Rəqəmsal Mühitdə Kibercinayətkarlığın Həyata Keçirilməsi Mexanizmləri və Texnologiyalarının Təhlili

Təhmasib Fətəliyev[1], Şakir Mehdiyev[2]
[1, 2] İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*depart_5@iit.science.az,* [2] *shakir.mehtieff@gmail.com*

Xülasə– **Məqalədə rəqəmsal mühitdə istifadə olunan müasir kibercinayətkarlıq metodları, mexanizmləri və texnologiyaları araşdırılır. Kiberhücumların əsas metodları, o cümlədən zərərli proqram təminatının istifadəsi, nformasiya sistemlərində mövcud zəifliklərdən istifadə və sosial mühəndislik metodları araşdırılır. Kibercinayətkarlıq fəaliyyətində istifadə olunan texnoloji vasitələrin təhlili, eləcə də onların həyat dövrünün müxtəlif mərhələlərində hücumların həyata keçirilməsi mexanizmləri araşdırılmışdır.**

Açar sözlər– kibercinayətkarlıq; kiberhücumlar; zərərli proqram təminatı; sosial mühəndislik; rəqəmsal texnologiyalar; kibertəhdidlər.

I. GİRİŞ

Rəqəmsal texnologiyaların sürətli inkişafı və iqtisadiyyatın müxtəlif sahələrinin, eləcə də dövlət idarəçiliyinin geniş miqyasda rəqəmsallaşması informasiya sistemlərini müasir cəmiyyətin əsas infrastruktur komponentlərindən birinə çevirmişdir. Şəbəkə texnologiyalarının, bulud hesablamalarının, mobil platformaların və rəqəmsal xidmətlərin geniş miqyasda tətbiqi böyük həcmli məlumatların emalı və ötürülməsi üçün mürəkkəb və paylanmış sistemlərin formalaşmasına səbəb olmuşdur.

Rəqəmsal transformasiyanın dərinləşməsi ilə yanaşı, informasiya sistemlərinə və rəqəmsal platformalara yönəlmiş kibertəhdidlərin miqyası və mürəkkəbliyi də xeyli dərəcədə artmışdır. Xüsusilə dövlət informasiya sistemləri, maliyyə institutları, korporativ şəbəkələr və kritik infrastruktur obyektləri hazırkı kiberhücumların əsas hədəflərinə çevrilmişdir. Rəqəmsal xidmətlərin və elektron ödəniş sistemlərinin geniş şəkildə yayılması kibermәkanda qanunsuz fəaliyyət üçün əlavə imkanlar yaradır [1].

Süni intellekt (Sİ), böyük verilənlər, bulud hesablamaları və Əşyaların İnterneti (Əİ) kimi texnologiyaların intensiv tətbiqi müasir sosial-iqtisadi sistemlərin arxitekturasını yenidən formalaşdırır. Bu texnologiyalar eyni zamanda onların rəqəmsal infrastrukturdan asılılığını artırır. Bu isə paylanmış sistemlərin mürəkkəbliyi, texnoloji platformaların heterojenliyi və təhlükəsizlik mexanizmlərinin yetərli səviyyədə olmaması səbəbindən yeni zəifliklərin yaranmasına gətirib çıxarır. Nəticədə, kiberhücumların miqyası artır və onlar həm informasiya sistemlərini, həm də kiber-fiziki sistemləri əhatə edir.

Müasir kibercinayətkarlıq yüksək səviyyədə texnoloji mürəkkəblik, uyğunlaşma qabiliyyəti və avtomatlaşdırma ilə xarakterizə olunur. Hücumçular zəifliklərin avtomatlaşdırılmış aşkarlanması, zərərli proqram təminatının yaradılması və sosial mühəndislik üsullarının tətbiqi vasitəsilə hədəfli hücumların effektivliyini artırırlar. Eyni zamanda, kibertəhdidlər getdikcə transmilli xarakter alır ki, bu da onların aşkarlanmasını, mənbəyinin müəyyən edilməsini və hüquqi tənzimlənməsini çətinləşdirir.

