**MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA**
**Universitatea Tehnică a Moldovei**
**Facultatea Calculatoare, Informatică şi Microelectronică**
**Departamentul Ingineria Software și Automatică**

**Admis la susţinere**
**Şef departament:**
**FIODOROV Ion dr., conf.univ.**

**----------**
**„___" _____ 2025**

# ANALIZA EMPIRICĂ A TEHNICILOR DE PROTEJARE A ANONIMITĂȚII FOLOSITE DE REȚELELE ANONIME

## Teză de master

**Student:** _____ **Stroncea Ion, TI-231M**

**Coordonator:** _____ **Marusic Galina, dr., conf. univ.**

**Consultant:** _____ **Cojocaru Svetlana, asist.univ.**

**Chişinău, 2025**

# REZUMAT

Lucrarea de față abordează problematica anonimității în mediul digital, evidențiind rolul esențial al protejării confidențialității utilizatorilor într-o lume marcată de digitalizare rapidă și colectare intensivă de date. Cercetarea pornește de la premisa că anonimitatea devine un element esențial pentru menținerea libertății personale și a securității informațiilor.

În prima parte a lucrării este stabilit cadrul conceptual, evidențiindu-se motivele pentru care anonimitatea este importantă și riscurile generate de lipsa acesteia. Se arată că utilizatorii pot fi expuși la monitorizare excesivă, manipulare sau discriminare, ceea ce justifică nevoia unor sisteme capabile să le protejeze identitatea.

Sunt prezentate și analizate tehnici de protejare a anonimității precum transmiterea pachetelor de dimensiuni egale, segmentarea traficului, transmiterea sincronizată și rutarea datelor prin noduri intermediare. Pentru fiecare metodă, se descriu principiile de funcționare, avantajele și limitările.

Pe lângă descrierea tehnicilor existente, lucrarea propune criterii clare de evaluare, precum costul de viteză, costul de calcul și costul de memorie. Aceste criterii oferă un cadru obiectiv pentru compararea și interpretarea performanțelor soluțiilor analizate, facilitând identificarea opțiunilor optime.

Un element central al cercetării constă în proiectarea și utilizarea unor aplicații experimentale menite să testeze direct tehnicile de anonimizare. Aceste aplicații permit simularea unor scenarii reale, în care sunt măsurate latența, consumul de resurse și gradul de securitate asigurat.

Datele colectate în urma testelor sunt supuse unei analize detaliate, urmărindu-se evidențierea pattern-urilor și corelațiilor între nivelul de anonimitate și costurile implicate. Scopul este de a obține o imagine clară asupra compromisurilor necesare între securitate și performanță.

Fără a anticipa concluziile, lucrarea caută direcții de optimizare a tehnicilor existente, adaptând soluțiile la nevoile concrete ale aplicațiilor și utilizatorilor. Astfel, se subliniază importanța unei abordări flexibile, capabilă să răspundă diferitelor modele de amenințări și constrângeri tehnologice.

Lucrarea furnizează, de asemenea, recomandări pentru proiectanți și dezvoltatori. Ei pot alege strategiile adecvate în funcție de necesitățile lor specifice, punând în balanță viteza, resursele disponibile și nivelul de anonimitate dorit. Astfel, este posibilă ajustarea fină a sistemelor anonime pentru diferite contexte.

Dintr-o perspectivă mai largă, se evidențiază faptul că anonimitatea nu este doar o problemă tehnică, ci și una cu implicații etice, sociale și juridice. Protecția confidențialității și a libertății utilizatorilor devine un obiectiv complex, care presupune integrarea mai multor discipline și abordări.

În ansamblu, lucrarea oferă un cadru teoretic și practic pentru înțelegerea, evaluarea și îmbunătățirea sistemelor anonime. Prin analiza aprofundată, testarea empirică și propunerea de recomandări, se creează un ghid valoros pentru viitorii cercetători, dezvoltatori și factori de decizie preocupați de menținerea anonimității în mediul digital.

