Onlayn Platformada Seçki Sistemlərinə Kibertəhlükələrin Araşdırılması və Rəqəmsal Kriminalistikası

Raqif İsmayılov[1], Kəmalə Qurbanova[2]
[1,2]İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*raqif.ismayilov@gmail.com*, [2]*kemalewamil@gmail.com*

***Xülasə*— Tədqiqat işində onlayn seçki sistemlərinin mahiyyəti, struktur komponentləri və səsvermə prosesinin ardıcıllığını təmin edən funksional model təhlil edilmişdir. Sistemlərin hüquqi meyarları olan anonimlik və şəffaflıq balansı, bu prinsiplərin e-səsvermə infrastrukturuna inteqrasiyası ilə şərh olunmuşdur. Qlobal təcrübə əsasında kibertəhdidlərin təsnifatı hücum vektorlarına görə aparılmışdır, blokçeyn və sıfır-bilik sübutları vasitəsilə səslərin konfidensial təsdiqlənməsi araşdırılmışdır. Təhlükəsizlik arxitekturası sistemin kiberdayanıqlılığını artırsa da, qayda pozuntularının tam aradan qaldırılması təmin olunmur. Rəqəmsal kriminalistika müstəvisində sistem qeydlərinin analizi, hadisələrin əlaqələndirilməsi və sübutların bütövlüyü tədqiq olunmuş, təhlükəsizlik səviyyəsinin yüksəldilməsi üçün təkliflər verilmişdir.**

Açar sözlər*— *blokçeyn; elektron səsvermə; sıfır-bilik sübutları; rəqəmsal kriminalistika.

I. GİRİŞ

Süni intellekt və bulud texnologiyalarının inkişafı dövlət idarəçiliyinin rəqəmsallaşdırılmasını və demokratik proseslərin rəqəmsal mühitə inteqrasiyasını sürətləndirmişdir. Onlayn platformalar əsasında qurulan seçki sistemləri səsvermənin operativliyini, şəffaflığını və əlçatanlığını artırır. Bununla yanaşı, bu sistemlər yeni nəsil kibertəhlükələr üçün hədəfə çevrilir. Nəticədə seçki sistemlərinin kibertəhlükəsizliyi texniki məsələ çərçivəsindən çıxaraq milli təhlükəsizlik və institusional sabitlik kontekstində strateji əhəmiyyət qazanır.

Müasir dövrdə seçki infrastrukturuna yönəlmiş kiberhücumlar və informasiya manipulyasiyası və seçici davranışına təsir edən rəqəmsal əməliyyatlar risklərin sistemli xarakter aldığını göstərir. Sosial media platformalarında koordinasiya olunan dezinformasiya kampaniyaları və hədəflənmiş hücumlar seçkilərin legitimliyini zəiflədir və ictimai etimadı azaldır. Bu isə seçki sistemlərinin həm texniki infrastruktur, həm də informasiya mühiti səviyyəsində kompleks qorunmasını zəruri edir.

Bu sahədə beynəlxalq səviyyədə bir sıra normativ və tövsiyə xarakterli sənədlər qəbul edilmişdir. Avropa Şurasının Kiber-cinayətkarlıq haqqında Konvensiyası (Budapeşt Konvensiyası) kiberməkanda törədilən cinayətlərin qarşısının alınması və rəqəmsal sübutların toplanması üzrə əsas hüquqi çərçivəni müəyyən edir [1]. ATƏT tərəfindən seçki proseslərində informasiya-kommunikasiya texnologiyalarının təhlükəsiz istifadəsinə dair tövsiyələr hazırlanmışdır [2]. Bununla yanaşı, BMT tərəfindən qəbul edilmiş Dayanıqlı İnkişaf Məqsədləri çərçivəsində rəqəmsal təhlükəsizliyin təmin olunması və kritik infrastrukturun qorunması güclü, dayanıqlı və etibarlı institutların formalaşdırılmasının əsas şərtlərindən biri kimi müəyyən edilmişdir [3]. Bu yanaşmalar seçki sistemlərinin kibertəhlükəsizliyinin təmin olunmasını qlobal idarəetmə və təhlükəsizlik gündəliyinin mühüm tərkib hissəsinə çevirir.

Mövzunun aktuallığı qlobal səviyyədə təsdiq olunur. Beynəlxalq təşkilatlar seçki təhlükəsizliyini kritik infrastrukturun qorunması kimi qiymətləndirir. Rəqəmsal seçki sistemlərinin tətbiqi genişləndikcə kibertəhdidlərin miqyası və mürəkkəbliyi artır. Bu isə onların vaxtında aşkarlanması və sübutlandırılması üçün yeni texnoloji yanaşmaların tətbiqini tələb edir. Rəqəmsal kriminalistika bu prosesdə əsas alət kimi çıxış edir və rəqəmsal izlərin analizi vasitəsilə müdaxilə faktlarının müəyyən edilməsinə imkan yaradır.

Tədqiqatın məqsədi onlayn seçki platformalarına yönəlmiş kibertəhlükələrin sistemli təhlili və onların rəqəmsal kriminalistika metodları ilə aşkarlanması mexanizmlərinin əsaslandırılmasıdır. Tədqiqatın obyekti rəqəmsal seçki sistemləri və bu sistemlərə yönəlmiş kiberhücum vektorlarıdır. Tədqiqatın predmeti isə kibertəhdidlərin texniki və davranış indikatorlarının müəyyən edilməsi və rəqəmsal sübutların formalaşdırılması üsullarıdır. Problemin qlobal xarakter daşıması demokratik institutların qorunması baxımından onu beynəlxalq prioritetlərdən birinə çevirir.

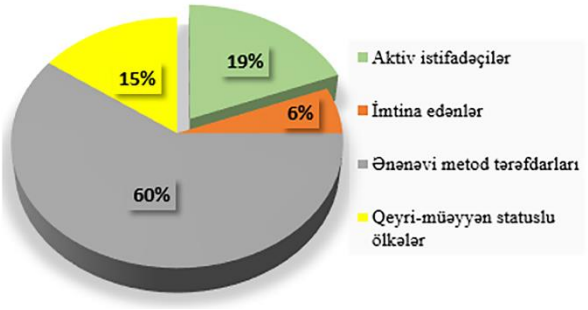
Tədqiqatın əsas məqsədi onlayn səsvermənin hüquqi legitimliyini təmin etmək üçün süni intellekt və rəqəmsal kriminalistikanın inteqrasiya imkanlarını araşdırmaq, elmi yeniliyi isə sistemin dayanıqlığını artıran yeni təhlükəsizlik modeli təklif etməkdir.

