Süni İntellekt Əsaslı Kiberhücumların Cinayət Məsuliyyətinin Müəyyənləşdirilməsi Problemləri

Ələddin Ağayev
Daxili İşlər Nazirliyinin Polis Akademiyası, Bakı, Azərbaycan
aladdinagayev2002@gmail.com

Xülasə— **İnformasiya-kommunikasiya sistemlərinin meydana gəlməsi və geniş yayılması zamanla həmin sistemlərdən cinayətkar məqsədlərlə istifadə edilməsinə səbəb olmuşdur. Bu gün süni intellekt texnologiyalarının insan həyatının müxtəlif sahələrində tətbiqi müsbət dəyişikliklərə səbəb olsa da, bəzi şəxslər bu texnologiyalardan qeyri-qanuni əməllərin törədilməsi üçün vasitə kimi istifadə edirlər. Məqalədə süni intellekt texnologiyalarından qanunsuz məqsədlərlə istifadə olunmasına, eləcə də belə texnologiyalara əsaslanan kiberhücumların törədilməsinə görə cinayət məsuliyyətinin müəyyənləşdirilməsi problemləri araşdırılır.**

Açar sözlər— süni intellekt; kiberhücum; kibercinayət; “deepfake”; cinayət məsuliyyəti.

I. GİRİŞ

Hər il kiberhücumlar qlobal və ölkə miqyasında artmaqdadır. Əvvəlki dövrlərdən fərqli olaraq artıq primitiv zərərverici viruslardan deyil, daha mürəkkəb və dağıdıcı təsirə malik texnologiyalardan istifadə olunur. Elmi ədəbiyyatda kiberhücumlar müxtəlif meyarlara görə təsnifatlaşdırılır ki, belə bölgülər nisbi xarakter daşıyır. Ümumilikdə, kiberhücumları əsaslarına görə aşağıdakı növlərə ayırmaq olar:

İnsan tərəfindən idarə olunan hücumlar (Human-operated attack), başqa sözlə, insan faktoruna əsaslanan kiberhücumlar - avtomatlaşdırılmış alətlər əvəzinə insanların özlərinin müdaxiləyə birbaşa nəzarət etdiyi, çox vaxt taktikanın real-vaxtda dəyişdirildiyi kiberhücum növü [1].

Kompüter əsaslı kiberhücumlar – DDoS, MITM, Ransomware və s. kiberhücum növlərini aid etmək olar ki, belə hücumlar kompüter sistemlərinin və şəbəkələrinin zəifliklərindən istifadə etməklə onların bloklanmasına, şifrələnməsinə və zədələnməsinə yönəlmişdir.

Süni intellekt əsaslı kiberhücumlar – son zamanlar süni intellekt alətlərinin geniş yayılması ilə əlaqədar cinayətkarlar tərəfindən müxtəlif növ cinayətlərin törədilməsində bu hücumlardan istifadə olunur. Məsələn, "deepfake" texnologiyasına əsaslanan dələduzluq

II. BEYNƏLXALQ TƏCRÜBƏDƏ SÜNİ İNTELLEKT TEXNOLOGİYALARINDAN CİNAYƏTKAR MƏQSƏDLƏRDƏ İSTİFADƏ

İnsan faktoruna əsaslanan hücumlar sosial mühəndisliyin müxtəlif növlərini özündə birləşdirir. Belə ki, Avropa İttifaqının Kibertəhlükəsizlik Agentliyinin (ENISA) 2023-cü il hesabatına əsasən, süni intellekt texnologiyalarının inkişafı sosial mühəndislik hücumlarının əhəmiyyətli dərəcədə artmasına səbəb olmuşdur. Bundan əlavə, Avropol "ChatGPT" kimi süni intellekt əsaslı çatbotlardan fişinq, informasiya manipulyasiyası və digər kibercinayətlərdə sui-istifadə olunması barədə xəbərdarlıq etmişdir. Süni intellekt texnologiyalarından olan “ChatGPT”nin cəmiyyətə təqdim edilməsi böyük ictimai diqqət qazanmışdır. Lakin öz növbəsində insan ünsiyyətini təqlid etmək qabiliyyətinə görə o, yeni növ sosial mühəndislik texnikaları üçün tamamilə geniş imkanlar yaratmışdır. Həmin hesabata əsasən, süni intellekt texnologiyaları hazırda əsasən aşağıdakı üç istiqamətdə cinayətkar məqsədlərlə istifadə olunur:

