

# GENERATIV SUN'IY INTELLEKT YORDAMIDA KIBERHUJUMLARNI ANIQLASH VA OLDINI OLISH USULLARI

*Imamaliyev Aybek Turapbayevich*

*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti dotsenti, PhD*

*G'ulomova Ko'hinur Murod qizi*

*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti*

**Annotatsiya:** Ushbu maqolada generativ sun'iy intellekt (AI) yordamida kiberhujumlarni aniqlash va oldini olish usullari tahlil qilinadi. Zamonaviy axborot tizimlarida DoS, DDoS va to'liq ajratib bajariladigan hujumlarining murakkablashuvi hamda keng tarqalishi ko'rib chiqiladi. Tadqiqotda mashinali o'qitish va teran o'rganish modellari asosida tarmoq trafiklari, server loglari va foydalanuvchi xatti-harakatlarini tahlil qilish usullari tahlil etiladi. Shuningdek, AI asosidagi tizimlarning an'anaviy xavfsizlik vositalariga nisbatan ustunliklari yoritilib, real vaqt rejimida tahdidlarni aniqlash va oldini olish imkoniyatlari ko'rsatildi. Amaliy tajribada virtual muhitda to'liq ajratib bajariladigan hujumlar sinovdan o'tkazilib, ularni aniqlash va bloklash samaradorligi tahlil qilindi. Olingan natijalar sun'iy intellekt texnologiyalarining kiberxavfsizlikda yuqori samaradorlikka ega ekanligini tasdiqlaydi.

**Kalit so'zlar:** Sun'iy intellekt, generativ AI, kiberxavfsizlik, DoS hujum, DDoS hujum, to'liq ajratib bajariladigan hujum, IDS/IPS, tarmoq xavfsizligi, log tahlili, mashinali o'qitish, teran o'rganish, Fail2Ban.

## *Kirish*

Hozirgi kunda axborot texnologiyalarining jadal rivojlanishi va raqamli transformatsiya jarayonlarining kengayishi natijasida kiberxavfsizlik masalalari dolzarb ahamiyat kasb etmoqda. Internet tarmoqlari va bulutli texnologiyalarning rivojlanishi DoS, DDoS, to'liq ajratib bajariladigan, malware va fishing kabi kiberhujumlar xavfini oshirmoqda.

An'anaviy xavfsizlik vositalari zamonaviy murakkab hujumlarni aniqlashda ko'pincha yetarli emas. Shu sababli, sun'iy intellekt va mashinali o'qitishga asoslangan yondashuvlarga ehtiyoj ortmoqda. Generativ sun'iy intellekt katta hajmdagi ma'lumotlarni tahlil qilish, noodatiy faoliyatni aniqlash va tahdidlarni oldindan bashorat qilish imkonini beradi. Shu bilan birga, hujumlarni simulyatsiya qilish va tizim zaifliklarini aniqlash orqali proaktiv xavfsizlikni ta'minlashga xizmat qiladi. Mazkur maqolaning maqsadi generativ sun'iy intellekt yordamida kiberhujumlarni aniqlash va oldini olish usullarini tahlil qilishdan iborat.

## *Generativ sun'iy intellekt va kiberxavfsizlik asoslari*

Sun'iy intellekt (Artificial Intelligence - AI) zamonaviy axborot texnologiyalarining muhim yo'nalishlaridan biri bo'lib, u kompyuter tizimlariga ma'lumotlarni tahlil qilish, qaror qabul qilish, naqshlarni aniqlash va prognozlash kabi inson aqliy faoliyatiga xos vazifalarni bajarish imkonini beradi. So'nggi yillarda AI texnologiyalari tibbiyot, moliya, transport va ayniqsa kiberxavfsizlik sohasida keng qo'llanilmoqda.

AI ning muhim yo'nalishlaridan biri generativ sun'iy intellekt hisoblanadi. Generativ AI mavjud ma'lumotlar asosida yangi ma'lumotlar yaratishga qodir bo'lib, teran o'rganish algoritmlariga asoslanadi. U matn, tasvir va nutqni qayta ishlash kabi ko'plab vazifalarni bajaradi hamda murakkab jarayonlarni modellashtirish imkonini beradi.