II. ONLAYN SEÇKİ SİSTEMLƏRİNİN MAHİYYƏTİ VƏ ƏSAS KOMPONENTLƏRİ

Elektron səsvermənin tarixi təkamülü 1960-cı illərdə perfokartların tətbiqi və səslərin maşınla hesablanması ilə başlamışdır. Sonrakı mərhələdə optik skanerlər perfokartları əvəz etsə də, XX əsrin sonlarında birbaşa qeydiyyat aparan elektron sistemlər ön plana çıxmışdır. Lakin 2000-ci illərdən

DOI: 10.25045/forensic.gov.2026.55

etibarən e-səsvermə sistemlərinin praktiki tətbiqi zamanı mütəmadi olaraq ciddi təhlükəsizlik boşluqları aşkarlanmışdır: buraya Hindistanın DRE sistemindəki texniki qüsurlar, Vaşinqtonun pilot internet səsvermə layihəsinin manipulyasiyası və İsveçrənin «sVote» sistemində aşkarlanan kriptoqrafik zəifliklər daxildir. Hazırda qlobal miqyasda ölkələrin yalnız 19%-i e-səsvermədən aktiv istifadə edir; 6%-i bu texnologiyanı sınaqdan keçirsə də, sistemin şəffaflığı və kiberdayanıqlığı ilə bağlı yaranan yüksək risklər səbəbindən ondan imtina edərək yenidən ənənəvi üsullara qayıtmış, 15 %-i üzrə məlumat mövcud deyil, 60%-i isə hələ də kağız səsverməsinə üstünlük verməkdədir (Şəkil 1) [4].



Şəkil 1. Ölkələrin e-səsverməyə yanaşması (%)

Müasir dövrdə dövlət idarəçiliyinin rəqəmsal transformasiyası fonunda demokratik strukturun təməl daşı hesab olunan seçki proseslərinin onlayn platformalara keçidi obyektiv zərurət xarakteri almışdır. İnformasiya-kommunikasiya texnologiyalarının sürətli inkişafı seçki institutlarının daha çevik, əlçatan və inklüziv formatda təşkilinə zəmin yaradır. Bu kontekstdə onlayn seçki sistemləri texnoloji yenilik olmaqla yanaşı, eyni zamanda demokratik iştirakçılığın genişləndirilməsinə xidmət edən strateji institusional mexanizm mahiyyəti daşıyır.

Onlayn seçki sistemlərinin mahiyyəti, ilk növbədə, elektron səsvermənin (e-voting) daha təkmil və uzaqdan icra olunan forması olan internet səsverməsi (i-voting) anlayışı ilə xarakterizə olunur. Bu sistemlər seçicinin fiziki olaraq seçki məntəqəsinə getmədən, açıq və ya qorunan şəbəkə infrastrukturu üzərindən öz iradəsini rəqəmsal formada ifadə etməsinə imkan verir (Şəkil 2). Bununla yanaşı, bu model coğrafi məhdudiyyətləri aradan qaldıraraq xaricdə yaşayan vətəndaşların seçki prosesində iştirakını asanlaşdırır və seçici fəallığının artırılmasına müsbət təsir göstərir [5].

İnternet səsvermə sistemlərinin texnoloji və funksional mahiyyətinin düzgün anlaşılması üçün onların əsasını təşkil edən səsvermə protokollarının strukturunun təhlili xüsusi əhəmiyyət kəsb edir. Bu protokollar seçki prosesinin bütün mərhələlərini tənzimləyən ardıcıl mexanizmlər toplusu kimi çıxış edir və sistemin təhlükəsizliyini, şəffaflığını və etibarlılığını təmin edən əsas çərçivəni formalaşdırır. Bu baxımdan, internet səsvermə protokolları səsvermə prosesinin ardıcıllığını təmin edən üç əsas mərhələ üzrə nəzərdən keçirilir [6]:

- Hazırlıq mərhələsi (setup / pre-election): Seçki sisteminin qurulması, kriptoqrafik açarların yaradılması və seçicilərin qeydiyyatı həyata keçirilir.
- Səsvermə mərhələsi (voting / election): Seçici autentifikasiya olunur, öz səsini verir və səsin düzgün qeydə alınması təsdiqlənir.
- Nəticələrin hesablanması mərhələsi (counting / tallying): Səslər deşifrə olunur, hesablanır və yekun nəticələr formalaşdırılır.

Şəkil 2. Ənənəvi səsvermədən internet səsverməsinə keçid modeli

Bu yanaşma göstərir ki, seçki sisteminin texnoloji arxitekturası yüksək təhlükəsizlik standartlarına əsaslanır: səsin yaradılması, ötürülməsi, saxlanması və hesablanması mərhələlərinin hər birində kriptoqrafik mexanizmlərlə təmin olunmasını nəzərdə tutur. Beləliklə, sistem daxilində hər bir əməliyyatın yoxlanılması mümkün olur və seçki prosesinin şəffaflığı ilə yanaşı, texniki bütövlüyü də qorunur. Eyni zamanda, bu texnoloji platformalar milli və etnik azlıqların səsvermədə iştirak problemlərinin həlli üçün mühüm alətdir. Rəqəmsal seçki institutlarının uğurlu tətbiqi, xüsusilə cəmiyyətin həssas qruplarının və azlıqların demokratik iştirakçılığını təmin etməklə, qlobal miqyasda demokratik dayanıqlığın gücləndirilməsinə töhfə verir [7].

Səsvermə prosesində məxfilik və anonimlik prinsiplərinin qorunması əsas prioritetlərdəndir. Bu məqsədlə homomorfik şifrləmə, sıfır-bilik sübutları və digər müasir kriptoqrafik alqoritmlər tətbiq olunur. Bu texnologiyalar səslərin məzmununu açıqlamadan onların düzgün hesablanmasını təmin edir və seçici iradəsinin gizliliyini qoruyur. Beləliklə, anonimlik ilə şəffaflıq arasında balans təmin edilir ki, bu da seçki sistemlərinin legitimliyinin əsas şərtlərindən biridir [8].

Sıfır-bilik sübutları (ZKPs) əsas verilənləri açıqlamadan səslərin doğruluğunu sübut etməyə imkan verən kritik kriptoqrafik mexanizmdir [9].

- Səsvermə sistemləri kontekstində ZKPs seçicilərə öz seçimlərini ifşa etmədən səslərinin düzgün qeydə alındığını yoxlamaq imkanı yaradır;
- Müşahidəçilərə fərdi səs seçimlərini əldə etmədən ümumi nəticələrin doğruluğunu təsdiqləməyə şərait yaradır;
- Həmçinin sistemə həssas məlumatları açıqlamadan protokolun qaydalara uyğun icra olunduğunu sübut etməyə imkan verir.