1. Daha inandırıcı fişinq e-poçtlarının və mesajlarının hazırlanması;
2. Səs klonlama üzərində fokuslanan “deepfake” texnologiyaları;
3. Süni intellekt tərəfindən idarə olunan məlumatların analiz edilməsi və çıxarılması [2].

Süni intellekt alətlərinə əsaslanan kiberhücum növlərindən olan “deepfake” son zamanlar həm dünyada, həm də ölkəmizdə geniş yayılmaqdadır. Süni intellekt əsaslı “deepfake” dedikdə, süni intellekt tərəfindən yaradılan və real insanları və ya hadisələri inandırıcı şəkildə təqlid edən audio, video və ya foto görüntülər başa düşülür. Bu texnologiya şəxsləri imitasiya etmək, saxta ssenarilər yaratmaq və ya ictimai rəyin manipulyasiyası üçün istifadə oluna bilər və çox vaxt da dələduzluq, yanlış məlumatlandırma və ya dezinformasiyanın yayılmasına səbəb olur [1].

Dünyada və ölkəmizdə baş vermiş süni intellekt texnologiyalarına əsaslanan hücum faktlarına nəzər yetirək.

Böyük Britaniyada yerləşən enerji şirkətinin Almaniyadakı əməliyyatlarının icraçı direktoru (CEO) süni intellekt əsaslı “deepfake” səs texnologiyası vasitəsilə təqlid edilmiş və nəticədə şirkət 243000 ABŞ dolları məbləğində dələduzluğa məruz qalmışdır. Həmin şirkətin Böyük Britaniyadakı “CEO”su Almaniyadakı həmkarı tərəfindən ona pulun Macarıstandakı bir təchizatçıya köçürülməsi barədə müraciət edildiyini düşünmüş və dərhal bu köçürməni həyata keçirmişdir. Şirkətin sığortaçısı olan “Euler Hermes Group”un məlumatına görə, dələduz çox güman ki, bu fırıldaqçılığı həyata keçirmək üçün kommersiya məqsədli mövcud olan süni intellekt əsaslı səs yaradıcı proqram təminatından istifadə etmişdir. Bu hadisə göstərdi ki, artıq başqasının səsini klonlaşdırmaq və bundan istifadə edərək dələduzluq və ya digər məqsədlərlə sui-istifadə etmək çox asanlaşmışdır [3].

DOI: 10.25045/forensic.gov.2026.80

III. AZƏRBAYCAN RESPUBLİKASINDA SÜNİ İNTELLEKT ƏSASLI KİBERHÜCUMLARIN CİNAYƏT-HÜQUQİ TƏNZİMİ

Operativ Məlumat Mərkəzinin 13 mart 2026-cı il tarixli məlumatına əsasən, ölkəmizdə sosial şəbəkələrdə qadınlara qarşı şantaj hallarına yönəlmiş yeni kiberəməliyyatlar həyata keçirilmişdir. Belə ki, Daxili İşlər Nazirliyinin Kibercinayətkarlıqla Mübarizə Baş İdarəsi vətəndaşların foto və videolarını təhrif edərək təhqiredici formaya salmaqda və onların silinməsi üçün pul tələb etməkdə təqsirləndirilən şəxsi saxlayıb. Müəyyən olunub ki, 21 yaşlı M.Atakişiyev qadınlara məxsus foto və videomaterialları "TikTok", "Instagram" və "Telegram" platformalarından əldə edib. Bu hadisə "deepfake" texnologiyası və süni intellektdən istifadə edilərək həyata keçirilən şantajın qlobal miqyasda artan təhlükə olduğunu bir daha göstərir [4].

Beləliklə, hər iki hadisədən göründüyü kimi süni intellekt texnologiyalarının inkişafı cinayətkarlığın yeni üsul və formalarının meydana gəlməsinə zəmin yaradır.