Kiberxavfsizlik sohasida generativ AI texnologiyalarining ahamiyati ortib bormoqda. Zamonaviy kiberhujumlar murakkab va tez o'zgaruvchan bo'lgani sababli, an'anaviy xavfsizlik tizimlari ko'pincha faqat oldindan ma'lum tahdidlarni aniqlash bilan cheklanadi. AI asosidagi

tizimlar esa yangi va noma'lum hujumlarni ham aniqlash imkoniyatiga ega bo'lib, xavfsizlik darajasini oshiradi.

Generativ AI kiberxavfsizlikda asosan anomaliyalarni aniqlash, tahdidlarni prognozlash, hujumlarni modellashtirish va avtomatlashtirilgan himoya tizimlarini yaratishda qo'llaniladi. Masalan, foydalanuvchi faoliyatidagi noodatiy o'zgarishlar yoki qisqa vaqt ichida ko'p marotaba ruxsatsiz kirishga urinishlar aniqlansa, tizim buni hujum sifatida baholashi mumkin. Shuningdek, tarmoq trafiklarini tahlil qilish orqali DDoS hujumlarini oldindan bashorat qilish mumkin.

Bundan tashqari, generativ AI yordamida hujum ssenariylarini modellashtirish orqali tizim zaifliklarini aniqlash va xavfsizlik vositalarini sinovdan o'tkazish mumkin. Bu esa proaktiv xavfsizlikni ta'minlashga yordam beradi. AI asosidagi tizimlar ko'pincha mashinali o'qitish va teran o'rganish algoritmlariga tayanadi va katta hajmdagi ma'lumotlarni yuqori aniqlik bilan tahlil qiladi.

Shu bilan birga, generativ AI texnologiyalari hujumchilar tomonidan ham qo'llanilishi mumkin. Masalan, avtomatlashtirilgan fishing xatlari yaratish yoki zararli dasturlarni ishlab chiqishda AI dan foydalanish mumkin. Bu esa ushbu texnologiyaning ikki tomonlama xususiyatga ega ekanligini ko'rsatadi.

Xulosa qilib aytganda, generativ sun'iy intellekt kiberxavfsizlik sohasida muhim vosita bo'lib, u nafaqat tahdidlarni aniqlash, balki ularning oldini olishda ham samarali yechim hisoblanadi. Shu sababli, AI texnologiyalarini kiberxavfsizlik tizimlariga integratsiya qilish zamonaviy axborot tizimlarini himoya qilishda muhim ahamiyatga ega.

### *3. Sun'iy intellekt yordamida kiberhujumlarni aniqlash usullari.*

*1-jadval.*

Kiberhujumlarni aniqlash usullarining taqqoslanishi.

| Usul             | Afzalligi                  | Kamchiligi                |
|------------------|----------------------------|---------------------------|
| An'anaviy IDS    | Tez ishlaydi               | Yangi hujumni aniqlamaydi |
| AI asosidagi IDS | Yangi hujumlarni aniqlaydi | Resurs talab qiladi       |
| Fail2Ban         | Oddiy va samarali          | Faqat login hujumlar      |

Zamonaviy axborot tizimlarida kiberhujumlarni aniqlash muhim vazifalardan biri hisoblanadi. An'anaviy usullar asosan oldindan ma'lum bo'lgan hujum izlariga (signatura) asoslanadi, biroq bugungi kunda murakkab va noma'lum hujumlarni aniqlashda bu yondashuv yetarli emas. Shu sababli sun'iy intellektga asoslangan usullar keng qo'llanilmoqda.

Sun'iy intellekt tizimlari katta hajmdagi ma'lumotlarni tahlil qilib, undagi yashirin qonuniyatlarni aniqlaydi. Ular tarmoq trafiklari, server loglari va foydalanuvchi xatti-harakatlarini o'rganib, odatiy holatdan chetga chiqishlarni aniqlaydi. Bu usul anomaliyalarni aniqlash deb ataladi va kiberxavfsizlikda samarali yondashuvlardan biri hisoblanadi.