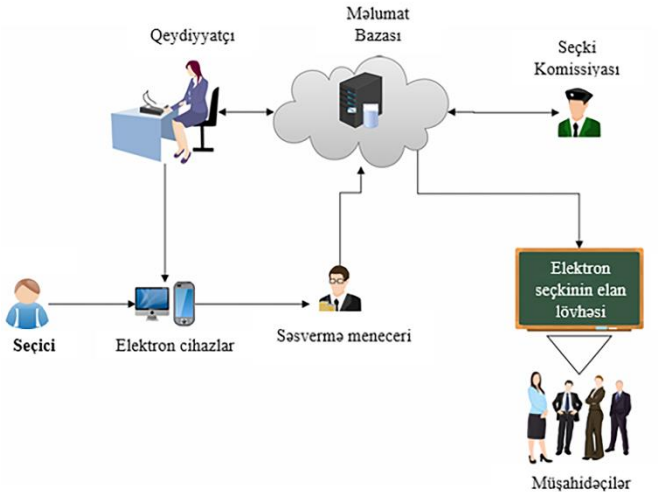
Kriptoqrafik təhlükəsizliklə yanaşı, sistemin bütövlüyü məlumatların saxlanılması və emalı metodologiyasından birbaşa asılıdır. Bu xüsusda, ənənəvi mərkəzləşdirilmiş verilənlər bazalarından fərqli olaraq, paylanmış reyestr texnologiyalarına əsaslanan arxitekturalar məlumatların dəyişdirilməzliyini və kəsilməzliyini fundamental səviyyədə təmin edir. Blokçeyn infrastrukturunun təqdim etdiyi bu xüsusiyyət seçki nəticələrinin manipulyasiya riskini minimuma endirməklə yanaşı, hər bir tranzaksiyanın şəffaf audit izinin formalaşdırılmasını da təmin edir. Belə bir rəqəmsal iz, potensial kibermüdaxilələrin operativ aşkarlanması və rəqəmsal kriminalistika metodları ilə sübuta yetirilməsi üçün etibarlı baza rolunu oynayaraq, sistemin ümumi təhlükəsizlik filtrini tamamlayır.

E-səsvermə sisteminin bütövlüyü, təhlükəsizliyi və şəffaflığı onun əsas komponentlərinin düzgün inteqrasiyasından asılıdır. Sistem səsvermənin bütün mərhələlərini qeydiyyatdan nəticələrin hesablanmasına qədər demokratik prinsiplərə uyğun idarə etməli və potensial kiber-təhdidləri minimuma endirməlidir. Sistemin əsas struktur elementləri aşağıdakılardır [10]:

- *İstifadəçi interfeysi və giriş*: seçicilərin sistemlə təmasını təmin edən intuitiv veb-portallar, mobil tətbiqlər və ya terminal interfeysləridir.
- *Autentifikasiya və avtorizasiya*: seçici hüququnun təsdiqi üçün biometrik məlumatlar, unikal identifikatorlar və ya kriptoqrafik açarlar vasitəsilə həyata keçirilən təhlükəsizlik mexanizmidir.
- *Rəqəmsal bülleten və şifrələmə*: seçimin konfidensiallığını qorumaq üçün səslər qeydə alındığı andan etibarən mürəkkəb şifrələmə alqoritmləri ilə qorunur və anonimlik təmin edilir.
- *Məlumatların saxlanılması və aqreqasiyası*: səslər mərkəzləşdirilmiş bazalarda və ya mərkəzsizləşdirilmiş paylanmış reyestrlərdə saxlanılır, giriş nəzarəti və audit izləri ilə bütövlüyü qorunur.
- *Yoxlama və audit interfeysi*: seçicilərin və müstəqil müşahidəçilərin səsvermənin dürüstlüyünü yoxlamasına imkan verən şəffaflıq mexanizmidir.
- *Dayanıqlılıq və ehtiyatlılıq mexanizmləri*: texniki nasazlıqlar və ya kiberhücumlar zamanı sistemin işini davam etdirməsi üçün ehtiyat serverlər və qəza bərpa planları ilə təmin olunmuş infrastrukturdur.

[11]-ci işdə təqdim olunan elektron səsvermə sisteminin arxitekturası qarşılıqlı əlaqədə fəaliyyət göstərən əsas mərhələlərdən ibarətdir (Şəkil 3): ilkin olaraq qeydiyyat və autentifikasiya mərhələsində seçici məlumatları qeydiyyat agenti tərəfindən yoxlanılaraq şifrələnmiş məlumat bazasına ötürülür və seçki qurumu tərəfindən ümumi təhlükəsizlik nəzarət altında saxlanılır; növbəti mərhələdə seçici elektron cihazlar vasitəsilə səs verir, səsvermə meneceri isə bu səsi qəbul edərək onun anonimliyini və bütövlüyünü qorumaq şərtilə şifrələnmiş bazaya inteqrasiya edir; son mərhələdə isə səslər cəmlənir, nəticələr elektron seçki elan lövhəsində dərc edilir və müşahidəçilərə sistemin düzgünlüyünü və şəffaflığını yoxlamaq imkanı yaradılır. Bu arxitektura səsvermə prosesinin bütün mərhələlərində həm texniki təhlükəsizliyi, həm də ictimai audit imkanlarını təmin edir [11].

Beləliklə, onlayn seçki sistemləri dövlət, cəmiyyət və fərd arasında formalaşan rəqəmsal etimad münasibətlərinin mühüm indikatorudur. Bu sistemlərin təhlükəsizliyinin təmin olunması isə yalnız texniki tədbirlərlə məhdudlaşmır, eyni zamanda kibertəhdidlərin vaxtında aşkarlanması və onların rəqəmsal kriminalistika metodları ilə sübuta yetirilməsini də zəruri edir.



Şəkil 3. Elektron seçki prosesinin mərhələli idarəetmə strukturu

III. ONLAYN SƏSVERMƏ SİSTEMLƏRİNDƏ KİBERTƏHDİDLƏR: QLOBAL TƏCRÜBƏ

Onlayn səsvermə sistemləri qlobal miqyasda dövlətin kritik informasiya strukturu hesab olunur və strateji olaraq milli təhlükəsizlik müstəvisinə aiddir. Beynəlxalq təcrübə və aparılan tədqiqatlar göstərir ki, biometrik eyniləşdirmə və rəqəmsal qeydiyyat vasitələri şəffaflığı artırsa da, infrastruktur çatışmazlıqları, kiberhücumlar və ən əsası insan amilindən irəli gələn manipulyasiyalar seçkinin legitimliyini qlobal səviyyədə risk altına qoya bilir. Bu səbəbdən, seçki saxtakarlıqlarının qarşısının alınması üçün yalnız proqram təminatının tətbiqi kifayət deyil; bu proses həm texniki müdafiə sistemlərinin, həm də fərdlərin düşüncə tərzinin və etik dəyərlərinin yenilənməsini nəzərdə tutan kompleks bir yanaşma tələb edir.