Mövcud tədqiqatlar göstərir ki, Sİ və avtomatlaşdırma texnologiyalarının tətbiqi kiberhücumların həyata keçirilmə mexanizmlərini əhəmiyyətli şəkildə təkmilləşdirir və onların effektivliyini artırır [2, 3]. Bu şəraitdə kibercinayətkarlığın metodlarının, mexanizmlərinin və istifadə olunan texnologiyaların sistemli şəkildə öyrənilməsi xüsusi aktuallıq kəsb edir.

Bu tədqiqatın məqsədi rəqəmsal transformasiya kontekstində kibercinayətkarlıq metodlarını təhlil etmək, kiberhücumların həyata keçirilmə mexanizmlərini sistemləşdirmək və kibercinayətkarlıqda istifadə olunan müasir texnologiyaları ümumiləşdirməkdir.

İşin elmi yeniliyi kibercinayətkarlığın metodları, mexanizmləri və texnologiyaları arasında qarşılıqlı əlaqələri əks etdirən üçsəviyyəli inteqrasiya olunmuş konseptual modelin təklif edilməsidir. Bu model kiberhücumların formalaşma və həyata keçirilməsi proseslərini sistemli şəkildə təsvir etməyə və onların daha dəqiq təhlilinə imkan verir.

Təklif olunan model çərçivəsində metodlar, mexanizmlər və texnologiyalar arasında qarşılıqlı əlaqələr sistemli şəkildə nəzərdən keçirilir. Bu yanaşma kiberhücumların formalaşma və həyata keçirilməsi proseslərini daha dərindən başa düşülməsinə və onların kompleks təhlilinə imkan yaradır.

II. ƏLAQƏLİ İŞLƏR

Elmi ədəbiyyatın cari təhlili göstərir ki, kibercinayətkarlıq problemi informasiya təhlükəsizliyi, kompüter elmləri və rəqəmsal kriminalistika sahələrinin kəsişməsində formalaşan kompleks və çoxşaxəli tədqiqat istiqamətidir. Mövcud işləri şərti olaraq bir neçə əsas istiqamət üzrə qruplaşdırmaq olar.

Birinci istiqamət rəqəmsal transformasiya şəraitində kibertəhdidlərin təkamülünün öyrənilməsini əhatə edir. Sənaye 4.0, bulud texnologiyaları və paylanmış sistemlərin inkişafı

DOI: 10.25045/forensic.gov.2026.25

kiberhücumların strukturuna və xarakterinə birbaşa təsir göstərir [4, 5]. Bu tədqiqatlarda vurğulanır ki, müasir kibertəhdidlər yalnız texniki zəifliklərə deyil, həm də mürəkkəb sistem inteqrasiyası problemlərinə əsaslanır və nəticədə hücum səthi xeyli genişlənir.

İkinci istiqamət Sİ və maşın öyrənməsi metodlarının kibertəhlükəsizlikdə tətbiqinə yönəlmişdir. [6] və [7]-də təqdim olunan yanaşmalar göstərir ki, anomaliyaların aşkarlanması, şəbəkə trafikinin təhlili və müdaxilələrin identifikasiyası sahəsində maşın öyrənməsi alqoritmləri ənənəvi metodlarla müqayisədə daha yüksək dəqiqlik təmin edir. Bununla belə, bu işlərdə qeyd olunur ki, modellərin effektivliyi təlim verilənlərinin keyfiyyətindən və hücum ssenarilərinin müxtəlifliyindən əhəmiyyətli dərəcədə asılıdır ki, bu da real mühitdə tətbiq zamanı məhdudiyyətlər yaradır.

