

Ministerul Educației, Culturii și Cercetării  
Universitatea Tehnică a Moldovei

Facultatea Calculatoare, informatică și microelectronică  
Departamentul Ingineria Software și Automatică



# RAPORT

Lucrare de Laborator nr.4

Disciplina: Proiectarea sistemelor informaționale

Tema: Modelarea și analiza datelor pentru un proces specific din cadrul sistemului propus  
pentru dezvoltare

A efectuat:  
A verificat:

Chirita Stanislav  
Magdei Octavian

Chișinău 2024

## Introducere

În cadrul acestei lucrări de laborator, obiectivul principal este de a dezvolta un model logic al datelor pentru un proces specific din cadrul unui sistem integrat de interceptare și analiză a traficului de rețea. Modelarea datelor este o activitate esențială în dezvoltarea oricărui sistem informatic, deoarece ajută la structurarea și organizarea informațiilor într-un mod care facilitează procesarea eficientă și corectă a acestora.

Pentru realizarea acestei lucrări, vom folosi aplicația **AllFusion ERwin Data Modeler**, un instrument performant care permite crearea și gestionarea modelelor de date complexe. De asemenea, vom aplica standardul **IDEF1x**, utilizat pentru crearea modelelor logice de date, care definește entitățile de date, attributele acestora și relațiile între entitățile din sistem.

Scopul acestei lucrări este de a înțelege cum se structurează datele într-un sistem de interceptare și analiză a traficului de rețea, de a familiariza utilizatorul cu instrumentele și tehnicile de modelare a datelor și de a crea un model logic care să reflecte fluxurile de informații și interacțiunile din cadrul procesului selectat. Această activitate va contribui la o mai bună înțelegere a cerințelor de date ale sistemului propus și va facilita dezvoltarea și implementarea ulterioară a acestuia.

# Diagrama IDEF1x

Diagrama IDEF1x prezintă procesul de filtrare a traficului de rețea pe baza unor opțiuni specifice. Traficul de rețea capturat este direcționat pentru a fi înregistrat sau izolat, iar utilizatorul selectează pachetele relevante pentru analiză. După ce traficul de rețea interesant este ales, acesta este analizat pentru a identifica comportamente anormale, cum ar fi atacurile cibernetice sau alte probleme de rețea. După analiza traficului, utilizatorul selectează tipul de eveniment care trebuie raportat, iar informațiile suplimentare, cum ar fi comentarii sau descrierea evenimentului, sunt adăugate pentru a completa raportul. La final, raportul generat cuprinde detaliile despre traficul analizat, tipul de eveniment identificat și orice alte informații relevante, oferind un rezumat complet al incidentului și recomandările corespunzătoare.