Seçki kontekstində kiberhücum anlayışı texniki müdaxilələrlə yanaşı, sistemin bütövlüyünü, verilənlərin doğruluğunu və ictimai etimadı hədəfləyən bütün rəqəmsal əməliyyatları əhatə edir. Bu təhdidlər seçki infrastrukturunun funksional dayanıqlığına və legitimliyinə qarşı kompleks risk faktoru kimi qiymətləndirilir. Müasir tədqiqatlara əsasən, bu tip təhlükələr çoxsəviyyəli təhdid modeli çərçivəsində nəzərdən keçirilir və üç əsas iyerarxik səviyyədə təzahür edir [12]:

- *Texnoloji səviyyə:* server infrastrukturuna kənar müdaxilələr, xidmətdən imtina hücumları (DDoS), proqram təminatı boşluqlarının istismarı və şəbəkə

seqmentlərinin zədələnməsi.

- *İnsan faktoru:* fişinq əməliyyatları, fərdi identifikasiya məlumatlarının ələ keçirilməsi və daxili istifadəçi xətaları.
- *İnformasiya mühiti:* dezinformasiya kampaniyaları, sosial media manipulyasiyaları və bot şəbəkələri vasitəsilə seçici rəyinin süni şəkildə yönləndirilməsi.

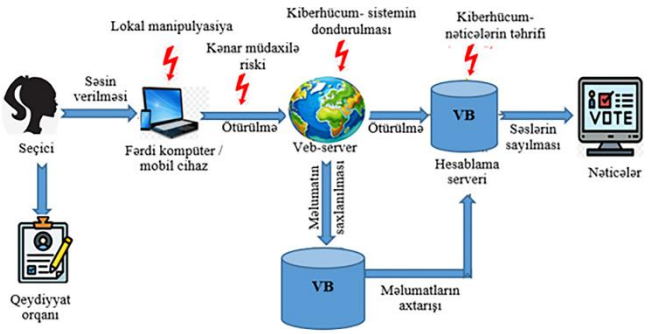
Onlayn səsvermə sistemlərinə yönəlmiş kibertəhdidlərin təhlili göstərir ki, bu risklər seçki prosesinin strukturuna təsir mexanizmləri üzrə qiymətləndirilməlidir. Müasir elmi yanaşmalarda kibertəhlükələrin məhz bu platformanın struktur-funksional arxitekturasına təsiri üç təməl sütunu olan əlçatanlıq, bütövlük və məxfilik prinsiplərinin pozulma dərəcəsinə görə təsnif edilir [13]:

- *Əlçatanlıq prinsipi*: Seçki sistemlərinə qarşı həyata keçirilən DDoS və digər kiberhücumlar platformaların əlçatanlığını məhdudlaşdıraraq səsvermə prosesinin fasiləsizliyini pozur və seçicilərin sistemə çıxış imkanlarını zəiflədir.
- *Bütövlük prinsipi*: Məlumat bazalarına müdaxilə nəticəsində seçki məlumatlarının dəyişdirilməsi və ya saxtalaşdırılması ehtimalı yaranır ki, bu da nəticələrin düzgünlüyünü və etibarlılığını sual altına qoyur.
- *Məxfilik prinsipi*: Seçicilərə aid fərdi və biometrik məlumatların sızması məxfilik prinsiplərinin pozulmasına səbəb olmaqla yanaşı, istifadəçilərin sistemə olan inamını zəiflədir.

Sistem infrastrukturunda yaranan fasilələr, məlumatların manipulyasiyası və ya konfidensial məlumatların sızması seçki prosesinin legitimliyini sarsıdan və ictimai etimadı zəiflədən strateji risk amilləridir. Kiberhücumların təsir dairəsi texniki nasazlıqlarla məhdudlaşmır. Eyni zamanda, kiber-fiziki mühitdən ictimai rəyə qədər uzanan zəncirvari bir təsir mexanizmini ifadə edir. Bu baxımdan, təhdidlərin qiymətləndirilməsi zamanı texnoloji infrastrukturla (serverlər, verilənlər bazası) yanaşı, prosesin subyektləri olan seçicilərin və siyasi tərəflərin kibertəhlükəsizlik həssaslığı mütləq nəzərə alınmalıdır. Müasir elmi yanaşmalarda kibertəhdidlərin seçki proseslərinə funksional təsir mexanizmləri aşağıdakı fundamental aspektlər üzrə təsnif olunur [14]:

- *Səsin saxtalaşdırılması*: səslərin qeydə alınması, ötürülməsi və ya hesablanması mərhələlərində baş verən müdaxilələr seçki nəticələrinin obyektivliyinə mənfi təsir göstərir.
- *İcazəsiz giriş*: sistemə icazəsiz giriş imkanları seçki infrastrukturunun idarə olunmasına kənar müdaxilə riskini artırır və təhlükəsizlik mexanizmlərinin effektivliyini zəiflədir.
- *Manipulyasiya*: dezinformasiya və manipulyativ informasiya axınları seçici davranışına təsir göstərərək ictimai rəyin süni şəkildə formalaşdırılmasına səbəb olur.
- *İctimai etimadın zəifləməsi*: yuxarıda qeyd olunan texniki və informasiya yönümlü təsirlər seçicilərin seçki sistemlərinə və nəticələrinə olan etimadını azaldır.
- *Seçki legitimliyinin zəiflədilməsi:* nəticə etibarilə, kibertəhdidlərin kumulyativ təsiri seçki prosesinin legitimliyinin şübhə altına düşməsinə və demokratik institutların zəifləməsinə gətirib çıxarır.

Onlayn səsvermə prosesində məlumatın ötürülməsi, saxlanması və emalı bir neçə müstəqil mərhələ üzrə həyata keçirildiyindən, sistemin hər bir həlqəsi potensial hücum nöqtəsinə çevrilə bilər. Seçicinin istifadə etdiyi fərdi cihazdan başlayaraq server infrastrukturuna qədər olan bütün zəncir boyunca lokal manipulyasiya, kənar müdaxilə, xidmətin dayandırılması (DoS/DDoS tipli hücumlar) və nəticələrin təhrif olunması kimi risklər mövcuddur (Şəkil 4). Bu baxımdan, təhlükəsizlik arxitekturasının çoxsəviyyəli və inteqrasiya olunmuş şəkildə qurulması zəruridir [15].



Şəkil 4. Onlayn səsvermə prosesinin təhlükəsizlik arxitekturası və kiberhücumlar

Qeyd olunan kibertəhdidlərin və sistem manipulyasiyalarının real şəraitdə qarşısının alınması zərurəti onlayn səsvermə texnologiyalarının qlobal miqyasda müxtəlif tətbiq modellərinin meydana gəlməsini şərtləndirmişdir. Beynəlxalq təcrübədə bu risklərin neytrallaşdırılması üçün tətbiq olunan mütərəqqi rəqəmsal arxitekturalar arasında Estoniya nümunəsi xüsusi əhəmiyyət kəsb edir.

