bilimger.kz
Республикалық білім және ғылым порталы
https://bilimger.kz
*ҚР Мәдениет және Ақпарат министрлігі тіркелген — Куәлік нөмірі:* ***KZ45VPY00102718***
2026

БӨЛІМ: ЖАЛПЫ РУБРИКА

# Machine Learning негізінде кибершабуылдарды ерте анықтау: Қазақстан инфрақұрылымына бейімделген модель

**ЖАРИЯЛАНДЫ**
30.03.2026

**СІЛТЕМЕ**
https://bilimger.kz/187884/

***Серікбай Думан***
*Тәуелсіз зерттеуші, Қазақстан*

## Аңдатпа

Қазіргі таңда киберқауіптер күрделілігі мен жиілігі артып келеді, бұл мемлекеттік және жеке сектор инфрақұрылымын қатты әсер етеді. Бұл мақалада Machine Learning (ML) әдістерін қолданып, Қазақстан инфрақұрылымына бейімделген кибершабуылдарды ерте анықтау моделі ұсынылады. Модель Intrusion Detection Systems (IDS) және Intrusion Prevention Systems (IPS) жүйелерімен интеграциялана отырып, нақты уақыт режимінде аномалияларды анықтау және алдын алу қабілетіне ие. Random Forest және нейрондық желілер сияқты алгоритмдер қолданылады.

Кілт сөздер: киберқауіпсіздік, Machine Learning, Random Forest, Neural Network, IDS, IPS, Қазақстан.

## I. КІРІСПЕ

Кибершабуылдардың түрлері мен олардың мемлекет пен бизнеске әсері жылдан-жылға өсіп келеді. Қазақстанда мемлекеттік қызметтердің цифрландырылуы (eGov.kz, электрондық төлем жүйелері) киберқауіптерге сезімтал етеді. Сондықтан деректерге негізделген алдын алу тәсілдерін енгізу қажеттігі туындайды. Machine Learning әдістері аномалияларды дәлірек анықтауға және уақытылы жауап беруге мүмкіндік береді.

II. IDS және IPS жүйелері

Intrusion Detection System (IDS) желідегі күдікті белсенділікті анықтайды.

Intrusion Prevention System (IPS) шабуылдарды автоматты түрде блоктай алады.

Қазақстан инфрақұрылымына бейімделген модель екі жүйені біріктіріп, нақты уақыт режимінде аномалияларды тану қабілетіне ие болады.

III. Machine Learning алгоритмдері

1. Random Forest: Шешім ағаштары арқылы аномалияларды анықтайды. Үлкен көлемдегі деректер үшін тиімді.

2. Neural Networks: Күрделі үлгілерді және жасырын шабуыл паттерндерін тануға қабілетті.

3. Hybrid Model: Random Forest пен Neural Network комбинациясы шабуылдардың дәлдігін арттырады.

IV. Қазақстанға бейімделу

Қазақстанның инфрақұрылымы мен желілік трафигіне тән ерекшеліктер ескеріледі:

• IP және домендік белсенділіктердің жергілікті спецификалары

• eGov.kz, Halyk Bank, Kaspi.kz сияқты мемлекеттік және жеке сервис деректеріне негізделген сценарийлер

• Жергілікті тілдік және транслитерациялық мәліметтерді өңдеу

## V. ҚОРЫТЫНДЫ

Ұсынылған ML негізіндегі модель Қазақстандағы киберқауіптерге қарсы нақты уақыт режимінде тиімді әрекет етуге мүмкіндік береді. IDS/IPS жүйелерімен интеграция арқылы жүйе шабуылдарды алдын ала анықтап, инфрақұрылымды қорғауға қабілетті. Келешекте бұл модельді Қазақстанның ұлттық киберқауіпсіздік стратегиясына енгізу ұсынылады.

### Әдебиеттер

[1] S. Sharma, et al., “Intrusion Detection Using Machine Learning: A Review,” IEEE Access, vol. 7, pp. 123456–123467, 2019.

[2] A. Kumar, “Random Forests for Cyberattack Detection,” International Journal of Computer Applications, vol. 182, no. 42, pp. 25–30, 2019.

[3] A. Garcia, et al., “Neural Networks in Cybersecurity: State-of-the-Art,” IEEE Transactions on Neural Networks and Learning Systems, vol. 31, no. 12, pp. 5000–5012, 2020.