Xidməti Danışıqların Kriptoqrafik Təminatı Məsələləri Dövlət Kibersuverenliyi Kontekstində

Bikəs Ağayev[1], Şakir Mehdiyev[2], Lalə Əliyeva[3]
[1,2,3] İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]bikies418@gmail.com, [2]shakir.mehtieff@gmail.com, [3]laleasirova@mail.ru

Xülasə— **Məqalədə "dövlət kibersuverenliyi", "texnoloji suverenlik", "informasiya təhlükəsizliyi", "kibertəhlükəsizlik" və digər əlaqəli anlayışlar araşdırılır və müqayisəli analizi aparılır. Bir sıra mənbələrə istinad edilərək əsaslandırılır ki, müxtəlif dərəcəli məxfi və dövlət sirri daşıyan məlumatlar, mühüm dövlət orqanlarının, təşkilatların məxfi məlumatları, qapalı xarakterli müzakirələri, xidməti danışıqlar çoxsəviyyəli struktura malik dövlət kibersuverenliyi və texnoloji suverenlik məsələlərinin tərkib hissələrindən biri hesab edilə bilər. Bu yanaşma çərçivəsində otaq şəraitində aparılan müəyyən məxfiliyə malik xidməti danışıqların iştirakçılar tərəfindən gizli yazılması və otaqdan kənara sızan vibroakustik siqnallar vasitəsilə məlumatların əldə edilməsinə qarşı bir sıra kriptoqrafik qorunma üsullarına baxılır və bu məqsədlə təklif və tövsiyələr verilir.**

Açar sözlər— dövlət kibersuverenliyi; texnoloji suverenlik; informasiya təhlükəsizliyi; məxfi və xidməti danışıqların qorunması; kriptoqrafik qorunma üsulları.

I. GİRİŞ

Texniki ədəbiyyatın araşdırılması göstərir ki, son illərdə qloballaşma və rəqəmsal transformasiyanın inkişaf tempi "Milli təhlükəsizlik", "Dövlət suverenliyi", "Texnoloji suverenlik", "Kiberfəza", "İnformasiya təhlükəsizliyi", "Kibertəhlükəsizlik" və digər əlaqəli anlayışlara istər bir termin, istərsə də bir proses kimi yeni tərif verilməsini, yeni yanaşma tələb edir [1-3]. Məsələn, internetin ilkin inkişaf mərhələsində - 1990-cı illərdə "Kiberfəza" məhfumu altında azad (sərbəst) yayılan, sərhədsiz, açıq, qeyri mərkəzləşmiş informasiya mühiti başa düşülürdü. Hal-hazırda dövlətin nəzarəti məqsədilə, o cümlədən internet kontentin filtrasiyası və ya silinməsi, yayılmasına məhdudiyyətlərin tətbiqi və s. məqsədlərlə müəyyən beynəlxalq, milli normativ sənədlərin, qanunvericilik bazasının yaradılmasına cəhd edilsə də indiyədək bu terminə və bir sistem kimi onun tənzimlənməsinə aid vahid beynəlxalq yanaşma işlənməmiş və qəbul edilməmişdir [4].

