi după domeniul de aplicare se vor răsfrînge asupra reţelei intranet şi reţelei extranet.

194. Aplicaţiile extranet vor oferi accesul la date şi informaţie contra unui set predefinit de atribute de autentificare şi doar unui număr concret de utilizatori.

195. Pentru un design eficient de autentificare la accesarea unei resurse informaţionale externe/interne, se vor lua în consideraţie principiile de asigurare a securităţii infrastructurii informaţionale cum ar fi separarea responsabilităţilor, principiul privilegiilor minimale, etc.

196. Aplicarea practică a principiului separării responsabilităţilor constă în divizarea anumitor funcţii de bază a unui sistem (accesul direct la DBMS, update la java applet-e, patch la SO, instalarea software) între personalul tehnic competent.

197. Principiul privilegiilor minimale în aplicarea practică constă în restricţionarea utilizatorului (actualizări DBMS, sau administrarea de la distanţă) sau restricţionarea tipului de acces (citire, înscriere, executare, ştergere) la nivelul minim necesar pentru a-şi efectua activităţile zilnice.

8.1. Segmentarea reţelei telecomunicaţionale

198. Pentru asigurarea unei divizări eficiente a reţelei extranet de reţeaua intranet vor fi utilizate soluţii hardware/software specializate.

199. Separarea reţelelor intranet de extranet va asigura un nivel adiţional de securitate a infrastructurii informaţionale interne.

200. Combinarea tehnicilor de firewall şi IPS pentru detectarea activităţilor primejdioase şi abuzive trebuie să fie cît mai strictă şi să asigure un control adecvat asupra traficului de reţea.

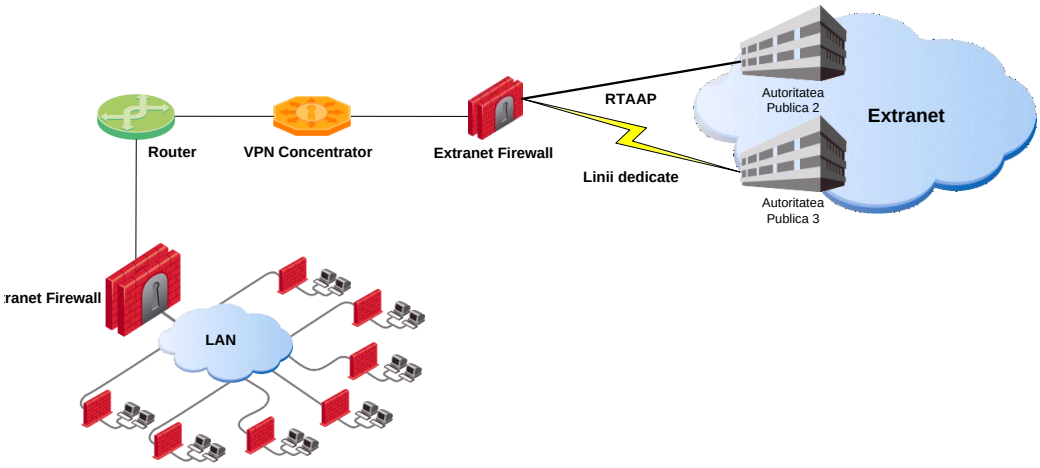

Fig.1. Topologia conexiunilor extranet

201. Fiecare segment de reţea trebuie să fie protejat, utilizînd un echipament dedicat, sau un subsistem de soluţie de securitate virtualizată, totodată nu va exista conexiune directă dintre segmentul extranet şi segmentul intranet.

202. Utilizatorii extranet vor avea acces către resursele intranet în baza canalelor VPN sau a liniilor dedicate.

203. Nu va fi permisa comunicarea între VPN clienţi în configuraţii „*hub and spoke"* cu VPN concentratorul ca *hub* şi VPN clienţi ca *spoke* .

204. Politicile de securitate a organizaţiei vor asigura interdicţiile de rutare între doi utilizatori VPN.

8.2. Autentificarea şi autorizarea extranet

205. Gestionarea utilizatorilor trebuie să ofere posibilitatea de a fixa anumite funcţii critice de utilizator. În acest context politica de securitate a autorităţii trebuie să definească responsabilitatea utilizatorului în termeni de răspundere şi consecinţe pentru activităţile sale.

206. Pentru conexiunile din extranet la nivel de reţea, aplicarea politicilor de autentificare a utilizatorului este sarcina personalului responsabil autorităţii extranet, din aceste considerente autentificarea utilizatorilor va fi efectuată la nivel de aplicaţii din partea intranet a autorităţii care prestează serviciul.

207. În condiţiile în care la accesarea resurselor externe nu se operează cu informaţie ce poate fi clasificată ca informaţie ce ţine de resursele informaţionale de bază, resurse informaţionale cu caracter secret sau confidenţial, se permite utilizarea mecanismelor de *proxy-authentification,*sau mecanismelor de *SSO* (single sign-on). Ca exemple de *proxy-authentification* pot servi *cross-certificarea* utilizînd

certificatele digitale, RADIUS/TACACS+ servere, sau un server partajat de Directory Service.