Üçüncü istiqamət kiberhücum metodları və zərərli proqramların təhlilini əhatə edir. [8]-də klassik və yeni nəsil proqram növləri sistemləşdirilir və onların yayılma mexanizmləri araşdırılır. Nəticələr göstərir ki, bu tip proqramlar yüksək uyğunlaşma qabiliyyəti və inkişaf etmiş gizlənmə mexanizmləri ilə xarakterizə olunur ki, bu da onların aşkarlanmasını və qarşısının alınmasını çətinləşdirir.

Bununla yanaşı, mövcud tədqiqatların əksəriyyəti ya texnoloji aspektlərə (məsələn, Sİ əsaslı aşkarlama metodları), ya da ayrı-ayrı hücum növlərinə fokuslanır. Kibercinayətkarlığın metodları, mexanizmləri və texnologiyalarının vahid sistem daxilində kompleks şəkildə təhlili isə kifayət qədər məhdud şəkildə təqdim olunur.

Beləliklə, aparılmış ədəbiyyat təhlili göstərir ki, kibercinayətkarlığın müxtəlif aspektləri geniş şəkildə araşdırılsa da, bu sahədə metodların, mexanizmlərin və texnologiyaların inteqrasiya olunmuş yanaşma əsasında sistemləşdirilməsi aktual elmi problem olaraq qalır və əlavə tədqiqatların aparılmasını tələb edir.

Bununla yanaşı, qeyd olunan istiqamətlərin təhlili göstərir ki, mövcud tədqiqatlarda kibercinayətkarlığın ayrı-ayrı komponentləri (metodlar, texnologiyalar və ya aşkarlama üsulları) əsas diqqət mərkəzində olsa da, onların qarşılıqlı əlaqələri və vahid sistem daxilində inteqrasiyası kifayət qədər araşdırılmamışdır. Bu isə kibercinayətkarlığın kompleks təhlilini çətinləşdirir və yeni konseptual yanaşmaların işlənməsini zəruri edir.

III. ƏSAS ANLAYIŞLAR VƏ KİBERCİNAYƏTKARLIĞIN NÖVLƏRİ

Kibercinayətkarlıq informasiya və kommunikasiya texnologiyalarından istifadə etməklə həyata keçirilən qanunsuz fəaliyyətlərin məcmusudur. Bu fəaliyyətlərin əsas məqsədi təxribat törətmək, qanunsuz qazanc əldə etmək, informasiya resurslarına icazəsiz giriş təmin etmək və ya sistemlərin fəaliyyətini pozmaqdır. Qeyd etmək lazımdır ki, kiberhücumlar bu fəaliyyətlərin həyata keçirilməsinin əsas texniki vasitələrindən biridir. Başqa sözlə, kiberhücumlar icra mexanizmi rolunu oynayır, kibercinayətkarlıq isə bu fəaliyyətin məqsəd və kontekstini müəyyən edir.

Elmi ədəbiyyatda kibercinayətkarlıq kompüter sistemlərinin, şəbəkə texnologiyalarının və rəqəmsal rabitə vasitələrinin istifadəsi ilə əlaqəli xüsusi cinayətkar fəaliyyət növü kimi qiymətləndirilir. Bu fəaliyyət həm informasiya sistemlərinin özlərini, həm də onlarda saxlanılan və emal edilən məlumatları hədəfə ala bilər [9].

Ən çox yayılmış kibercinayətkarlıq növlərinə aşağıdakılar aid edilir:

- informasiya sistemlərinə və məlumatlara qarşı cinayətlər (icazəsiz giriş, DDoS hücumları, məlumatlara müdaxilə);
- zərərli proqram təminatının yayılması (fidyə proqramları (*ransomware*) və *botnet*-lər daxil olmaqla);
- kompüter vasitəsilə fırıldaqçılıq (fişinq, maliyyə fırıldaqçılığı);
- məlumatların oğurlanması və qanunsuz istifadəsi ilə bağlı cinayətlər;
- kibercasusluq və inkişaf etmiş davamlı təhdidlər;
- kritik infrastruktura və kiberfiziki sistemlərə hücumlar;
- qanunsuz rəqəmsal məzmunla bağlı cinayətlər.

