**MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică şi Microelectronică**

**Departamentul Ingineria Software și Automatică**

**Programul de studii: Securitatea informațională**

**Sistem integrat pentru interceptarea și analiza traficului de rețea**

**Practica de licență**

|  |  |  |
| --- | --- | --- |
| **Student(ă):** | **\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Chirița Stanislav, SI-211** |
| **Coordonator întreprindere:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Jovmir Cristina, Head of CERT Gov** |
| **Coordonator de licență:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Masiutin Maxim, asist.univ.** |
| **Coordonator universitate:** | **\_\_\_\_\_\_\_\_\_\_\_\_\_** | **Bulai Rodica, lector universitar** |

**Chişinău, 2024**

**CUPRINS**

[ABREVIERI 3](#_Toc189658395)

[INTRODUCERE 4](#_Toc189658396)

[1 ANALIZA DOMENIULUI DE STUDIU 5](#_Toc189658397)

[1.1 Importanța temei 5](#_Toc189658398)

[1.2 Sisteme similare cu proiectul realizat 5](#_Toc189658399)

[1.3 Scopul, obiectivele și cerințele sistemului 6](#_Toc189658400)

[2 MODELAREA ȘI PROIECTAREA SISTEMUL INFORMATIC 8](#_Toc189658401)

[2.1 Descrierea comportamentală a sistemului 8](#_Toc189658402)

[2.1.1 Imaginea generală asupra sistemului 8](#_Toc189658403)

[2.1.2 Modelarea vizuală a fluxurilor 8](#_Toc189658404)

[2.1.3 Stările de tranzacție a sistemului 8](#_Toc189658405)

[2.1.4 Descrierea scenariilor de utilizare a aplicaţiei 8](#_Toc189658406)

[2.1.5 Fluxurile de mesaje şi legăturile dintre componentele sistemului 8](#_Toc189658407)

[2.2 Descrierea structurală a sistemului 8](#_Toc189658408)

[2.2.1 Descrierea structurii statice a sistemului 8](#_Toc189658409)

[2.2.2 Relatiile de dependență între componentele sistemului 8](#_Toc189658410)

[2.2.3 Modelarea echipamentelor mediului de implementare 8](#_Toc189658411)

[3 REALIZAREA SISTEMULUI 9](#_Toc189658412)

[CONCLUZII 10](#_Toc189658413)

[BIBLIOGRAFIE 11](#_Toc189658414)

[ANEXA A 12](#_Toc189658415)

# ABREVIERI

**IPS (Intrusion Prevention System)** – Sistem de prevenire a intruziunilor

**IDS (Intrusion Detection System)** – Sistem de detecție a intruziunilor

**SIEM (Security Information and Event Management)** – Soluție integrată pentru gestionarea informațiilor și evenimentelor de securitate

…

# INTRODUCERE

Practica desfășurată în cadrul **Serviciului Tehnologia Informației și Securitate Cibernetică (STISC)** a avut ca obiectiv principal aprofundarea cunoștințelor teoretice și aplicarea acestora într-un mediu real de lucru, în domeniul securității cibernetice și al analizei traficului de rețea. Activitatea s-a desfășurat pe parcursul perioadei **03.02.2025 – 28.03.2025**, timp în care am avut ocazia să mă familiarizez cu tehnologiile și metodele utilizate pentru interceptarea și analiza traficului de rețea, un domeniu esențial pentru asigurarea securității informaționale la nivel național.

Scopul principal al practicii a fost dezvoltarea unui **sistem integrat pentru interceptarea și analiza traficului de rețea**, utilizând tehnici avansate de captare și interpretare a pachetelor de date. Prin această experiență, am urmărit să înțeleg mai bine structura și vulnerabilitățile rețelelor, metodele de detecție a amenințărilor și utilizarea instrumentelor specifice pentru monitorizarea traficului. Importanța acestui subiect este majoră, având în vedere creșterea constantă a atacurilor cibernetice și necesitatea implementării unor soluții eficiente de protecție în infrastructurile critice.