Estoniya qlobal miqyasda ən inkişaf etmiş rəqəmsal seçki sistemlərindən birinə malik ölkə kimi qəbul edilir. Burada seçki prosesində rəqəmsal identifikasiya, kriptoqrafik mühafizə mexanizmləri və çoxsəviyyəli autentifikasiya tətbiq olunaraq səsvermənin təhlükəsizliyi və yoxlanıla bilmə imkanları gücləndirilmişdir. Bu model seçki prosesinin sürətini və əlçatanlığını artırsa da, eyni zamanda DDoS hücumları, identifikasiya təhlükəsizliyi və sistemə kənar müdaxilə riskləri kimi kibertəhdidlərin daim nəzarətdə saxlanmasını tələb edir. Buna baxmayaraq, Estoniya təcrübəsi elektron səsvermənin praktik tətbiqi baxımından ən qabaqcıl nümunələrdən biri kimi beynəlxalq ədəbiyyatda geniş şəkildə təhlil olunur [16].

Beləliklə, onlayn səsvermə sistemlərində müşahidə olunan bu çoxsəviyyəli kibertəhdidlər mövcud texnoloji yanaşmaların məhdudiyyətlərini ortaya qoyaraq daha dayanıqlı və şəffaf alternativ modellərin, xüsusilə mərkəzsizləşdirilmiş həllərin araşdırılmasını zəruri edir.

Rəqəmsal mühitdə seçki sistemlərinin təhlükəsizliyinin təmin edilməsi istiqamətində elmi ədəbiyyatda ən çox araşdırılan innovativ yanaşmalardan biri blokçeyn texnologiyasına əsaslanan elektron səsvermə modelləridir. Paylanmış reyestr texnologiyası olan blokçeyn əməliyyatların ardıcıl bloklar şəklində saxlanılmasını və kriptoqrafik mexanizmlərlə qorunmasını təmin edir. Mərkəzsizləşdirilmiş arxitekturaya malik olan bu sistemlər məlumatların dəyişdirilməzliyini, bütövlüyünü, şəffaflığını və yoxlanıla bilmə imkanlarını gücləndirməklə yanaşı, anonimlik, məsuliyyətdən yayınmanın mümkünsüzlüyü və sonadək yoxlanıla bilmə kimi xüsusiyyətləri də təmin edir. Beləliklə, blokçeyn əsaslı yanaşmalar həm ənənəvi e-səsvermə platformalarında müşahidə olunan bütövlük, etimad və audit problemlərinin, həm də səsin təkrarlanması, nəticələrin təhrif edilməsi və şəffaflığın pozulması kimi risklərin aradan qaldırılması baxımından perspektivli texnoloji həll kimi qiymətləndirilir [17].

Blokçeyn şəbəkəsində qeydə alınan hər bir əməliyyat dəyişməzdir və bu, baş vermiş pozuntuları araşdırmaq üçün etibarlı məlumat bazası yaradır. Məhz bu mərhələdə texnoloji imkanlar rəqəmsal kriminalistika ilə kəsişir. Beləliklə, blokçeyndəki qeydlər həm baş vermiş müdaxilələrin izlənilməsinə, həm də onların hüquqi sübuta çevrilməsinə şərait yaradır. Bu yanaşma təhlükəsizlik zəncirinin növbəti mərhələsi kimi rəqəmsal sübutların tədqiqini zəruri edir.

Göründüyü kimi, onlayn seçki infrastrukturunun təhlükəsizliyi yalnız qabaqlayıcı qorunma tədbirləri ilə kifayətlənmir. İstənilən kiberhücum cəhdindən sonra baş vermiş hadisənin izlənilməsi, elektron sübutların toplanması və hücumun qaynağının müəyyən edilməsi seçki prosesinin hüquqi etibarlılığı üçün həlledici əhəmiyyət daşıyır. Bu zərurət elektron səsvermə sistemlərində ortaya çıxan kənar yayınmaların elmi-hüquqi müstəvidə araşdırılmasını və rəqəmsal kriminalistika metodologiyasının tətbiqini müasir dövrün prioritet tələbi kimi ön plana çıxarır.

IV. Elektron Səsvermədə Rəqəmsal Kriminalistika

Onlayn seçki platformalarına qarşı törədilən kibercinayətlər yalnız texniki müdafiə tədbirləri ilə məhdudlaşmır. İnsidentlərin post-faktor araşdırılması və sistemli tədqiqi üçün rəqəmsal kriminalistika (digital forensics) əsas metodoloji çərçivəni formalaşdırır. Bu yanaşma hadisələrə dair texniki və operativ məlumatların toplanmasına və təhlilinə imkan verir. Nəticədə seçki sisteminin bütövlüyünün bərpası və nəticələrin hüquqi etibarlılığının təmin edilməsi mümkün olur.

Onlayn seçki platformalarında sistemin dayanıqlığı, həm daxili nasazlıqların, həm də kənar müdaxilələrin sistemli təhlili vasitəsilə təmin edilir. Real-vaxt rejimində aparılan monitorinq, həm təsadüfi texniki qüsurları, həm də qəsdən həyata keçirilən kiberhücumları dərhal aşkar etməyə imkan verir. Nəticədə, seçki infrastrukturunun manipulyasiyalara qarşı qorunma səviyyəsi yüksəlir və proses şəffaflığı təmin olunur.

Rəqəmsal kriminalistika elektron səsvermə sistemlərində həm statik, həm də dinamik məlumatların sistemli analizini əhatə edir. Bu prosesin əsas məqsədi, seçki prosesinə müdaxilə hallarında hər bir detal üzrə sübut toplamaq və bu məlumatları hüquqi baxımdan etibarlı şəkildə təqdim etməkdir [18]:

- Statik məlumatlar / qeydlər: Server loqları, autentifikasiya verilənlər bazaları və konfiqurasiya faylları kimi daimi yaddaşda saxlanılan məlumatları əhatə edir. Bu məlumatların təhlili insidentin metodologiyasını və hədəf strukturlarını müəyyən etməyə imkan verir.
- Dinamik məlumatlar / trafik izləri: Şəbəkə protokolları üzərindən ötürülən və uçucu xarakter daşıyan məlumatları əhatə edir. Paket səviyyəsində aparılan analiz (məsələn, DDoS hücumları və manipulyasiya cəhdləri) hücumun icra trayektoriyasını və real-vaxt anomaliyalarını aşkar etməyə imkan verir.