Kibercinayətkarlığın əsas xüsusiyyətlərindən biri onun qlobal xarakter daşımasıdır. Ənənəvi cinayət növlərindən fərqli olaraq, kiberhücumlar coğrafi məhdudiyyət olmadan həyata keçirilə və müxtəlif ölkələrdə yerləşən sistemləri hədəfə ala bilər.

Beləliklə, kibercinayətkarlıq mürəkkəb və dinamik inkişaf edən sahədir. O, rəqəmsal mühitdə geniş spektrli qanunsuz fəaliyyətləri əhatə edir və onun təhlili sistemli, fənlərarası yanaşma tələb edir.

IV. KİBERCİNAYƏTKARLIQ METODLARI VƏ MEXANİZMLƏRİ

A. Kibercinayətkarlıq metodları

Kibercinayətkarlıq metodları icazəsiz girişin əldə edilməsi, məlumatların oğurlanması və informasiya sistemlərinin fəaliyyətinin pozulmasına yönəlmiş texniki və davranış alətlərinin məcmusudur [10]. Bu metodlar əsasən aşağıdakı qruplara bölünür:

- sosial mühəndislik metodları (fişinq, nizə fişinqi, vişinq);
- zərərli proqram təminatı (viruslar, troyanlar, fidyə və casus proqramlar);
- zəifliklərin istismarı (sıfır gün zəiflikləri, SQL inyeksiyası, XSS);
- şəbəkə hücumları (DDoS, Man-in-the-Middle, DNS saxtakarlığı);
- APT hücumları və kibercasusluq;
- SCADA/ICS və kiberfiziki sistemlərə yönəlmiş hücumlar.

Beləliklə, kibercinayətkarlıq metodları həm texniki, həm də insan amilinə əsaslanan zəifliklərdən istifadə etməyə yönəlmiş

kompleks alətlər sistemini təşkil edir. Onların inkişafı artan avtomatlaşdırma və Sİ texnologiyalarının inteqrasiyası ilə müşayiət olunur ki, bu da hücumların miqyasını və effektivliyini artırır.

B. Kibercinayətkarlıq mexanizmləri

Kibercinayətkarlıq mexanizmləri kiberhücumların planlaşdırılması, həyata keçirilməsi və gizlədilməsini təmin edən çoxmərhələli proseslər toplusudur. Bu mexanizmlər hücum həyat dövrü modelləri (məsələn, *Cyber Kill Chain*) əsasında təsvir olunur [11-14]. Kiberhücumun əsas mərhələləri aşağıdakılardır:

- Kəşfiyyat (*reconnaissance*) – hədəf haqqında məlumatların toplanması (*Open Source Intelligence-OSINT* və aktiv skanlama vasitəsilə);
- İlkin giriş (*initial access*) – fişinq, zəiflik istismarı və ya etimadnamələrin komprometləşdirilməsi yolu ilə sistemə daxil olma;
- Davamlılıq (*persistence*) – sistemdə uzunmüddətli mövcudluğun təmin edilməsi;
- İmtiyazların artırılması (*privilege escalation*) – daha yüksək giriş hüquqlarının əldə edilməsi;
- Yan hərəkət (*lateral movement*) – şəbəkə daxilində yayılma;
- Məqsədlərə çatma (*actions on objectives*) – məlumatların oğurlanması, maliyyə əməliyyatları və ya təxribat;
- İzlərin gizlədilməsi (*anti-forensics*) – fəaliyyətin maskalanması və aşkarlamadan yayınma.