# 1 ANALIZA DOMENIULUI DE STUDIU

Analiza traficului de rețea are un rol important în securitatea cibernetică, permițând identificarea atacurilor și optimizarea performanței rețelelor. În cadrul practicii desfășurate la **Serviciul Tehnologia Informației și Securitate Cibernetică (STISC)**, am utilizat instrumente specializate pentru interceptarea și analiza pachetelor de date, având ca scop implementarea unui sistem integrat de monitorizare a traficului.

Am folosit tehnologii precum **Wireshark, tcpdump, Zeek și Suricata**, fiecare având roluri specifice în captarea și interpretarea traficului de rețea. Aceste instrumente au fost utilizate pentru a analiza avantajele și limitările fiecăruia, în scopul dezvoltării unei soluții proprii optimizate. Testele efectuate au permis identificarea punctelor forte și a aspectelor care necesită îmbunătățiri, oferind o bază solidă pentru crearea unui instrument personalizat, capabil să răspundă cerințelor specifice de securitate și monitorizare a rețelei.

Rezultatele au demonstrat eficiența unei soluții automatizate pentru detectarea amenințărilor. Optimizările viitoare pot include integrarea algoritmilor de **machine learning** pentru îmbunătățirea detecției anomaliilor. Această practică a oferit o înțelegere practică asupra monitorizării traficului și a metodelor de protecție a rețelelor informatice.

1.1 Importanța temei

Implementarea unui sistem integrat pentru interceptarea și analiza traficului de rețea contribuie la identificarea anomaliilor și la reacția rapidă împotriva incidentelor de securitate. Prin monitorizarea fluxului de date, se poate determina comportamentul anormal al utilizatorilor sau dispozitivelor dintr-o rețea, prevenind astfel compromiterea infrastructurii IT. De asemenea, analiza traficului permite optimizarea performanței rețelelor și asigurarea respectării politicilor de securitate și a reglementărilor legale.

Prin această lucrare, se urmărește testarea și compararea unor instrumente existente de analiză a traficului, identificarea punctelor lor slabe și dezvoltarea unei soluții îmbunătățite, capabile să ofere o detecție mai rapidă și mai precisă a amenințărilor. Astfel, cercetarea contribuie la îmbunătățirea metodelor de protecție a rețelelor informatice și la dezvoltarea unor tehnologii mai eficiente în domeniul securității cibernetice.

* 1. Sisteme similare cu proiectul realizat

În domeniul securității cibernetice, există numeroase sisteme dezvoltate pentru interceptarea și analiza traficului de rețea. Acestea sunt utilizate atât pentru monitorizare pasivă, cât și pentru detecția activă a amenințărilor. Printre cele mai relevante soluții similare cu proiectul realizat se numără:

**Wireshark** – Unul dintre cele mai populare instrumente de analiză a traficului de rețea. Permite captarea și inspecția detaliată a pachetelor, fiind utilizat atât pentru depanare, cât și pentru identificarea vulnerabilităților. Totuși, Wireshark necesită o analiză manuală intensă, ceea ce poate fi un dezavantaj pentru detecția rapidă a atacurilor. Wireshark oferă o flexibilitate remarcabilă prin posibilitatea de a defini filtre personalizate pentru captarea și analizarea pachetelor, facilitând o înțelegere mai detaliată a traficului de rețea. Datorită acestei granularități, un administrator poate identifica exact sursa problemelor de conectivitate sau poate descoperi comportamente suspecte cu precizie ridicată.

Cu toate acestea, utilizarea Wireshark necesită timp și expertiză pentru interpretarea corectă a datelor. În cazul unui volum mare de trafic, o echipă de securitate poate fi copleșită de cantitatea de informații brute, ceea ce face dificilă detectarea rapidă a atacurilor sofisticate. Din acest motiv, Wireshark este adesea folosit în combinație cu alte soluții – de exemplu, sisteme de detectare a intruziunilor (IDS/IPS) care asigură monitorizare în timp real și alerte automate.