Süni intellekt texnologiyalarının qanunsuz məqsədlərlə istifadə olunması hallarında əsas məsələ hüquqi tənzimləmə mexanizminin, eləcə də törədilmiş əməllərə görə qanunvericiliklə nəzərdə tutulmuş məsuliyyətin müəyyənləşdirilməsi ilə bağlıdır.

"JAMnews" tərəfindən 13 mart 2026-cı ildə verilmiş məlumata əsasən, Azərbaycanda süni intellektlə bağlı müzakirələr artıq yalnız innovasiya mövzusu ilə məhdudlaşmır Belə ki, bu məsələ getdikcə informasiya və şəxsi təhlükəsizlik probleminə çevrilir. Milli Məclisdə "rəqəmsal klonlaşdırma" və "deepfake" texnologiyaları sahəsində qanunvericilik boşluğunun mövcudluğu bildirilmişdir. Hansı ki, mövcud mexanizmlər bu risklərlə effektiv mübarizənin aparılmasına imkan vermir. "Deepfake" texnologiyalarına sadə şəkildə aşağıdakı məzmunda anlayış verilmişdir:

"Süni intellekt insanın üzünü, səsini və davranışını təqlid edir. Daha sonra isə real kimi görünən saxta video və ya audio materiallar yaradır".

Bu texnologiyaların əsasən üç istiqamətdə istifadə olunması vurğulanmışdır:

1. Xüsusilə qadınlara qarşı saxta intim görüntülərin yaradılması ilə nüfuza zərər vurulması və ya şantaj;
2. Səs klonlaşdırılması ilə pul tələb edilməsi kimi dələduzluq halları;
3. Dövlət və ictimai xadimlərə və ya tanınmış şəxslərə aid saxta bəyanatlarla ictimai və siyasi manipulyasiya [5].

Beləliklə, süni intellekt texnologiyalarının cinayətkar məqsədlərlə istifadə olunması ilə bağlı Azərbaycan Respublikası kontekstində mövcud problemləri aşağıdakı qaydada qruplaşdırmaq olar:

1. Süni intellekt texnologiyalarının tətbiqi sahələrini müəyyənləşdirən, eləcə də onlardan istifadəni hüquqi cəhətdən nizamlayan konkret normativ hüquqi aktların olmaması;
2. Qeyri-qanuni məqsədlərlə süni intellekt alətlərinin hazırlanması zamanı qanunvericilikdə konkret məsuliyyətin müəyyənləşdirilməməsi;
3. Süni intellektin cinayətin subyekti hesab edilib-edilməməsi.

Ən əvvəl qeyd etmək lazımdır ki, ölkəmizdə süni intellektin cinayətin subyekti kimi tanınması məsələsinə Cinayət Məcəlləsinin 19-cu maddəsinin məzmunundan irəli gələrək cavab vermək mümkündür. Belə ki, Cinayət Məcəlləsi ilə müəyyən olunmuş yaş həddinə çatmış və cinayət törətmiş anlaqlı şəxs cinayət məsuliyyətinə cəlb edilir [6]. Süni intellekt texnologiyalarında qeyd olunan iki əlamət, yəni anlaqlılıq və yaş faktoru istisna edildiyi üçün, süni intellekt cinayətin subyekti hesab edilə bilməz. Düzdür, Elmi ədəbiyyatda bəzi müəlliflər süni intellektin cinayət məsuliyyətini hüquqi şəxslərlə bərabər tuturlar. Süni intellektin cinayət məsuliyyətinin müəyyənləşdirilməsi ilə bağlı Səudiyyə Ərəbistanın Əl-Cövf Universitetinin müəllimi Alaa Saudun mövqeyilə razılaşmaq olar. O qeyd edir ki, süni intellekt texnologiyası sürətlə inkişaf etdiyinə görə, cəmiyyətin bu texnologiyanın cinayət hüququ tərəfindən icazə verilməyən təhlükələrindən qorunması üçün mövcud hüquqi vasitələrin təkmilləşdirilməsinə ehtiyac var. Bundan başqa, mövcud cinayət hüququ süni intellekt problemini həll etmək üçün bir çox yanaşma təqdim edir və süni intellekt sistemlərinin yaratdığı məsuliyyət məsələləri ənənəvi cinayət hüququnun sərhədlərini genişləndirir. Nəticə etibarilə, süni intellektin törətdiyi hərəkətlərə görə cavabdeh şəxslər məsuliyyət daşımalıdırlar, çünki yaranan zərərin əvvəlcədən proqnozlaşdırılması mümkün olan yeganə subyektlər məhz onlardır [7]. Beləliklə, vurğulamaq lazımdır ki, süni intellekt cinayətin subyekti ola bilməz, o sadəcə cinayətin aləti kimi qəbul edilə bilər.