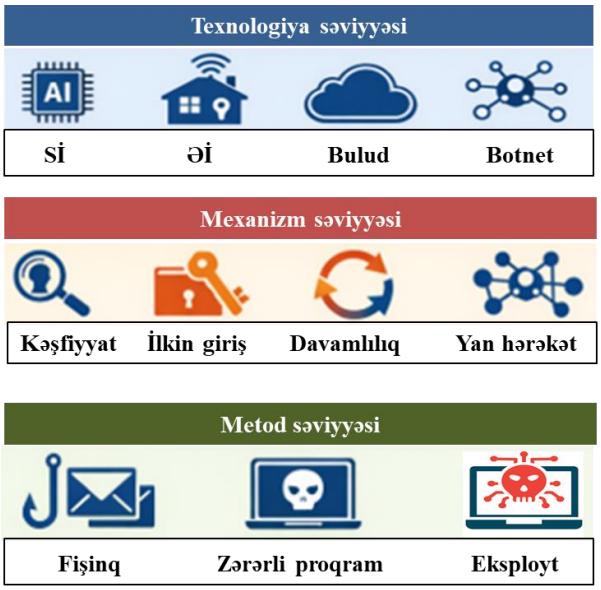
Müasir yanaşmalar göstərir ki, bu mexanizmlər yalnız xətti ardıcıllıqla deyil, həm də adaptiv və paralel şəkildə həyata keçirilə bilər. Sİ texnologiyalarının tətbiqi hücumların sürətini və effektivliyini artırmaqla yanaşı, onların aşkarlanmasını da çətinləşdirir. Bu yanaşmalar həmçinin müasir hücum davranışlarının sistemləşdirilməsini təmin edən *MITRE ATT&CK* modeli ilə uyğunluq təşkil edir [15].

Təklif olunan üçsəviyyəli model bu yanaşmaları ümumiləşdirərək metod, mexanizm və texnologiya səviyyələri arasında əlaqəni sistemləşdirir. Xüsusilə, *Cyber Kill Chain* modeli mexanizm səviyyəsində hücumun mərhələli strukturunu əks etdirir, *MITRE ATT&CK* isə konkret hücum texnikalarını metod səviyyəsində təsnif edir. Texnologiya səviyyəsi isə bu texnikaların reallaşdırıldığı mühit və alətləri əhatə etməklə modeli tamamlayır.

Beləliklə, kibercinayətkarlıq fəaliyyətini üç qarşılıqlı əlaqəli səviyyədə təsnif etmək olar:

- metod səviyyəsi – hücum alətləri və texnikaları;
- mexanizm səviyyəsi – hücumun həyata keçirilmə mərhələləri;
- texnologiya səviyyəsi – hücumların reallaşdırılmasını təmin edən platforma və vasitələr.

Bu üç səviyyə birlikdə kibercinayətkarlığın strukturlaşdırılmış konseptual modelini təşkil edir və onların qarşılıqlı əlaqəsi kiberhücumların dinamikasını və həyata keçirilmə məntiqini əks etdirir (Şəkil 1).



Şəkil 1. Kibercinayətkarlığın üçsəviyyəli konseptual modeli.

Model çərçivəsində metod səviyyəsi hücum alətlərini və texnikalarını müəyyən edir, mexanizm səviyyəsi hücumun mərhələli icra prosesini təsvir edir, texnologiya səviyyəsi isə bu proseslərin həyata keçirilməsini təmin edən texnoloji mühiti əhatə edir. Bu səviyyələr arasında qarşılıqlı təsir kiberhücumların kompleks xarakterini formalaşdırır.

Bu səviyyələr arasında qarşılıqlı əlaqələrin nəzərə alınması kiberhücumların daha dəqiq modelləşdirilməsinə və onların proqnozlaşdırılmasına imkan verir.

V. MÜASİR KİBERCİNAYƏTKARLIQ TEXNOLOGİYALARI

Müasir kibercinayətkarlıq texnologiyaları, paylanmış hesablama və rəqəmsal platformaların zəifliklərini birləşdirən mürəkkəb, çoxqatlı ekosistem təşkil edir. Əİ-nin geniş tətbiqi yeni təhlükəsizlik risklərinin yaranmasına səbəb olur, çünki bir çox cihazlar yetərli mühafizə mexanizmlərinə malik deyil.