Toplanmış statik və dinamik sübutlar "Sübutlar zənciri" (Chain of Custody) prinsipi əsasında rəsmiləşdirilir. Server loqları, verilənlər bazası nüsxələri və autentifikasiya qeydləri kimi statik məlumatlar, eləcə də şəbəkə trafikindəki dinamik məlumatlar hash funksiyaları və rəqəmsal imzalar vasitəsilə təsdiqlənir. Bu proses zamanı sübutların ilkin vəziyyəti qorunur və manipulyasiya riskini minimuma endirir. Eyni zamanda texniki etibarlılığı təmin edir. Belə bir sistemli hesabatlılıq seçki platformasının legitimliyini bərpa etməklə yanaşı, rəqəmsal mühitdə potensial cinayətkar niyyətlərin qarşısını alan mühüm amilə çevrilir [19].

Rəqəmsal sübutun etibarlılığı, akvizisiya mərhələsindən məhkəmə instansiyasına qədər olan bütün proseslərin şəffaflığı ilə müəyyən edilir. Verilənlərin bütövlüyü heş funksiyaları və rəqəmsal imza vasitəsilə təmin olunur. Bu isə texniki zərurət olmaqla yanaşı, eyni zamanda hüquqi legitimlik şərtidir:

- *Standartlaşdırma*: Onlayn səsvermə zamanı generasiya olunan statik (loqlar, nüsxələr) və dinamik (trafik) artefaktların "rəqəmsal sübut" statusu alması üçün ISO/IEC 27037 standartına uyğun identifikaciya və toplama protokolları tətbiq olunur.
- *İnkarolunmazlıq*: Rəqəmsal imza və zaman möhürü mexanizmləri inkarolunmazlıq prinsipini reallaşdırır, mənbənin autentifikasiyasını və bütövlüyünü sənədləşdirir.
- *Zəncirvari hesabatlılıq*: Sübutlar zəncirinin hər hansı mərhələdə pozulması (məsələn, heş dəyərlərinin diskrepantlığı) rəqəmsal sübutun hüquqi qüvvəsini ləğv edir

Elektron səsvermə sistemlərində rəqəmsal kriminalistika metodologiyasının tətbiqi seçki nəticələrinin hüquqi legitimliyinin sarsılmaz zəmanətidir. Sübutlar zəncirinin kriptoqrafik metodlarla qorunması, istənilən müdaxilə cəhdinin aşkarlanmasını və hüquqi müstəvidə sübut olunmasını təmin edir. Beləliklə, şəffaf kriminalistik prosedur seçicilərin rəqəmsal sistemə olan etimadını gücləndirərək, demokratik prosesin kiber-təhdidlərdən azad mühitdə keçirilməsini şərtləndirən həlledici elementə çevrilir.

V. Kriptoqrafik və Rəqəmsal Kriminalistika Əsasli Elektron Səsvermə Modeli

Elektron səsvermə sistemlərində rəqəmsal kriminalistika

mexanizmlərinin tətbiqi göstərir ki, seçki təhlükəsizliyi yalnız insidentlərin aşkarlanması ilə məhdudlaşmamalıdır. Eyni zamanda preventiv, audit edilə bilən və hüquqi baxımdan müdafiə oluna bilən vahid təhlükəsizlik arxitekturası ilə dəstəklənməlidir. Mövcud kiber təhdidlərin mürəkkəbləşməsi, seçici anonimliyinin qorunması və rəqəmsal sübutların hüquqi qüvvəsinin təmin olunması elektron səsvermə sistemlərində çoxsəviyyəli və inteqrativ modelin formalaşdırılmasını zəruri edir. Bu baxımdan aşağıda təqdim olunan model blokçeyn texnologiyası, kriptoqrafik müdafiə mexanizmləri, süni intellekt əsaslı monitorinq və rəqəmsal kriminalistika komponentlərini vahid təhlükəsizlik çərçivəsində birləşdirən konseptual arxitektura kimi təklif olunur.

Təklif olunan model məhkəmə müstəvisində müdafiə oluna bilən, şəffaf, audit edilə bilən və hüquqi legitimliyi təmin edən onlayn səsvermə sisteminin çoxlaylı təhlükəsizlik arxitekturasını ifadə edir. Modelin əsas məqsədi seçki prosesində kibertəhlükələrin qarşısının alınması, seçici anonimliyinin qorunması, rəqəmsal sübutların hüquqi baxımdan etibarlı şəkildə formalaşdırılması və nəticələrin müstəqil şəkildə yoxlanılmasının təmin edilməsidir. Model blokçeyn, süni intellekt, rəqəmsal kriminalistika, kriptoqrafiya və beynəlxalq təhlükəsizlik standartlarının inteqrasiyası əsasında qurulmuş kompleks referens arxitektura kimi təqdim olunur.

Model struktur baxımından yeddi əsas funksional müstəvidən ibarətdir və hər bir müstəvi seçki prosesinin müəyyən təhlükəsizlik və idarəetmə mərhələsini əhatə edir: Kimlik və uyğunluq müstəvisi: Bu müstəvi seçicinin identifikasiyası və autentifikasiyası proseslərini həyata keçirir. Sistem seçici cihazı, rəqəmsal cüzdan və çoxfaktorlu autentifikasiya mexanizmləri vasitəsilə istifadəçinin şəxsiyyətini təsdiqləyir. Burada biometrik identifikasiya, rəqəmsal sertifikatlar və uyğunluq yoxlamaları tətbiq edilir. Modeldə xüsusi diqqət anonim identifikasiya körpüsü komponentinə yönəldilir. Bu mexanizm seçicinin kimliyi ilə onun səs bülleteni arasında məntiqi və texniki ayrılmanı təmin edir. Nəticədə sistem seçicinin səs verdiyini təsdiqləyə bilir, lakin hansı seçim etdiyini müəyyən edə bilmir. Bu yanaşma anonimlik və hüquqi identifikasiya arasında balans yaradır.

Bülleten və sayım müstəvisi: Bu hissə elektron səsin yaradılması, şifrələnməsi və blokçeyn mühitinə ötürülməsi proseslərini idarə edir. Modeldə anonim səsvermə kredensialları, sıfır-bilik sübutları və kriptoqrafik şifrələmə texnologiyaları tətbiq olunur. Sıfır-bilik sübutları vasitəsilə seçicinin səsinin düzgün formalaşdırıldığı təsdiqlənir, lakin səsin məzmunu açıqlanmır. Relay/API Gateway infrastrukturu DDoS hücumlarına qarşı qoruma, trafik filtrasiyası və sürət məhdudiyyətləri həyata keçirərək sistemin əlçatanlığını təmin edir. Daha sonra səslər dəyişdirilə bilməyən paylanmış blokçeyn reyestrində saxlanılır. Burada bütün əməliyyatlar rəqəmsal imza və zaman möhürü ilə təsdiqlənir.