208. Autentificarea echipamentelor include concentratoarele VPN şi serverele ce utilizează infrastructura de PKI (Web Server cu suport de SSL, Directory Service Server, etc). Concentratoarele VPN pentru autentificarea utilizatorilor în condiţiile de accesare a informaţiei ce nu se clasifică ca informaţie de importanţă statală pot fi folosiţi la autentificarea în baza unei parole (*preshared key*).

209. Asigurînd accesul la reţeaua intranet prin intermediul autentificării, este obligaţiunea serverului de aplicaţie de a asigura autentificarea şi autorizarea ulterioară pentru resursele informaţionale situate în infrastructura informaţională internă. Autorizarea trebuie să fie una granulară, cu definirea drepturilor şi nivelelor utilizatorilor autentificaţi.

8.3. Acorduri de interconectare

210. Asigurarea accesului la resursele informaţionale interne pentru utilizatorii din extranet poate cauza anumite probleme de răspundere. Din punct de vedere al asigurării securităţii informaţionale acordurile de interconectare, de cele mai dese ori, nu sunt capabile să estimeze măsura de expunere a riscului infrastructurii informaţionale interne.

211. Cea mai eficientă metodă de asigurare a securităţii constă în crearea unei arhitecturi de asigurare a securităţii derivate din politica de securitate a autorităţii. Astfel problema asigurării securităţii în cadrul autorităţii este acoperită de politica de securitate a autorităţii, care nu se extinde asupra sistemelor informaţionale externe.

212. Orice autoritate ce va oferi servicii de interconexiune cu utilizatori din extranet va crea un acord de interconectare separat, scopul căruia va fi specificarea condiţiilor şi termenilor de bază pentru asigurarea schimbului de date reciproc într-o manieră securizată.

Capitolul IX
Dispoziţii finale

	lasa 1	lasa 1 e xtensii tip 1	lasa 1 e xtensii tip 1	lasa 1 e xtensii tip 2	lasa 2	lasa 2 e xtensii tip 1	lasa 2 e xtensii tip 2	lasa 2 e xtensii tip 3	lasa 3	lasa 3 e xtensii tip 1	lasa 3 e xtensii tip 2	lasa 3 e xtensii tip 3
Infrastructura de reţea internă												
Switch		C	C	C		C	C	C		C	C	C
Manged switch		F		F		F		F		F		F
MDF/IDF		F		F		F		F		F		F
Infrastructura de acces Internet												
Router		F	R	F		F	F	F		F	F	F
Wi-Fi Router		F	R	F		F	F	F		F	F	F
Servere de acces		C	R	F		C	F	F		C	F	F
IDP		F	R	F		F	F	F		F	F	F
Firewall		F	R	F		F	F	F		F	F	F
Proxy Server		C	R	C		F	C	C		C	C	F
Infrastructura de servere şi servicii												
Directory		C	R	F		F	F	F		F	F	F

Service												
DHCP/BOOTP		O	O	O		O	O	O		O	O	O
DNS/WINS		O	O	O		O	O	O		O	O	O
MAIL		O	O	O		O	O	O		O	O	O
Antispam		O	R	O		R	R	O		O	R	R
Aplication Server		O	O	O		O	O	O		O	O	O
Terminal Server		O	O	O		O	O	O		O	O	O
FTP/File transfer Server		O	O	O		O	O	O		O	O	O
RADIUS/TACACS+ Server		O	R	R		O	R	R		O	R	R
Antivirus/Personal Firewall/IPS Server		R	R	R		R	R	R		R	R	R
Antivirus/Personal Firewall/IPS Agent		R	R	R		R	R	R		R	R	R
DB Server		O	O	O		O	O	O		O	O	O
Collaboration Server		R	R	R		R	R	R		R	R	R
Logging Server		O	O	R		O	R	R		O	R	R
WEB Server		O	O	O		O	O	O		O	O	O
Infrastructura de remote acces şi interconexiune cu alte SI externe												
VPN Server		O	R	R		O	R	R		O	R	R
Dial-in Server		O	O	O		O	O	O		O	O	O
Linii dedicate		O	O	O		O	O	O		O	O	O
Router Edge		O	R	R		O	R	R		O	R	R
Infrastructura Data-Centru												
MDF/IDF		R	R	R		R	R	R		R	R	R
Sistem de alertă şi monitoring		R	R	R		R	R	R		R	R	R
Sistem antiincediar		O	R	O		R	R	O		O	R	R
Dulapuri Telecomunicaţionale		R	R	R		R	R	R		R	R	R
Sistem de asigurare cu energia electrică continuă		R	R	R		R	R	R		R	R	R

Opţiuni	***Descriere***
O	Elemente a infrastucturii cu caracter obligatoriu
R	Elemente a infrastucturii cu caracter recomandat