Universitatea Politehnica Timișoara  
Facultatea de Automatică și Calculatoare

Utilizarea inteligenței artificiale și machine learning în detecția amenințărilor cibernetice

Securitatea sistemelor de calcul

An universitar 2024-2025

**Ispas Daniela-Estera**

***Anul 3, TI***  
E-mail: [daniela.ispas@student.upt.ro](mailto:daniela.ispas@student.upt.ro)

## **Cuprins**

[**Cuprins** 2](#_Toc193125984)

[**1.Introducere** 3](#_Toc193125985)

[**1.1.** **Definiția inteligenței artificiale și a machine learning-ului** 3](#_Toc193125986)

[**1.2. Importanța securității cibernetice** 3](#_Toc193125987)

[**1.3. Rolul AI și ML în detecția amenințărilor cibernetice** 3](#_Toc193125988)

[**2. Metode AI utilizate în detecția amenințărilor cibernetice** 3](#_Toc193125989)

[2.1. Algoritmi folosiți în securitatea cibernetică 3](#_Toc193125990)

[2.2. Sistemele de detecție a intruziunilor bazate pe AI 3](#_Toc193125991)

[2.3. AI în analiza malware-ului și phishingului 3](#_Toc193125992)

[**3. Avantaje și limitări ale utilizării AI în securitatea cibernetică** 3](#_Toc193125993)

[3.1. Creșterea eficienței și reducerea erorilor 3](#_Toc193125994)

[3.2. Atacuri adversariale și vulnerabilități ale sistemelor AI 3](#_Toc193125995)

[3.3. Provocări în implementarea AI 3](#_Toc193125996)

[**4. Impactul automatizării în securitatea cibernetică** 3](#_Toc193125997)

[4.1. Beneficii și riscuri ale deciziilor automate 3](#_Toc193125998)

[**5. Concluzii și perspective viitoare** 3](#_Toc193125999)

[5.1. Evoluția AI în securitatea cibernetică 3](#_Toc193126000)

[5.2. Tendințe și recomandări pentru viitor 3](#_Toc193126001)

[**6.Bibliografie** 3](#_Toc193126002)

## **1.Introducere**

### Definiția inteligenței artificiale și a machine learning-ului

### 1.2. Importanța securității cibernetice

### 1.3. Rolul AI și ML în detecția amenințărilor cibernetice

## **2. Metode AI utilizate în detecția amenințărilor cibernetice**

### 2.1. Algoritmi folosiți în securitatea cibernetică

### 2.2. Sistemele de detecție a intruziunilor bazate pe AI

### 2.3. AI în analiza malware-ului și phishingului

## **3. Avantaje și limitări ale utilizării AI în securitatea cibernetică**

### 3.1. Creșterea eficienței și reducerea erorilor

### 3.2. Atacuri adversariale și vulnerabilități ale sistemelor AI

### 3.3. Provocări în implementarea AI

## **4. Impactul automatizării în securitatea cibernetică**

### 4.1. Beneficii și riscuri ale deciziilor automate

## **5. Concluzii și perspective viitoare**

### 5.1. Evoluția AI în securitatea cibernetică

### 5.2. Tendințe și recomandări pentru viitor

## **6.Bibliografie**

* <https://www.hostragons.com/ro/blog/inteligenta-artificiala-si-securitatea-cibernetica/?utm_source=chatgpt.com>
* <https://www.microsoft.com/ro-ro/security/business/security-101/what-is-ai-for-cybersecurity?utm_source=chatgpt.com>
* <https://www.mbd.ro/gestionarea-avansata-a-amenintarilor-revolutionarea-securitatii-cibernetice-prin-monitorizare-si-detectare-bazata-pe-inteligenta-artificiala/?utm_source=chatgpt.com>
* <https://www.prodefence.ro/inteligenta-artificiala-ai-si-securitatea-cibernetica/?utm_source=chatgpt.com>
* <https://trsdesign.ro/impactul-inteligentei-artificiale-ai-asupra-securitatii-cibernetice/?utm_source=chatgpt.com>
* <https://philarchive.org/archive/SFEIAI?utm_source=chatgpt.com>