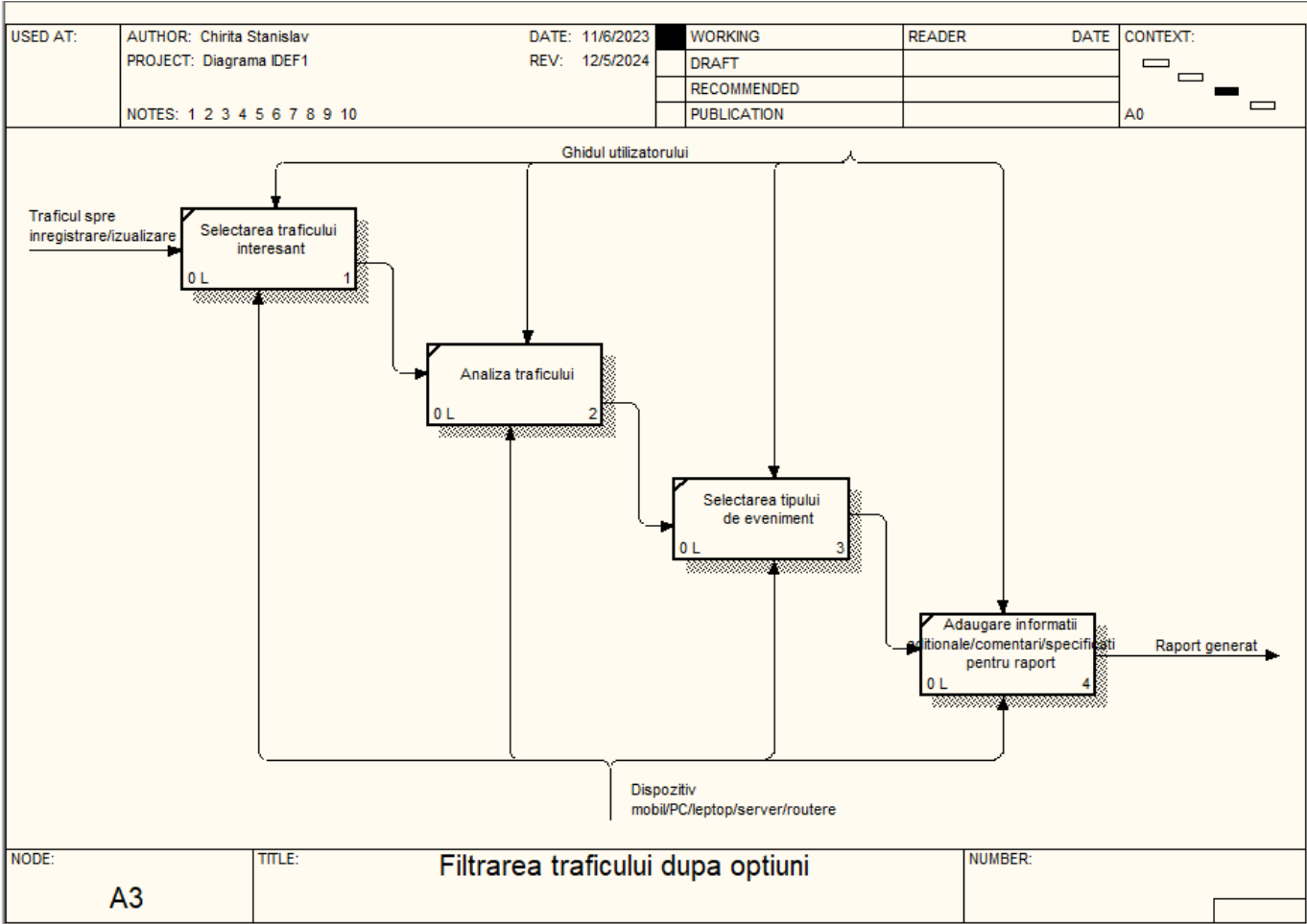


Figura 1 – Diagrama IDEF1

Aceste analize nu doar că ajută la detectarea amenințărilor în timp real, dar contribuie și la îmbunătățirea măsurilor preventive. Informațiile suplimentare adăugate în raport permit o documentare detaliată și o înțelegere clară a contextului în care a avut loc incidentul, facilitând astfel o reacție promptă și corectă. Raportul generat joacă un rol crucial în procesul decizional, permițând administratorilor să ia măsuri rapide pentru protejarea infrastructurii rețelei și pentru prevenirea unor posibile atacuri viitoare. Acest proces poate fi integrat în platforme de monitorizare și gestionare a securității, ajutând organizațiile să răspundă rapid și eficient la orice amenințare.

Concluzie: În concluzie, procesul de filtrare a traficului de rețea, detaliat în diagrama IDEF1x, reprezintă un element crucial în monitorizarea și protejarea infrastructurii rețelelor de comunicații. Prin capturarea, selecția și analiza atentă a pachetelor de trafic, sistemul permite identificarea rapidă a comportamentelor anormale și a eventualelor amenințări de securitate, cum ar fi atacurile cibernetice. Generarea unui raport detaliat, care include informații suplimentare relevante, ajută la documentarea incidentelor și la furnizarea de recomandări clare pentru măsurile corective. Acest proces nu doar că îmbunătățește securitatea rețelelor, dar și contribuie la optimizarea performanței acestora, asigurând o reacție rapidă și bine fundamentată în fața oricăror probleme de securitate. Implementarea unui astfel de sistem de monitorizare și raportare a traficului este esențială pentru menținerea unui mediu de rețea sigur, protejând atât infrastructura tehnologică, cât și datele sensibile ale organizațiilor.