Ölkəmizdə süni intellekt texnologiyalarının tətbiqini hüquqi cəhətdən nizamlayan əsas tənzimləyici sənəd 19 mart 2025-ci il tarixində Azərbaycan Respublikası Prezidentinin Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasının 2025–2028-ci illər üçün süni intellekt Strategiyası"dır. Həmin Strategiyanın 2-ci bəndinə əsasən, qurumlar yaratdıqları və istifadə etdikləri süni intellekt sistemlərinə görə cavabdeh olmalı və məsuliyyət daşımalıdırlar [8]. Lakin hansı formada məsuliyyət daşıması, eləcə də məsuliyyət müəyyən edən konkret normalar qanunvericilik sistemində nəzərdə tutulmamışdır. Mövcud vəziyyətin təhlili ona əsas verir ki, süni intellekt üzrə mütəxəssislərin və peşəkar kadrların artması gələcəkdə bu sahədə cinayətlərin törədilməsini qaçınılmaz edir.

Bu gün dünyada cinayət məqsədləri üçün süni intellekt texnologiyalarından istifadə marağı artır. Bu texnologiyalar cinayət şəbəkələrinə daha mürəkkəb təxribat ssenariləri hazırlamağa imkan verir [9]. Qeyd olunduğu kimi, süni intellekt alətlərindən istifadə etməklə törədilən cinayətlərin dinamik inkişafı öz növbəsində belə əməllərə görə cinayət məsuliyyətinin müəyyənləşdirilməsi məsələsini aktuallaşdırır. Xüsusilə vurğulamaq lazımdır ki, Azərbaycan Respublikasının Cinayət Məcəlləsində nəzərdə tutulmayan əməlin törədilməsinə görə cinayət məsuliyyəti yarana bilməz. Bəs onda hər hansı şəxs cinayətkar məqsədlərlə süni intellekt texnologiyaları hazırladığı və ya həmin texnologiyalardan istifadə etməklə kiberhücumlar törətdiyi halda cinayət məsuliyyəti necə həll olunmalıdır?

Azərbaycan Respublikasının Cinayət Məcəlləsinin 178-ci maddəsinin (Dələduzluq) məzmunundan irəli gələrək qeyd

etmək lazımdır ki, cinayətkarlar aldatma və ya etibardan sui-istifadə etməklə özgə əmlakının ələ keçirilməsinə və ya əmlak hüquqlarının əldə olunmasına nail olurlar. Belə ki, süni intellekt texnologiyalarından olan deepfak texnologiyası cinayətkarlara hədəf kimi seçdikləri şəxsi (şəxsləri) aldatmağa yeni imkanlar verir. Ənənəvi dələduzluq halları ilə müqayisədə "deepfake" dələduzluğu bir sıra xüsusiyyətlərinə görə fərqlənir:

1. Süni intellekt texnologiyalarına əsaslanır;
2. Törədilmə yeri kibermәkanı əhatə edir;
3. Cinayətin qurbanı istənilən şəxs ola bilər, yəni qeyri-müəyyən şəxslər dairəsini hədəf alır;
4. Qlobal və ölkə miqyasında dinamik inkişafdadır.