Server log fayllari kiberhujumlarni aniqlashda muhim manba bo'lib, ular tizimdagi barcha faoliyatni qayd etadi. AI yordamida ushbu loglar avtomatik tahlil qilinib, shubhali harakatlar aniqlanadi. Masalan, qisqa vaqt ichida ko'p marotaba noto'g'ri login urinishlari brute-force hujumining belgisi bo'lishi mumkin. Bunday holatlarda tizim IP manzilni bloklash yoki qo'shimcha himoya choralari qo'llashi mumkin.

DoS va DDoS hujumlarini aniqlashda esa tarmoq trafiklarini monitoring qilish muhim ahamiyatga ega. Agar trafik hajmi keskin oshsa yoki noodatiy faoliyat kuzatilsa, tizim hujum ehtimolini aniqlaydi va tegishli choralar ko'radi. Shuningdek, IDS va IPS tizimlari AI bilan integratsiya qilinib, yangi va noma'lum tahdidlarni ham aniqlash imkoniyatiga ega bo'ladi.

Amaliy jihatdan Fail2Ban kabi vositalar server loglarini tahlil qilib, shubhali faoliyatni aniqlaydi va hujum qiluvchi IP manzillarni bloklaydi. Uni AI tizimlari bilan birlashtirish orqali yanada samarali natijalarga erishish mumkin. Bundan tashqari, foydalanuvchi xatti-harakatlarini tahlil qilish (UBA) usuli yordamida noodatiy faoliyat aniqlanadi, masalan, noodatiy vaqt yoki joydan kirishlar xavf sifatida baholanadi.

AI asosidagi tizimlarning asosiy afzalligi ularning moslashuvchanligidir. Ular vaqt o'tishi bilan yangi ma'lumotlar asosida takomillashadi va yanada aniq natijalar beradi. Shu bilan birga, katta hajmdagi ma'lumotlarni tezkor qayta ishlash imkoniyati real vaqt rejimida tahdidlarni aniqlashga yordam beradi. Biroq, AI tizimlarida noto'g'ri ijobiy (false positive) va noto'g'ri salbiy (false negative) natijalar yuzaga kelishi mumkin. Shu sababli modellarning to'g'ri o'qitilishi va doimiy yangilanib borilishi muhim hisoblanadi.

#### *Sun'iy intellekt yordamida kiberhujumlarni oldini olish usullari*

Umuman olganda, sun'iy intellekt yordamida kiberhujumlarni aniqlash zamonaviy kiberxavfsizlik tizimlarining muhim qismiga aylanib bormoqda.

Zamonaviy kiberxavfsizlik tizimlarida nafaqat hujumlarni aniqlash, balki ularning oldini olish ham muhim ahamiyatga ega. Shu sababli sun'iy intellektga asoslangan texnologiyalar tahdidlarni real vaqt rejimida bartaraf etish va tizimlarni avtomatik himoya qilishda keng qo'llanilmoqda.

AI asosidagi tizimlarning asosiy afzalligi ularning moslashuvchanligi va avtomatlashtirilgan boshqaruv imkoniyatidir. Ular doimiy ravishda ma'lumotlarni tahlil qilib, aniqlangan tahdidlarga nisbatan avtomatik choralar ko'radi. Bu esa inson omiliga bog'liq xatoliklarni kamaytiradi va xavfsizlik darajasini oshiradi.

Kiberhujumlarni oldini olishda sun'iy intellekt bilan integratsiyalashgan "aqlli firewall" tizimlari muhim rol o'ynaydi. Ular tarmoq trafikini chuqur tahlil qilib, shubhali faoliyatni aniqlaydi va avtomatik ravishda bloklaydi. Masalan, noodatiy trafik aniqlanganda tizim uni cheklaydi yoki butunlay to'sib qo'yadi.

Brute-force hujumlariga qarshi esa kuchli autentifikatsiya va avtomatik bloklash mexanizmlari qo'llaniladi. AI foydalanuvchi xatti-harakatlarini tahlil qilib, shubhali faoliyat aniqlansa qo'shimcha autentifikatsiya talab qiladi yoki IP manzilni vaqtinchalik bloklaydi. Bu usul parolni buzishga qaratilgan hujumlarni samarali kamaytiradi.