Astfel, Wireshark rămâne un instrument esențial pentru investigații post-eveniment și pentru dezvoltarea abilităților de analiză a securității rețelei, dar nu trebuie privit ca un mijloc unic de protecție. Într-un mediu complex, el reprezintă doar o parte dintr-un ecosistem mai larg de soluții de securitate, completat de automatizări, monitorizare continuă și controale adecvate la nivelul infrastructurii.

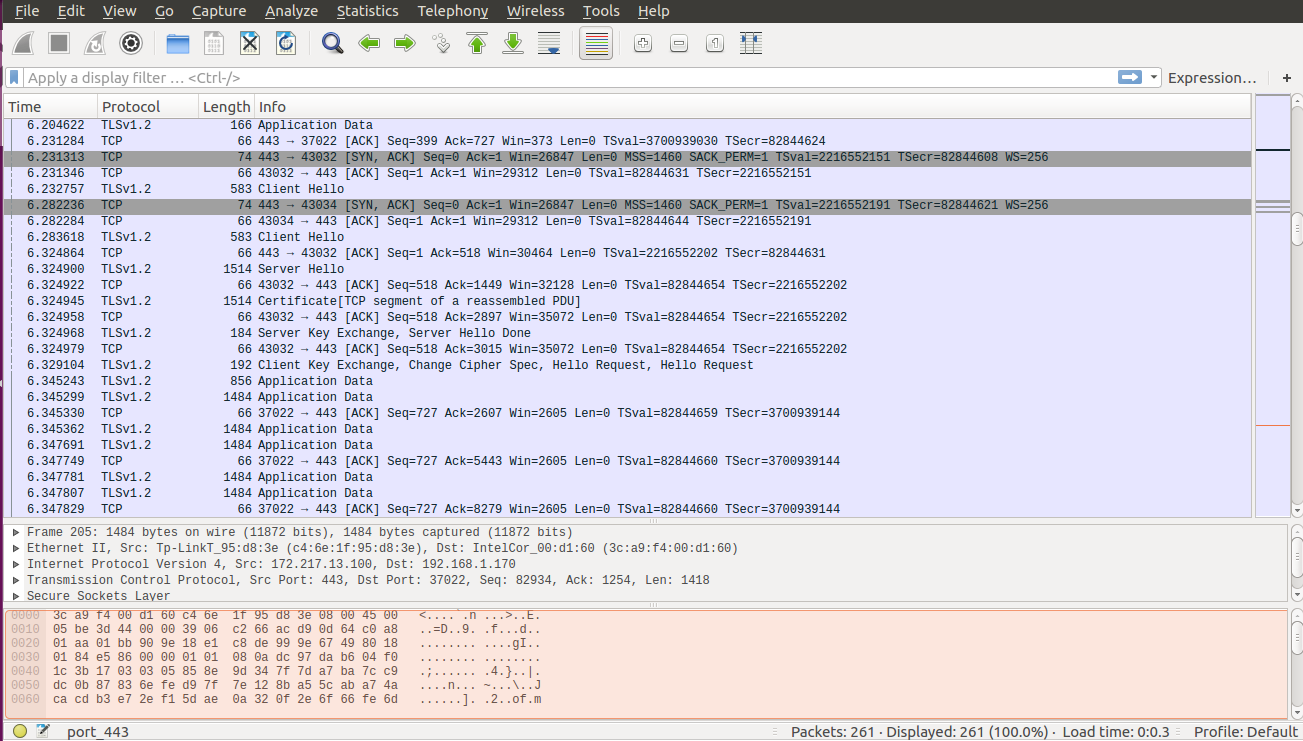


Figura 1 – Wireshark

**tcpdump** – Un instrument în linie de comandă care permite captarea și filtrarea pachetelor de date. Este eficient pentru analiza traficului în timp real, dar are o interfață limitată și necesită cunoștințe avansate pentru interpretarea rezultatelor. **tcpdump** este un instrument pentru specialiștii în securitate și administrare de rețea, însă se folosește exclusiv din linia de comandă. Datorită simplității și a consumului redus de resurse, este deseori preferat în diagnosticarea rapidă a problemelor de rețea și monitorizarea traficului în timp real, mai ales pe sisteme Linux/Unix.