NƏTİCƏ

Mövcud cinayət-hüquqi mexanizmlər süni intellekt əsaslı kiberhücumların cinayət məsuliyyətinin müəyyənləşdirilməsi tələblərinə cavab vermədiyi üçün qeyd olunan istiqamətdə qanunvericiliyin təkmilləşdirilməsinə ehtiyac vardırr. Bu məqsədlə, Azərbaycan Respublikasının Cinayət Məcəlləsinin 178-ci maddəsinin 2-ci hissəsinə aşağıdakı məzmunlu yeni bəndin əlavə edilməsini tövsiyə edirik:

Təklif olunan redaksiya**:** Eyni əməllər süni intellekt texnologiyalarından istifadə etməklə törədildikdə.

Bundan başqa, süni intellekt texnologiyalarını cinayətkar məqsədlər üçün hazırlayan aidiyyəti şəxslər barəsində cinayət məsuliyyətinin müəyyənləşdirilməsi üçün Azərbaycan Respublikasının Cinayət Məcəlləsinə aşağıdakı məzmunlu 273-3-cü maddənin əlavə edilməsinə zərurət vardır:

Təklif olunan redaksiya: Hazırlanmasının və ya uyğunlaşdırılmasının əsas məqsədi bu Məcəllənin müvafiq maddələrində nəzərdə tutulmuş cinayətlərin törədilməsi olan süni intellekt texnologiyalarının istehsalı, həmin cinayətlərin törədilməsi məqsədilə idxalı, istifadə üçün əldə olunması, saxlanılması, satışı, yayılması və ya əldə edilməsinə digər formalarda şərait yaradılması əhəmiyyətli zərər vurduqda.

Sonuncu təklif olunan əməlin Cinayət Məcəlləsinə əlavə edilməsi süni intellekt texnologiyalarının qanunsuz məqsədlərlə hazırlanması istiqamətində öz profilaktik təsirini göstərəcəkdir. Eyni zamanda qanunvericilik sistemində mövcud olan hüquqi tənzimləmə mexanizminin boşluğu aradan qaldırılmış olacaqdır.

ƏDƏBİYYAT

[1] ENISA, ENISA Threat Landscape 2023.

[2] Microsoft, Microsoft Digital Defense Report 2025 – Safeguarding Trust in the AI Era.

[3] AI, Algorithmic and Automation Incidents and Controversies Repository (AIAAIC), Fraudsters clone CEO voice to steal USD 243,000.

[4] Operativ Məlumat Mərkəzi, Azerbaijan arrests suspect in AI-driven blackmail case, 13 March 2026.

[5] JAMnews, Azərbaycanda süni intellekt və deepfake texnologiyaları ilə bağlı qanunvericilik boşluğu haqqında xəbər, 13 mart 2026.

[6] Azərbaycan Respublikasının Cinayət Məcəlləsi, 30 dekabr 1999-cu il, № 787-IQ (23 fevral 2024-cü il tarixli dəyişikliklərlə).

[7] A. Saud, "Criminal Liability about the Use of Artificial Intelligence: Investigating the Actus Reus Element of AI-driven Technology," American Journal of Law, vol. 6, pp. 1–25, 2023.

[8] Azərbaycan Respublikasının Prezidentinin 19 mart 2025-ci il tarixli Sərəncamı ilə təsdiq edilmiş Azərbaycan Respublikasının 2025–2028-ci illər üçün Süni İntellekt Strategiyası.

[9] D. Rustamov: Scale of crimes involving AI rapidly increasing. https://report.az/en/domestic-politics/davud-rustamov-scale-of-crimes-involving-ai-rapidly-increasing

Problems of Determining Criminal Liability for AI-Based Cyber Attacks

Aladdin Aghayev

Police Academy of the Ministry of Internal Affairs, Baku, Azerbaijan

aladdinagayev2002@gmail.com

Abstract - The emergence and widespread adoption of information and communication systems have, over time, led to their use for criminal purposes. Although the application of artificial intelligence technologies in various spheres of human life has resulted in positive developments, certain individuals exploit these tools as a means of committing unlawful acts. This article examines the challenges associated with determining criminal liability for the illegal use of artificial intelligence technologies, as well as for the perpetration of cyberattacks based on such technologies

Keywords - artificial intelligence; cyberattack; cybercrime; deepfake; criminal liability**.**