Etibarın paylanması və kripto-infrastruktur müstəvisi: Bu müstəvi sistem daxilində etimadın bir mərkəzdə cəmlənməsinin qarşısını alır. Açar idarəetmə sistemi, hardware security module və threshold mexanizmləri vasitəsilə kriptoqrafik açarlar bir neçə etibarlı tərəf arasında bölüşdürülür. Bunun nəticəsində heç bir iştirakçı sistem üzərində tam nəzarət əldə edə bilmir. Modeldə Trusted Execution Environment texnologiyası vasitəsilə əməliyyatların təhlükəsiz icra mühitində aparılması nəzərdə tutulur. Bundan əlavə, threshold tally, Multi-Party Computation və mixnet mexanizmləri seçicinin anonimliyini qorumaqla nəticələrin kollektiv şəkildə hesablanmasını təmin edir. Bu yanaşma həm mərkəzsizləşdirməni, həm də nəticələrin kriptoqrafik doğrulanmasını gücləndirir.

Sübut, audit və rəqəmsal kriminalistika müstəvisi: Burada SIEM sistemləri və süni intellekt əsaslı anomaliya aşkarlama modulları vasitəsilə sistem logları, şəbəkə trafiki və davranış indikatorları real-vaxt rejimində analiz edilir. Sistem mümkün kiberhücumları, manipulyasiya cəhdlərini və şübhəli fəaliyyətləri avtomatik aşkarlayır. Toplanan rəqəmsal sübutlar heş qiymətləri, rəqəmsal imzalar və zaman möhürü vasitəsilə qorunur. Bu isə sübutların dəyişdirilməzliyini təmin edir. Modeldə "ictimai verifikasiya müşahidəçi portalı" komponenti vasitəsilə vətəndaşlar və müstəqil müşahidəçilər seçki prosesinin şəffaflığını yoxlaya bilir. Eyni zamanda e-discovery mexanizmi məhkəmə üçün rəqəmsal sübut paketlərinin formalaşdırılmasına imkan yaradır.

Əsas texnologiya və təhlükəsizlik infrastrukturu: Bu hissədə bulud və ya hibrid infrastruktur, şəbəkə təhlükəsizliyi, ehtiyat nüsxələmə, monitorinq və zaman sinxronizasiyası kimi texniki komponentlər yerləşir. Modeldə NTP/PTP əsaslı zaman sinxronizasiyası xüsusi əhəmiyyət daşıyır. Çünki bütün log və əməliyyat qeydlərinin eyni zaman koordinatında saxlanılması rəqəmsal kriminalistika baxımından kritik tələbdir. Burada məlumatların saxlanma zamanı ilə yanaşı ötürülmə zamanı da şifrələnməsini nəzərdə tutulur.

Standartlar və çərçivələr bloku: Təklif olunan model beynəlxalq standartlarla uyğunlaşdırılmış şəkildə formalaşdırılmışdır. Buraya ISO/IEC 27001 və ISO/IEC 27037 informasiya təhlükəsizliyi standartları, ISO/IEC 27552 elektron səsvermə prinsipləri, ETSI EN 319 401 elektron etimad xidmətləri standartı, GDPR məlumatların qorunması qaydaları və W3C Verifiable Credentials modeli daxildir. Bu yanaşma modelin hüquqi və normativ baxımdan tətbiq edilə bilməsini təmin edir.

İdarəetmə, siyasət və uyğunluq müstəvisi: Burada təşkilati təhlükəsizlik siyasətləri, risk idarəetməsi, audit prosedurları, hüquqi uyğunluq və istifadəçi maarifləndirilməsi mexanizmləri yerləşir. Model göstərir ki, seçki təhlükəsizliyi yalnız texniki müdafiə tədbirləri ilə məhdudlaşmır; eyni zamanda insan faktoru, prosedur nəzarəti və institusional idarəetmə də kritik rol oynayır.

Təklif olunan modelin əsas elmi yeniliyi blokçeyn texnologiyası, süni intellekt əsaslı monitorinq, rəqəmsal kriminalistika və hüquqi audit mexanizmlərinin vahid inteqrativ arxitektura daxilində birləşdirilməsidir. Modeldə seçici anonimliyi ilə audit şəffaflığı arasında balans qorunur. Eyni zamanda bütün inzibati əməliyyatların rəqəmsal imzalanması, zaman möhürlənməsi və sonradan müstəqil şəkildə yoxlanılması təmin edilir. Bu xüsusiyyətlər modelin məhkəmə müstəvisində müdafiə oluna bilən və hüquqi

legitimliyi təmin edən elektron səsvermə arxitekturası kimi çıxış etməsinə imkan yaradır.

NƏTİCƏ

Aparılan tədqiqat göstərdi ki, onlayn seçki sistemlərinin təhlükəsizliyi və etibarlılığı yalnız proqram təminatı ilə məhdudlaşmır. Rəqəmsal kriminalistika metodlarının tətbiqi bu mühitdə baş verən insidentlərin aşkarlanması, təhlili və sübutların qorunması üçün vacibdir. Tədqiqatın əsas nəticələri aşağıdakı kimi ümumiləşdirilə bilər:

- İnteqrativ təhlükəsizlik modeli şəffaflıq və anonimlik arasında balans yaradır. Bu yanaşma onlayn seçkilərin kiberhücumlara qarşı müqavimətini əhəmiyyətli dərəcədə artırır.
- Rəqəmsal kriminalistika elektron səsvermədə hüquqi legitimliyi təmin edən kriminalistik şəffaflığın formalaşdırılmasına xidmət edir. Statik loq faylları və dinamik şəbəkə trafikinin analizi kiberhücumların trayektoriyasını müəyyən edir və müdaxilə faktlarını sübutlara çevirir.
- Hüquqi və texniki standartlaşdırma rəqəmsal dəlillərin məhkəmə instansiyalarında qəbulunu təmin edir və texniki diskrepantlıqların vaxtında aşkarlanmasına imkan yaradır.
- Rəqəmsal kriminalistika metodlarının tətbiqi seçici etimadını bərpa edir və demokratik institutları rəqəmsal manipulyasiyalardan qoruyur.

Tədqiqatın yekununda onlayn seçki sistemlərinin təhlükəsizliyini təmin etmək üçün aşağıdakı praktiki və strateji tövsiyələr verilir:

- Kriptoqrafik və blokçeyn texnologiyalarının geniş tətbiqi ilə sistemlərin dayanıqlılığını artırmaq.
- Rəqəmsal kriminalistika proseslərini standartlaşdırmaq, sübutların hüquqi qüvvəsini təmin etmək.
- Süni intellekt əsaslı kriminalistik analiz sistemlərinin inkişaf etdirilməsi və kvant-dözümlü kriptoqrafik metodların tədqiqi ilə gələcək təhlükəsizlik səviyyəsini yüksəltmək.
- Milli təhlükəsizlik və seçici etimadının qorunması üçün strateji prioritetlər müəyyən etmək və uzunmüddətli planlama aparmaq.