Eyni konteksdə digər bir nümunədə İKT-nin təkamül prosesi ilə bağlı "İnformasiya təhlükəsizliyi" və "Kibertəhlükəsizlik" anlayışlarının inerpretasiya trendi daha aydın görünür. XX əsrə qədər "İnformasiya təhlükəsizliyi" termini işlədilməsə də "məlumatların/informasiyanın qorunması" (bəzi hallar üçün mühafizəsi) ifadələri müasir təhlükəsizlik anlamında istifadə edilib (dövlət sirrinin, konfidensiallığın, sirliliyin, məxfiliyin və s. qorunması). İKT-nin nisbətən sonrakı inkişaf mərhələsində, bəzi texniki mənbələrdə "İnformasiya təhlükəsizliyi" və "İnformasiyanın qorunması" fərqli anlayışlar kimi, və ya sinonimlər kimi istifadə edilib. Bu mərhələdə "İnformasiya təhlükəsizliyi" dedikdə bütün informasiya fəzasında (mühitində) olan informasiyanın qorunması ideyası qəbul edilirdi. Rəqəmsallaşma prosesinin başlanması və genişlənməsi ilə bağlı bu iki məhvuma baxışlar da dəyişməyə başladı. Hələ keçən əsrin 60-70-ci illərindən başlayaraq fərdi kompüterlərin meydana gəlməsi və sonralar geniş yayılması, internetin yaranması, optik-rəqəmsal surətçıxarma avadanlıqlarının (skanerlər və digər analoji texniki vasitələr) ucuzlaşması (əlyetərliliyi) və mətnin tanınma texnologiyalarının inkişafı və s. amillər kağız daşıyıcılarda olan informasiyanın rəqəmsallaşdırılması prosesinin bir sıra təşəbbüs hallarından kollektiv fəaliyyət növünə keçməsinə, daha sonralar isə kütləvi hal alması ilə nəticələndi.

2000-ci illərdə rəqəmsal informasiya resusrlarının sürətlə artması, elektron sənəd dövriyyəsinin yaranması və inkişafı, elektron dövlət və s. rəqəmsal resursların təhlükəzizliyi və onun qorunması məsələlərini özündə ehtiva edən yeni bir məhfumun – "Kibertəhlükəsizlik" termininin yaranması ilə nəticələndi. Bu səbəbdən hazırda akademik yanaşmada "İnformasiya təhlükəsizliyi" dedikdə bütün formalarda olan informasiyanın, "Kibertəhlükəsizlik" dedikdə isə ancaq rəqəmsal resursların (informasiya, İKT sistemləri, şəbəkə sistemləri və s.) təhlükəsizliyi (funsionallığının qorunmuş halında olması) başa düşülür [5].

Yəni, kibertəhlükəsizlik informasiya təhlükəsizliyinin alt sahəsi, bir istiqaməti kimi başa düşülür. Elə bu səbəbdəndir ki, bir sıra qabaqcıl ölkələrin universitetlərində informasiya təhlükəsizliyi və kibertəhlükəsizlik ayrıca ixtisaslar kimi tədris edilir, böyük şirkətlərdə fərqli ixtisas mütəxəssisləri kimi fəaliyyət göstərirlər. Lakin qeyd olunan fərqlərə baxmayaraq hər iki yanaşmanın əsasını eyni üç xüsusiyyət (CIA): məxfilik (Confidentiality), tamlıq (Integrity) və əlyetərlilik (Availability) təşkil etməsidir. Eyniylə də qeyd olunan hər bir anlayış özündə informasiya təhlükəsizliyini və bu təhlükəsizliyi təmin edən müəyyən konkret üsullara, alətlərə, tədbirlərə, o cümlədən kriptoqrafik qorunma üsullarına malikdir [6-7]. Məqalədə dövlət kibersuverenliyi və texnoloji suverenlik kontekstində müəyyən məxfiliyə malik xidməti danışıqların kriptoqrafik və onların texniki təminatı üsullarından istifadə etməklə informasiya təhlükəsizliyinin təmin edilməsi məsələləri araşdırılır.

DOI: 10.25045/cyber.gov.2026.42

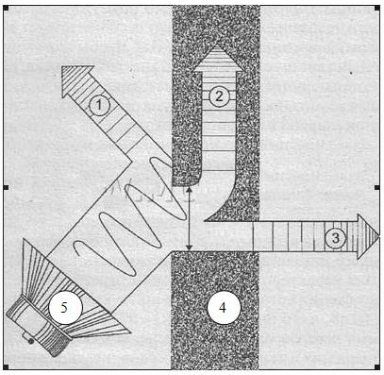
II. XİDMƏTİ DANIŞIQLARIN TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ ZƏRURƏTİ HAQQINDA