## ABSTRACT

This paper addresses the issue of anonymity in the digital environment, highlighting the essential role of protecting users' privacy in a world marked by rapid digitalization and intensive data collection. The research starts from the premise that anonymity has become a crucial element for maintaining personal freedom and information security.

In the first part of the paper, a conceptual framework is established, emphasizing the reasons why anonymity is important and the risks posed by its absence. It is shown that users may be exposed to excessive monitoring, manipulation, or discrimination, which justifies the need for systems capable of protecting their identity.

Techniques for safeguarding anonymity are presented and analyzed, including the transmission of equal-sized packets, traffic segmentation, synchronized transmission, and data routing through intermediary nodes. For each method, the principles of operation, as well as their advantages and limitations, are described.

In addition to describing existing techniques, the paper proposes clear evaluation criteria, such as speed cost, computational cost, and memory cost. These criteria provide an objective framework for comparing and interpreting the performance of the analyzed solutions, facilitating the identification of optimal options. A central element of the research involves designing and using experimental applications aimed at directly testing anonymization techniques. These applications allow the simulation of real scenarios, in which latency, resource consumption, and the degree of security provided are measured.

The data collected from the tests undergo a detailed analysis to highlight patterns and correlations between the level of anonymity and the associated costs. The goal is to obtain a clear understanding of the necessary trade-offs between security and performance.

Without anticipating conclusions, the paper seeks directions for optimizing existing techniques, adapting solutions to the concrete needs of applications and users. Thus, it underscores the importance of a flexible approach capable of responding to different threat models and technological constraints.

The paper also provides recommendations for designers and developers. They can select appropriate strategies based on their specific needs, balancing speed, available resources, and the desired level of anonymity. In this way, anonymous systems can be fine-tuned for various contexts.

From a broader perspective, the fact that anonymity is not merely a technical problem, but also one with ethical, social, and legal implications, is highlighted. Protecting users' privacy and freedom becomes a complex objective, requiring the integration of multiple disciplines and approaches.

Overall, the paper offers both a theoretical and practical framework for understanding, evaluating, and improving anonymous systems. Through in-depth analysis, empirical testing, and the provision of recommendations, it creates a valuable guide for future researchers, developers, and decision-makers concerned with maintaining anonymity in the digital environment.

# CUPRINS

# LISTA DE ABREVIERI

**Memorie RAM (Random Access Memory)** - Memoria RAM este un tip de memorie volatilă a calculatorului, utilizată pentru stocarea temporară a datelor și instrucțiunilor pe care procesorul le accesează în timp real. Aceasta este responsabilă de viteza și fluiditatea cu care sistemul rulează aplicațiile și procesele.

**CPU (Central Processing Unit)** - CPU-ul, sau unitatea centrală de procesare, este adesea descris ca „creierul" unui calculator. Este componenta principală care execută instrucțiunile programelor, efectuând calcule aritmetice, operații logice și controlând fluxul de date dintre diferitele componente ale sistemului.

**I2P(invisible internet project)-** O rețea anonimă care ascunde identitatea și destinația traficului prin criptare și rutare printr-un lanț distribuit de noduri.

**VoIP(Voice over IP) -** Tehnologie care transmite apeluri vocale prin rețele IP, transformând vocea în pachete de date și eliminând necesitatea liniilor telefonice tradiționale.

**TOR(The onion router) -** Un sistem de anonimizare a traficului online ce utilizează o rutare în straturi criptate prin noduri voluntare, ascunzând sursa și destinația datelor.

# INTRODUCERE

Într-o eră marcată de o digitalizare accelerată și de o prezență online tot mai accentuată, anonimitatea devine un element esențial pentru menținerea confidențialității și a libertății individuale. Evoluția tehnologiei a permis colectarea și analiza unui volum fără precedent de date, fapt ce a generat preocupări majore legate de modul în care informațiile personale sunt gestionate, stocate și distribuite.

Pe parcursul acestei cercetări, se urmărește explorarea, într-o manieră sistematică, a fundamentelelor și complexității asigurării anonimității în mediul digital. Prin intermediul unei analize teoretice și practice, se încearcă înțelegerea modului în care diverse tehnici de protecție a identității utilizatorilor pot fi implementate, evaluate și optimizate.