Cu toate acestea, tcpdump oferă doar o interfață textuală, care poate părea intimidantă pentru utilizatorii neexperimentați. Pentru a utiliza eficient filtrele și pentru a interpreta corect datele capturate, este necesar un nivel avansat de cunoștințe de rețea (protocoale, formate de pachete etc.). În plus, pentru analiza post-captură și interpretarea avansată a vulnerabilităților, se recomandă exportarea fișierelor pcap către soluții cu interfață grafică (de exemplu, Wireshark).

Ca și în cazul oricărui instrument de analiză a traficului, tcpdump nu oferă un mecanism automat de detectare a atacurilor. Este util în identificarea problemelor punctuale și în înțelegerea traficului la nivel de pachete, dar nu poate înlocui soluțiile automatizate de monitorizare și securitate (IDS/IPS, SIEM etc.). Prin urmare, implementarea tcpdump în cadrul unei strategii mai ample de securitate trebuie să fie dublată de alte instrumente și procese de detecție și răspuns la incidente.

Изображение выглядит как текст, снимок экрана, Шрифт, число

Автоматически созданное описание

Figura 2 - tcpdump

**Zeek (Bro)** – Un sistem de monitorizare a rețelei care nu doar capturează traficul, ci și analizează comportamentul acestuia pentru detectarea anomaliilor. Comparativ cu alte soluții, Zeek oferă un nivel mai ridicat de automatizare și posibilitatea de a genera rapoarte detaliate despre activitatea rețelei. Pe lângă rolul său de **capturare** a traficului la nivel de rețea, **Zeek (cunoscut anterior sub denumirea Bro)** se diferențiază printr-un **motor sofisticat de analiză a comportamentului**. Practic, Zeek corelează evenimentele de la nivelul aplicațiilor (HTTP, DNS, SSL etc.), transformând fluxurile de trafic în **informații structurate** care pot fi folosite pentru a identifica anomalii și potențiale amenințări de securitate.

Spre deosebire de alte unelte de tip IDS/IPS care se bazează preponderent pe semnături, Zeek adoptă o abordare **mai flexibilă**, analizând semnalele comportamentale și colectând metadate valoroase, cum ar fi cererile DNS sau parametrii tranzacțiilor HTTP. Această abordare face posibilă **detectarea atacurilor necunoscute** sau a tacticilor avansate folosite de atacatori, în condițiile în care semnăturile tradiționale nu ar oferi rezultate.

Beneficiind de un **sistem de scripturi** extensibil, Zeek permite personalizarea regulilor de monitorizare în funcție de nevoile organizației, precum și **integrarea cu alte soluții** de securitate (SIEM, platforme de automatizare etc.). Rapoartele generate de Zeek oferă o **imagine detaliată** asupra activității rețelei, fiind extrem de utile în investigațiile post-eveniment și în luarea deciziilor strategice de securitate. Astfel, Zeek reprezintă o componentă solidă într-o arhitectură de securitate modernă, funcționând atât ca instrument de monitorizare continuă, cât și ca bază pentru detecția proactivă a amenințărilor.