Amaliy jihatdan Fail2Ban kabi vositalar server loglarini tahlil qilib, takroriy noto'g'ri login urinishlarini aniqlaydi va hujum qiluvchi IP manzillarni bloklaydi. Uni sun'iy intellekt bilan integratsiya qilish orqali yanada murakkab hujumlarni aniqlash va bartaraf etish mumkin.

DoS va DDoS hujumlarini oldini olishda esa tarmoq trafikini monitoring qilish va yuklamani boshqarish muhim ahamiyatga ega. AI tizimlari trafikdagi keskin o'zgarishlarni aniqlab, shubhali manbalarni bloklaydi yoki yuklamani balanslaydi. Bu esa xizmatlarning uzluksiz ishlashini ta'minlaydi.

Shuningdek, sun'iy intellekt proaktiv himoyani ta'minlash imkonini beradi. Tizimlar kelajakdagi tahdidlarni bashorat qilib, oldindan himoya choralari ishga tushiradi. Bundan tashqari, SOAR kabi avtomatlashtirilgan xavfsizlik tizimlari orqali hujum aniqlangach, darhol choralar ko'riladi, masalan, firewall qoidalarini yangilash yoki zararli IP manzillarni bloklash.

AI yordamida zaifliklarni aniqlash va ularni bartaraf etish ham mumkin. Tizimlar infratuzilmani tahlil qilib, xavfsizlikdagi kamchiliklarni aniqlaydi va ularni tuzatish bo'yicha tavsiyalar beradi.

Biroq, AI tizimlarining ayrim cheklovlari ham mavjud. Masalan, noto‘g‘ri sozlash natijasida normal foydalanuvchilar bloklanishi mumkin yoki tizim katta hisoblash resurslarini talab qiladi. Shunga qaramay, sun‘iy intellekt yordamida kiberhujumlarni oldini olish zamonaviy kiberxavfsizlikning muhim yo‘nalishlaridan biri hisoblanadi.

### SSH uchun Fail2Ban ni qanday sozlash mumkin

Fail2Ban konfiguratsiyasi asosan uning **jail fayllari** atrofida aylanadi . Fayl standart sozlamalarni o‘z ichiga oladi, ammo maxsus konfiguratsiyalar uchun xizmatga xos fayllardan jail.conf foydalanish eng yaxshi amaliyotdir .jail.local.local.

```
[DEFAULT]

# =====
# Fail2Ban Global Settings
# =====

# IP addresses or networks to ignore (never ban).
# Add your trusted subnets and management IPs here.
ignoreip = 127.0.0.1/8 ::1 192.168.178.0/24

# Duration for which an IP is banned after exceeding maxretry attempts.
# Format examples: s (seconds), m (minutes), h (hours), d (days)
bantime = 1h

# Time window within which maxretry failures must occur to trigger a ban.
findtime = 10m

# Number of failed attempts before an IP gets banned.
maxretry = 3

# Backend used to read logs.
# 'systemd' is recommended for modern systems using journalctl.
backend = systemd

# Control DNS usage in logs and actions.
# Options: yes | warn | no
# 'warn' tries to resolve but continues if it fails.
usedns = warn

# =====
# Ban Action Configuration
# =====

# Action to take when a rule is triggered.
%(action_mwl)s:
# - Ban the IP
# - Send an email with whois info and relevant logs
action = %(action_mwl)s
```

### 1-rasm. Global standart sozlamalar fayli –/etc/fail2ban/jail.local

```
[sshd]

# =====
# SSH Jail Configuration
# =====

# Enable the SSH jail to monitor and protect against brute-force attacks.
enabled = true

# Port fail2ban should monitor for SSH connections.
# If you run SSH on a custom port, replace 'ssh' with the actual port number (e.g., 2222).
port = ssh

# Filter definition to use.
# 'sshd' refers to the default filter that matches common SSH authentication failures.
filter = sshd

# Log file location.
# '%(sshd_log)s' uses the default value set by the system, typically /var/log/auth.log or journalctl.
logpath = %(sshd_log)s

# Backend for reading logs.
# 'systemd' is recommended if your system uses journalctl for logging.
backend = systemd

# =====
# SSH-Specific Overrides
# =====

# Time window to evaluate failed login attempts.
# If 'maxretry' failures occur within this time, the IP will be banned.
findtime = 5m

# Number of failed attempts allowed before triggering a ban.
maxretry = 4
```