De-a lungul investigației, se va stabili cadrul conceptual care justifică necesitatea sistemelor anonime, evidențiind atât avantajele asigurării anonimității, cât și riscurile pe care lipsa acesteia le implică. În absența unui nivel adecvat de protecție, utilizatorii pot deveni vulnerabili la monitorizare excesivă, ingerințe în viața privată, manipulare psihologică sau diferite forme de discriminare, evidențiind astfel nevoia unor soluții eficiente.

Pe parcursul lucrării, se vor identifica și analiza principalele tehnici utilizate în prezent pentru protejarea anonimității. Printre acestea, se vor examina metode precum transmiterea pachetelor de dimensiuni uniforme, segmentarea traficului în pachete mai mici, transmiterea sincronizată, precum și rutarea datelor prin lanțuri de noduri intermediare.

În plus, se vor stabili criterii clare de evaluare a soluțiilor analizate: costul de viteză, costul de calcul și costul de memorie, pentru a oferi un cadru obiectiv în interpretarea rezultatelor și luarea unor decizii informate privind aplicarea acestora.

De asemenea, pe parcursul cercetării se vor dezvolta și utiliza aplicații experimentale, menite să testeze direct soluțiile de protecție a anonimității. Prin rularea lor se vor simula scenarii reale, ce vor permite colectarea unor date relevante despre latență, consumul de resurse și nivelul de securitate. Abordarea experimentală va completa analiza teoretică și va furniza o bază empirică solidă.

Ulterior, se vor analiza datele obținute în urma testelor pentru a evidenția pattern-uri, corelații și tendințe. Fără a anticipa concluziile, obiectivul este de a identifica direcții de optimizare și rafinare a tehnicilor, astfel încât să se atingă un echilibru între anonimitate și performanță, în funcție de cerințele specifice ale diverselor aplicații și contexte de utilizare.

În paralel, se vor formula recomandări pentru proiectanții și dezvoltatorii de sisteme, astfel încât aceștia să poată alege strategiile adecvate nevoilor lor. Înțelegerea punctelor forte și limitărilor fiecărei metode va permite adaptarea sistemelor anonime, ținând cont de constrângerile de resurse, cerințele de latență sau modelele de amenințare specifice situațiilor analizate.

# BIBLIOGRAFIE


1] "What Does Google Do With Your Data?," 30 9 2024. [Online]. Available: https://www.avast.com/c-how-google-uses-your-data.

[2] "Data Policy," 30 09 2024. [Online]. Available: https://www.facebook.com/about/privacy/plain_text_p.

[3] A. Esteve, "The business of personal data: Google, Facebook, and privacy issues in the EU and the USA," *International Data Privacy Law,* pp. 36-47, 2017.

[4] B. J. Z. Guo, "Influence of personalised advertising copy on consumer engagement: a field experiment approach," *Electron Commer Res,* 2023.

[5] N. Singer, "This Ad's for You (Not Your Neighbor)," 20 09 2022. [Online]. Available: https://www.nytimes.com/2022/09/15/business/custom-political-ads.html.

[6] J. R. P. M. Burkell, "Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more autonomy," *Internet Policy Review,* pp. 1-24, 2019.

[7] "What is Regional Pricing? A Beginner's Guide to Adapting Your Prices Globally," 9 09 2024. [Online]. Available: https://worldwidepricing.com/blog/what-is-regional-pricing .

[8] S. Ion, "PROTEJAREA IDENTITĂȚILOR, PROTEJAREA CONFIDENȚIALITĂȚII: O EXAMINARE A TEHNICILOR UTILIZATE DE REȚELELE ANONIME," in *Conferinţa tehnico-ştiinţifică a studenţilor, masteranzilor şi doctoranzilor = Technical Scientific Conference of Undergraduate, Master and PhD Students: Chişinău, 27-29 martie 2024. Universitatea Tehnică a Moldovei. Vol. 1*, Chisinau, 2024.