Əİ mühitində təhlükəsizlik və rəqəmsal kriminalistika problemləri də müasir tədqiqatların əsas istiqamətlərindən biridir. Bu mühitdə sübutların toplanması, saxlanması və təhlili ilə bağlı ciddi çətinliklər mövcuddur [16].

Əsas tendensiyalardan biri kiberhücumların intellektuallaşdırılmasıdır. [17]-yə görə, hücumçular Sİ texnologiyalarından istifadə etməklə hücumun bütün mərhələlərini – kəşfiyyatdan başlayaraq gizlətməyə qədər – avtomatlaşdırırlar. Generativ modellər isə realistik fişinq mesajlarının və uyğunlaşdırılmış zərərli proqramların yaradılmasına imkan verir.

Müasir zərərli proqram təminatı polimorfizm, metamorfizm və faylsız texnologiyalar kimi xüsusiyyətlərlə xarakterizə olunur. Bu isə onların ənənəvi antivirus sistemləri tərəfindən aşkarlanmasını çətinləşdirir və qarşısının alınmasını mürəkkəbləşdirir [18]. Bundan əlavə, "kibercinayətkarlıq xidmət kimi" modeli hücum alətlərinin

kommersiyalaşdırılmasına şərait yaradır və kibercinayətkar fəaliyyətin miqyasını genişləndirir [19]. Təchizat zənciri hücumları və sıfır gün zəifliklərinin istismarı isə müasir təhlükələrin ən kritik istiqamətlərindən biridir.

NƏTİCƏ

Kibercinayətkarlıq müasir rəqəmsal infrastruktur üçün əsas təhdidlərdən biri olaraq qalır və rəqəmsal texnologiyaların inkişafı kiberhücumların mürəkkəbliyini, miqyasını və həyata keçirilmə mexanizmlərini daha da genişləndirir. Müasir kibercinayətkarlıq yüksək texnoloji mürəkkəblik, zərərli proqram təminatının aktiv istifadəsi, sosial mühəndislik metodları və zəifliklərin istismarı ilə xarakterizə olunur. Əşyaların İnterneti, süni intellekt və bulud hesablamalarının geniş tətbiqi rəqəmsal iqtisadiyyatın imkanlarını artırmaqla yanaşı, kiberrisklərin səviyyəsini də yüksəldir.

Bu tədqiqat çərçivəsində kibercinayətkarlığın metodları, mexanizmləri və texnologiyaları arasında qarşılıqlı əlaqələri əks etdirən üçsəviyyəli inteqrasiya olunmuş konseptual model təklif edilmişdir. Təklif olunan model kiberhücumların strukturlaşdırılmış şəkildə təhlilinə, onların formalaşma və həyata keçirilməsi proseslərini sistemli şəkildə dərk edilməsinə imkan verir.

Bu yanaşma kibertəhdidlərin daha dəqiq modelləşdirilməsi, onların proqnozlaşdırılması və adaptiv müdafiə strategiyalarının formalaşdırılması üçün nəzəri əsas kimi çıxış edə bilər.

Bununla yanaşı, tədqiqatın müəyyən məhdudiyyətləri mövcuddur. Təklif olunan model konseptual xarakter daşıyır və onun praktiki tətbiqi empirik verilənlər əsasında əlavə yoxlamalar tələb edir. Gələcək tədqiqatlarda modelin müxtəlif tətbiq ssenarilərində effektivliyinin qiymətləndirilməsi məqsədəuyğun hesab olunur.

ƏDƏBİYYAT

[1] Y. Yigit, et al., "Generative AI and LLMs for Critical Infrastructure Protection: Evaluation Benchmarks, Agentic AI, Challenges, and Opportunities," Sensors, 25(6), 1666, 2025.