### 2-rasm. SSH-ga xos sozlamalar fayli –/etc/fail2ban/jail.d/sshd.local

Konfiguratsiyalarni toza va tartibli saqlash uchun biz xuddi shu tuzilmani boshqa shunga o'xshash `nginx.local` yoki `apache.local` undan past xizmatlar uchun qo'llashingiz mumkin.

Fail2Ban konfiguratsiya fayllarini quyidagi tartibda qayta ishlaydi:

1. `/etc/fail2ban/jail.conf` (Standart sozlamalar – O'zgartirmang)
2. `/etc/fail2ban/jail.local` (Global bekor qilishlar)
3. Barcha local fayllar `/etc/fail2ban/jail.d/` (Xizmatga xos sozlamalar)

### Fail2Ban himoyasini sinovdan o'tkazish

Fail2Ban-ni o'rnatgandan so'ng, uning qo'pol kuch urinishlarini to'g'ri aniqlayotganini va kamaytirayotganini tekshirish juda muhimdir.

```
#!/bin/bash

# =====
# Fail2Ban SSH Ban Trigger Script
# =====
# This script intentionally generates failed SSH login attempts
# to test if Fail2Ban properly detects and blocks brute-force attacks.

# -----
# Target Configuration
# -----
TARGET_HOST="192.168.178.13" # IP address or hostname of the target server to test
FAKE_USER="invaliduser"      # Non-existent username to force authentication failure
ATTEMPTS=5                   # Number of failed attempts (match or exceed Fail2Ban 'maxretry' setting)

echo "Triggering Fail2Ban by attempting to SSH as user '$FAKE_USER' to $TARGET_HOST"

# -----
# Brute-Force Simulation Loop
# -----
for i in $(seq 1 $ATTEMPTS); do
    echo "Attempt $i..."
    ssh \
        -o PreferredAuthentications=password \ # Force password authentication (skip public key)
        -o PubkeyAuthentication=no \           # Disable public key authentication entirely
        -o StrictHostKeyChecking=no \          # Avoid host key verification prompts
        -o ConnectTimeout=5 \                  # Limit each connection attempt to 5 seconds
        "$FAKE_USER@$TARGET_HOST" exit        # Attempt to connect and immediately exit if successful (won't be)
done

# -----
# Final Status Message
# -----
echo "Done. Check Fail2Ban status on the target server using:"
echo "  sudo fail2ban-client status sshd"
```

3-rasm. Muvaffaqiyatsiz SSH loginlarini simulyatsiya qilish uchun oddiy skript

Fail2Ban holatini tekshirish buyrug'i: `sudo fail2ban-client status sshd`

Misol chiqishi:

```
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 5
| `-- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`-- Actions
    |- Currently banned: 1
    |- Total banned: 1
    `-- Banned IP list: 192.168.178.11
```

Taqiq muddati tugashidan oldin IP-ni qo'lda blokdan chiqarish uchun:

`sudo fail2ban-client status sshd unbanip 192.168.178.11`

### Natijalar va tahlil

Mazkur tadqiqot doirasida generativ sun'iy intellekt asosidagi kiberhujumlarni aniqlash va oldini olish usullarining samaradorligini baholash maqsadida amaliy tajribalar o'tkazildi. Tajriba VirtualBox muhitida tashkil etilib, unda Kali Linux hujumchi, Windows Server 2022 esa himoyalalanuvchi tizim sifatida ishlatildi. Ushbu muhit orqali real sharoitga yaqin tarmoq modeli yaratilib, turli hujum ssenariylari sinovdan o'tkazildi.