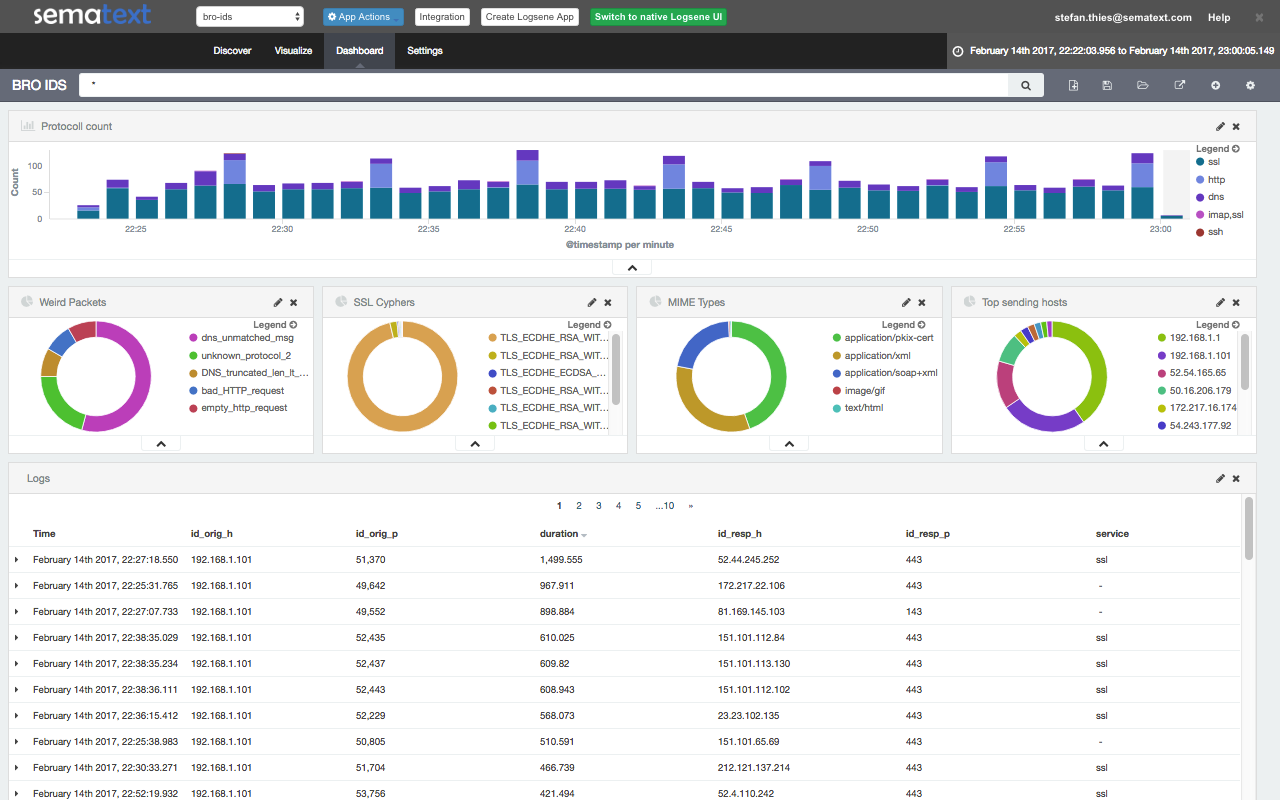


Figura 3 – Zeek

**Suricata** – Un sistem de detecție și prevenire a intruziunilor (IDS/IPS) care analizează traficul în timp real. Spre deosebire de Wireshark și tcpdump, care sunt axate pe captare, Suricata este capabilă să blocheze traficul suspect, având o abordare mai proactivă în securitatea rețelei.

**Sistemul propus** se bazează pe îmbinarea celor mai relevante caracteristici din diverse soluții de monitorizare și analiză a traficului (precum Wireshark, tcpdump sau Zeek), pentru a oferi o **platformă unitară și eficientă**. În loc să se limiteze la captarea pachetelor brute și la o analiză manuală extensivă, noul proiect introduce **funcționalități de filtrare și clasificare avansată**, concepute să reducă semnificativ timpul și expertiza specializată necesare în interpretarea datelor.