[2] H. Zeng, M. Yunis, A. Khalil, and N. Mirza, "Towards a conceptual framework for AI-driven anomaly detection in smart city IoT networks," Journal of Innovation & Knowledge, 9(4), 100601, 2024.

[3] I. H. Sarker, "Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects," Annals of Data Science, 10, pp. 1473-1498, 2023.

[4] M. Ahmed, Q. Alasad, J-S Yuan , M. Alawad, "Re-Evaluating Deep Learning Attacks and Defenses in Cybersecurity Systems,". Big Data and Cognitive Computing, 8(12):191, 2024.

[5] A. J. G. de Azambuja, C. Plesker, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Artificial Intelligence-Based Cyber Security in the Context of Industry 4.0– A Survey," Electronics, 12(8):1920, 2023.

[6] N. Mohamed, "Cutting-edge advances in AI and ML for cybersecurity: a comprehensive review of emerging trends and future directions", Cogent Business & Management, 2025, 12(1).

[7] I. J. Vourganas, and A. L. Michala, "Applications of Machine Learning in Cyber Security: A Review," Journal of Cybersecurity and Privacy, 4(4), pp. 972-992, 2024.

[8] Z. He, D. Davila, S. Bi, T. Wang, and T.Hou, "Machine Learning for Cybersecurity: A Survey of Applications, Adversarial Challenges, and Future Research Directions," Electronics, 14, 4563, 2025.

[9] Y. Liu, "Intrusion into Computer Information System: Criminal Law Rule Based on Different Judicial Recognition Perspectives of State Affairs," Lecture Notes in Education Psychology and Public Media, 17, pp. 63-72, 2023.

[10] H. Taherdoost, "Insights into Cybercrime Detection and Response: A Review of Time Factor. Information," 15(5), 273, 2024.

[11] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," Leading Issues in Information Warfare & Security Research, 1(1), 80.

[12] L. Zhao, "Navigating the Cyber Kill Chain: A modern approach to pentesting," Applied and Computational Engineering, vol. 38, pp. 170–175, 2024.

[13] R. Kour, R. Karim, and P. Dersin, "Modelling cybersecurity strategies with game theory and cyber kill chain," International Journal of System Assurance Engineering and Management, 2025.

[14] H. Taherdoost, "Insights into Cybercrime Detection and Response: A Review of Time Factor," Information, 15(5), p. 273, 2024.

[15] MITRE Corporation, "MITRE ATT&CK Framework," 2024.

[16] G. Grispos, H. Studiawan, S. Alrabaee, "Internet of things (IoT) forensics and incident response: The good, the bad, and the unaddressed," Forensic Science International: Digital Investigation, v. 48, pp. 301671, 2024.

[17] M. Uddin, M. S. Irshad, I. A. Kandhro, et al., "Generative AI revolution in cybersecurity: a comprehensive review of threat intelligence and operations," Artificial Intelligence Review, 58, 236, 2025.

[18] A. H. Salem, S. M. Azzam, O. E. Emam, et al., "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," Journal of Big Data, 11, 105, 2024.

[19] A. Ali, M. Shah, M. Foster, M. N. Alraja, "Cybercrime resilience in the era of advanced technologies," Computers, 214(2), p. 38, 2025.

A Study of Cybercrime Methods, Mechanisms, and Technologies in the Context of Digital Transformation

Tahmasib Fataliyev[1], Shakir Mehdiyev[2]

[1, 2] Institute of Information Technology, Baku, Azerbaijan
[1]depart_5@iit.science.az, [2]shakir.mehtieff@gmail.com

Abstract– The article examines modern cybercrime methods, mechanisms, and technologies used in the digital environment. The primary methods of cyberattacks, including the use of malware, exploiting vulnerabilities in information systems, and social engineering techniques, are investigated. The analysis covers the technological tools utilized in cybercriminal activities, as well as the mechanisms of executing attacks at various stages of their lifecycle.

Keywords– cybercrime; cyberattacks; malware; social engineering; digital technologies; cyberthreats.