Tajriba davomida asosiy e'tibor brute-force hujumlarini aniqlashga qaratildi. Kali Linux orqali serverga ko'p marotaba login urinishlari amalga oshirilib, bu jarayon server loglarida qayd etildi. Windows Server tomonida firewall sozlamalari faollashtirilib, ko'p sonli so'rovlar cheklab qo'yildi. Bu esa hujumlarning samaradorligini kamaytirishga yordam berdi.

Log fayllarni tahlil qilish orqali shubhali faoliyat aniqlanib, ko'p marotaba muvaffaqiyatsiz login urinishlari kuzatilgan IP manzillar bloklandi. Ushbu yondashuvni sun'iy intellekt bilan integratsiya qilish orqali yanada samarali natijalarga erishish mumkinligi aniqlandi.

Tajriba natijalari shuni ko'rsatdiki, AI asosidagi tizimlar an'anaviy usullarga nisbatan samaraliroq bo'lib, katta hajmdagi ma'lumotlarni tezkor tahlil qilish va noodatiy faoliyatni aniqlash imkonini beradi. Bu esa hujumlarni erta bosqichda aniqlash va oldini olishga yordam beradi. Shuningdek, tarmoq trafikini monitoring qilish orqali DoS hujumlariga o'xshash holatlar aniqlanib, avtomatik cheklovlar qo'llanildi. Foydalanuvchi xatti-harakatlarini tahlil qilish orqali esa noodatiy faoliyatlar aniqlanib, ichki tahdidlarni ham aniqlash mumkinligi kuzatildi. Biroq, tajriba davomida ayrim kamchiliklar ham aniqlandi. Jumladan, ba'zi hollarda tizim normal faoliyatni ham xavf sifatida baholashi (false positive) mumkin. Bu esa AI tizimlarini yanada takomillashtirish zarurligini ko'rsatadi.

### **Xulosa**

Tadqiqot natijalari shuni ko'rsatdiki, sun'iy intellekt, xususan generativ AI texnologiyalari kiberxavfsizlik sohasida yangi imkoniyatlar yaratadi. Ushbu texnologiyalar katta hajmdagi ma'lumotlarni tezkor tahlil qilish, yashirin qonuniyatlarni aniqlash va potentsial tahdidlarni oldindan bashorat qilish imkonini beradi. Bu esa kiberhujumlarni erta bosqichda aniqlash va ularning oldini olishda muhim rol o'ynaydi.

Generativ sun'iy intellekt texnologiyalarini kiberxavfsizlik tizimlariga joriy etish zamonaviy axborot tizimlarini himoya qilishning eng istiqbolli yo'nalishlaridan biri hisoblanadi. Ushbu yondashuvlar yordamida tizimlarning ishonchliligi, barqarorligi va xavfsizlik darajasini sezilarli darajada oshirish mumkin. Shu sababli, kelgusida ushbu yo'nalishda ilmiy tadqiqotlarni kengaytirish va amaliyotga joriy etish muhim vazifalardan biri bo'lib qoladi.

### *Foydalanilgan adabiyotlar*

1. Goodfellow I. et al. Deep learning. – Cambridge : MIT press, 2016. – T. 1. – №. 2. – C. 1-800..
2. Stallings W. Network security essentials: applications and standards //(No Title). – 2014.
3. Kaspersky Lab. (2023). *Cybersecurity and AI: Threats and Opportunities*. Veb sayt: <https://www.kaspersky.com> (murojaat vaqti: 05.04.2026y.)
4. IBM Security. (2023). *AI in Cybersecurity Report*. Veb sayt: <https://www.ibm.com/security> (murojaat vaqti: 05.04.2026y.)
5. Cisco Systems. (2022). *Network Security and Artificial Intelligence*. Veb sayt: <https://www.cisco.com> (murojaat vaqti: 05.04.2026y.)
6. OpenAI. (2023). *Generative AI and Security Implications*. Veb sayt: <https://openai.com> (murojaat vaqti: 05.04.2026y.)
7. Metta S. et al. Generative AI in cybersecurity //arXiv preprint arXiv:2405.01674. – 2024.
8. Alqahtani H., Kumar G. A comprehensive review of generative AI techniques and their impact on cybersecurity //Soft Computing. – 2025. – T. 29. – №. 13. – C. 4945-4982.