Prin agregarea și corelarea informațiilor din surse multiple, sistemul oferă **rapoarte sintetice** care sprijină luarea rapidă de decizii și permite **detecția proactivă** a potențialelor incidente de securitate. Astfel, **abordarea propusă** depășește limitele instrumentelor tradiționale, facilitând un **proces de analiză mai fluid și mai bine integrat** în cadrul infrastructurii de rețea.

1.3 Scopul, obiectivele și cerințele sistemului

Scopul principal al acestui proiect este dezvoltarea unui **sistem integrat pentru interceptarea și analiza traficului de rețea**, care să permită monitorizarea și detecția eficientă a activităților suspecte. Sistemul trebuie să ofere o metodă rapidă și automatizată de captare, filtrare și interpretare a pachetelor de date, contribuind astfel la îmbunătățirea securității cibernetice prin prevenirea și investigarea amenințărilor informatice.

1. **Captarea traficului de rețea** – Dezvoltarea unui modul care să intercepteze pachetele de date în timp real folosind tehnologii precum **tcpdump, Wireshark, Zeek** sau **Suricata**;
2. **Filtrarea și clasificarea pachetelor** – Implementarea unor algoritmi care să extragă și să analizeze doar informațiile relevante, eliminând traficul nesemnificativ;
3. **Detecția activităților suspecte** – Identificarea anomaliilor și a potențialelor atacuri informatice prin metode bazate pe semnături și comportament;
4. **Stocarea și gestionarea datelor** – Crearea unei baze de date sau a unui sistem de logare pentru păstrarea și analizarea ulterioară a traficului interceptat;
5. **Interfață de utilizator (GUI)** – Dezvoltarea unei interfețe intuitive care să permită utilizatorilor să vizualizeze datele capturate și să genereze rapoarte relevante;
6. **Automatizarea procesului** – Integrarea unor funcționalități care să reducă necesitatea intervenției manuale, crescând astfel eficiența detecției.

Pentru ca sistemul să funcționeze eficient, acesta trebuie să îndeplinească o serie de cerințe esențiale, atât funcționale, cât și non-funcționale. Din punct de vedere funcțional, sistemul trebuie să fie capabil să captureze și să analizeze traficul de rețea în timp real, asigurând în același timp filtrarea și clasificarea pachetelor de date pe baza protocoalelor utilizate și a adreselor IP. De asemenea, este necesară integrarea unor mecanisme eficiente de detecție pentru identificarea anomaliilor sau a posibilelor atacuri informatice. Un alt aspect important este posibilitatea de stocare și raportare a datelor relevante, permițând astfel investigarea ulterioară a incidentelor de securitate. Pentru a facilita utilizarea, sistemul trebuie să dispună de o interfață grafică care să permită analiza și gestionarea traficului interceptat într-un mod intuitiv.

Pe lângă cerințele funcționale, sistemul trebuie să respecte și o serie de cerințe non-funcționale. Acesta trebuie să fie scalabil, astfel încât să permită extinderea funcționalităților în funcție de necesități. Performanța trebuie optimizată pentru a evita introducerea unor latențe semnificative în rețea, menținând un echilibru între eficiența analizelor și resursele consumate. Interfața utilizatorului trebuie să fie intuitivă și ușor de utilizat, astfel încât specialiștii în securitate să poată interpreta rapid datele obținute. Nu în ultimul rând, sistemul trebuie să respecte normele legale privind interceptarea și analiza traficului de rețea, asigurând conformitatea cu reglementările în vigoare.

# 2 MODELAREA ȘI PROIECTAREA SISTEMUL INFORMATIC

.....................

2.1 Descrierea comportamentală a sistemului

2.1.1 Imaginea generală asupra sistemului

2.1.2 Modelarea vizuală a fluxurilor

2.1.3 Stările de tranzacție a sistemului

2.1.4 Descrierea scenariilor de utilizare a aplicaţiei

2.1.5 Fluxurile de mesaje şi legăturile dintre componentele sistemului

2.2 Descrierea structurală a sistemului

2.2.1 Descrierea structurii statice a sistemului

2.2.2 Relatiile de dependență între componentele sistemului

2.2.3 Modelarea echipamentelor mediului de implementare

3 REALIZAREA SISTEMULUI

# CONCLUZII

Concluziile reprezintă o secțiune importantă în care se prezintă principalele constatări, rezultate și observații relevante. Această secțiune oferă o perspectivă sintetizată a ceea ce s-a învățat și s-a realizat pe parcursul stagiului.