Tədqiqatın sonunda təklif olunan yeni model, blokçeyn, süni intellekt və rəqəmsal kriminalistika metodlarını vahid arxitekturada sintez edərək e-səsvermə sistemlərinin kibertəhlükəsizliyi üçün kompleks istinad çərçivəsi formalaşdırır. Yeddi funksional müstəvidən ibarət olan bu struktur, sıfır-bilik sübutları və kriptoqrafik zaman möhürləri vasitəsilə seçici anonimliyi ilə məlumatların tamlığı arasında texniki balans yaradır. Modelin əsas elmi yeniliyi, insidentlərin real-vaxt rejimində monitorinqi ilə yanaşı, toplanan rəqəmsal sübutların beynəlxalq standartlar (ISO/IEC) çərçivəsində hüquqi legitimliyini və audit edilə bilən mərkəzsizləşdirilmiş etimad infrastrukturunu təmin etməsidir.

ƏDƏBİYYAT

[1] G. Cami, K. Karsai, "International Cooperation Mechanisms in Criminal Justice: Human Rights Implications and Sovereignty Constraints in Cross-Border Access to Electronic Evidence",Balkans Legal, Economic and Social Studies (BLESS), 2025, vol. 2 (2), pp. 93-110.

[2] P. Fantozzi et al., "Electronic Voting Worldwide: The State of the Art", Information, 2025. vol. 16 (8) pp. 650.

[3] T. Atobishi, H. Mansur, "Bridging digital divides: Validating government ICT investments accelerating sustainable development goals", Sustainability, 2025, vol. 17 (5), pp. 2191.

[4] R. Barelli, M. D'Onghia, S. Longari, "Towards Secure Electronic Voting: a Survey on E-Voting Systems and Attacks", Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, 20133 Milan, Italy, IEEE Access, 2025, vol 13, pp 89600-89626.

[5] P.Fantozzi, M. Iecher, L. Laura, M. Naldi, and V. Rughetti, "Electronic Voting Worldwide: The State of the Art", Information, 2025. vol. 16.(8), pp. 650.

[6] S. Barański, B. Biedermann, J. Ellul, "Internet Voting Maturity Framework–Quantifying Maturity in Internet Voting Protocols", Distributed Ledger Technologies: Research and Practice, 2026, pp 51(7).

[7] K. S. L. P. Perbawa, P. A. Aidonojie, B. O. Ajah, "Disability and Electoral Justice for Inclusive Participation", Journal of Sustainable Development and Regulatory Issues (JSDERI), 2025, vol. 3 (2), pp. 221-246.

[8] E. Ologunde, "Cryptographic Protocols for Electronic Voting Systems: A Comprehensive Framework for Secure Democratic Processes" IEEE Transactions On Information Forensics And Security. JOUR. Ologunde, Ezekiel SSRN Electronic Journal, 2023, pp. 5. Cryptographic Protocols for Electronic Voting Systems: A Comprehensive Framework for Secure Democratic Processes

[9] F. E. Ezeh et al, "Designing a Post-Quantum Blockchain Voting Protocol with Zero-Knowledge Proofs for Tamper-Resilient Electoral Infrastructure", 2025, pp 9. Designing a Post-Quantum Blockchain Voting Protocol with Zero-Knowledge Proofs for Tamper-Resilient Electoral Infrastructure

[10] H. O. Ohize, et al,, "Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges", Cluster Computing, 2025, vol. 28 (2), pp. 132.

[11] D. M. Abalogu, "The role of human transformation in curbing electoral malpractices: analyzing the limitations of technology in the nigerian electoral process", Journal Of Psychology, Sociology, History And International Studies, 2025, vol. 1 (1), pp 13-19.

[12] N. Islam, S. Kim, M. Pirooz, S. Shvetsov, "Cyber Threats to Canadian Federal Election: Emerging Threats, Assessment, and Mitigation Strategies" , arXiv preprint, Kanada (Royal Military College of Canada / Queen's University, Kingston, Canada), 2024., pp 2410.05560. (1–25).

[13] A .Suherman et al. "Information Disorder and Electoral Integrity: The Impact of Disinformation on Elections in Developing Democracies", IntechOpen, 2026. Information Disorder and Electoral Integrity: The Impact of Disinformation on Elections in Developing Democracies | IntechOpen

[14] J. P. Merchan, "Trust, technology and Electoral Integrity: A Comparative Analysis of", Technology, 2025, vol. 6 (8), pp. 74.

[15] A. Kaur et al, "Cybersecurity challenges in the ev charging ecosystem", ACM Computing Surveys, 2025, vol. 58 (1), pp. 1-32.

[16] T. Treier, K. Düüna, "Identifying and solving a vulnerability in the estonian internet voting process: Subverting ballot integrity without detection", IEEE Access, 2024, vol.. 12, pp. 197766-197782.

[17] K. M. Khan, J. Arshad, M. M. Khan, "Secure digital voting system based on blockchain technology", International Journal of Electronic Government Research (IJEGR), 2018, vol. 14 (1). pp. 53-62.

[18] A. Karn, "Bayesian And Probabilistic Methods For Assessing And Ensuring The Dynamic Reliability of Electronic Voting Machines (EVMs)", For Assessing And Ensuring The Dynamic Reliability of Electronic Voting Machines (EVMs) (08 october 2025), 2025, pp 1–16.

[19] T. Bromley, P. Reeves, A. Shvartsman, "Elections, Technology, and the Pursuit of Integrity: the Connecticut Landscape", State Certification Testing of Voting Systems National Conference, Indianapolis, 2025, pp. 1-14.

Investigation and Digital Forensics of Cyber Threats to Election Systems on Online Platforms

Raqif Ismayılov[1], Kamala Gurbanova[2]
[1,2]Institute of Information Technology, Baku, Azerbaijan
[1]*raqif.ismayilov@gmail.com*,[2]*kemalewamil@gmail.com*

Abstract- The research paper analyzes the nature of online election systems, their structural components, and the functional model that ensures the sequence of the voting process. The balance between anonymity and transparency, which are the legal criteria of the systems, is interpreted through the integration of these principles into the e-voting infrastructure. Based on global experience, a classification of cyber threats was conducted according to attack vectors, and the confidential verification of votes via blockchain and zero-knowledge proofs was investigated. Although the security architecture increases cyber-resilience, the complete elimination of violations is not guaranteed. Within the framework of digital forensics, the analysis of system logs, event correlation, and evidence integrity were researched, and proposals were made to enhance the security level.

Keywords- blockchain; electronic voting; zero-knowledge proofs; digital forensics.