Rezultatele obținute.

Îndeplinirea obiectivelor.

Observații și feedback

Învățăminte și experiențe.

Importanța practicii.

Concluziile trebuie să fie concise, clare și să ofere o imagine de ansamblu asupra experienței și rezultatelor obținute în timpul practicii tehnologice.

# BIBLIOGRAFIE

1. ȚURCAN, Nelly. Comunicarea ştiinţifică în contextul accesului deschis la informaţie. Chişinău: CEP USM, 2012. 324 p. ISBN 978-9975-71-253-8.
2. WILD, R. Essentials of Production and Operations Management. 3rd ed. London: Cassell Educational Ltd, 1990. 420 p. ISBN 0-304-31674-1.
3. СОЛОМОН, Д. И. Дробное программирование и недифференцируемая оптимизация. Кишинев: Эврика, 2010. ISBN 978-9975-941-53-2
4. POPA, Ana, PROHNIŢCHI, Valeriu. Sectorul de cercetare, dezvoltare şi inovare din Moldova: este oare necesară o reformă? Versiune preliminară [online]. Chişinău: ExpertGrup, 2011 [citat 02.09.2016]. Disponibil: http://www.expertgrup.org/library\_upld/d360.pdf.
5. BOYD-BARRETT, Oliver. Free Flow Doctrine. In: STEPHEN, W. L., FOSS, Karen A., eds. Encyclopedia of Communication Theory [online]. Los Angeles; London: SAGE Publications, 2009 [citat 22.01.2015]. ISBN 978-1-4129-5938-4. Disponibil: http://sk.sagepub.com/reference/communicationtheory.

# ANEXA A

**Denumire anexă**

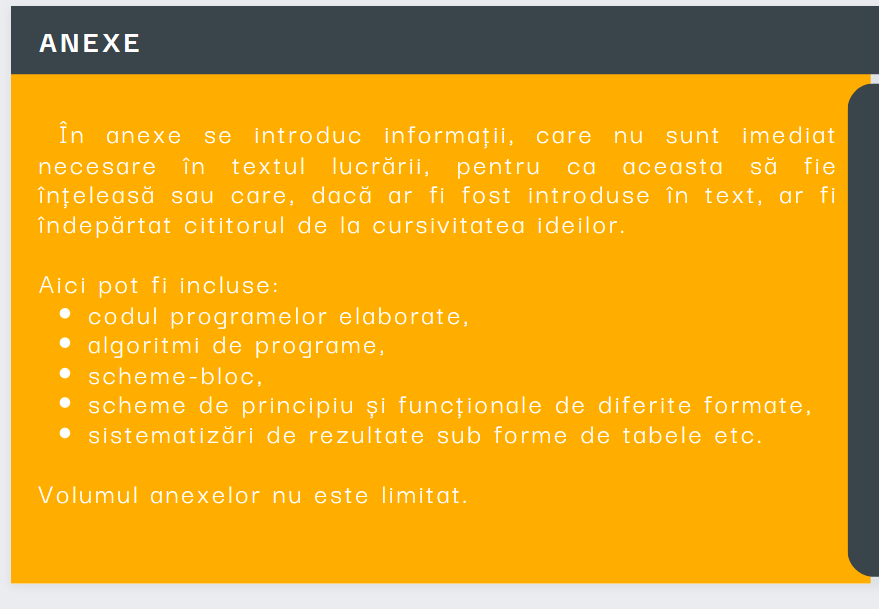


Figura A.1- Denumire figură