İnsanlar arasında ünsiyyət əsas etibarilə danışıqlar, nitq informasiyası vasitəsilə həyata keçirilir. Bu ünsiyyət istər birbaşa danışıqlar, yəni akustik kanallarla, istərsə də texniki vasitələrdən istifadə etməklə elektromaqnit, elektroakustik, vibroakustik, elektrooptik və s. kanallarla həyata keçirilə bilər. Bu danışıqların məzmununda adi məişət məsələlərinə aid məlumatlardan tutmuş şəxslərin fərdi məlumatları, təşkilatın maliyyə və kommersiya sirləri, elmi tədqiqatların nəticələri, hərbi və dövlət sirləri və s. yayılması arzu olunmayan və ya qanunla qadağan olunmuş məlumatlar ola bilər. Burada danışıqların məzmununa münasibətdə maraqları əks olan iki tərəf var: məlumatların digərlərinin əlinə keçməməsində maraqlı olan danışıq iştirakçıları və bu danışıqları əldə etməklə ondan qərəzli məqsədlərlə istifadə etməyə çalışan digər tərəf. Texnika və texnologiyaların hazırkı inkişaf səviyyəsində hər iki tərəfin maraqlarını təmin etməyə imkan yaradan çoxlu sayda mükəmməl texnologiyalar, texniki vasitələr, metodlar yaradılsa da onların tətbiqi zamanı bir sıra çətinliklərlə üzləşirlər. Bu ilk növbədə təşkilatın informasiya təhlükəsizliyi siyasətinin, təhlükəsizliyi təmin edən qorunma/mühafizə taktikasının düzgün formalaşdırılmasından, o cümlədən qorunma məqsədilə düzgün texniki həll variantının seçilməsindən asılıdır. Digər tərəfdən təşkilat rəhbərliyinin informasiyanın qorunması/mühafizəsi problemləri və onların həlli yolları haqqında bilik səviyyəsi və məsələyə münasibəti, təşkilatın maliyyə imkanları və s. informasiya təhlükəsizliyi tədbirlərinin həyata keçirilməsinə təsir edən amillərdəndir. Göründüyü kimi nitq informasiyasının təhlükəsizliyinin təmin edilməsi hər bir fərd, təşkilat və dövlət üçün aktual və əhəmiyyətli məsələdir.

III. SƏS VƏ AKUSTİK KÜY HAQQINDA

Nitq informasiyasının təhlükəsizliyinin təşkilinə aidiyyatı olan hər bir şəxs səsin mahiyyəti, yayılması və qəbulu haqqında minimal məlumatlara malik olmalıdır. Səs havada (qazvari mühitdə), bərk cisimlərdə və mayelərdə dalğalar şəklində yayılan elastik mühitin hissəciklərinin rəqsi hərəkəti nəticəsində yaranır. Səs, o cümlədən nitq dalğaları enerji daşımaqla qarşılaşdığı maneədə müəyyən təzyiq yaradır. Əgər bu təzyiqin qiyməti yayılma mühitinin təzyiqindən, məsələn atmosfer təzyiqindən böyükdürsə müəyyən intensivliyə malik səs yaradır. Bu maneə qulaq pərdəsidirsə biz, dalğa enerjisinin yaratdığı təzyiqi subyektiv olaraq səs hissi kimi qəbul edirik. Bu səs gücü (intensivliyi) və tezliyi ilə xarakterizə edilir. Otaqda danışıqların, hərəkət edən cisimlərin və s. mənbələrin yaratdığı səs dalğalarının enerjisinin bir hissəsi istənilən maneədən əks edərək ətrafa yayılır, bir hissəsi maneə tərəfindən udulur, digər hissəsi isə maneədən keçərək əks tərəfə yayılır (Şəkil 1).

İnsan qulağının eşitməsi üçün səsin qulaqda yaratdığı təzyiqin səviyyəsi nisbi qiymətlərdə sıfır desibeldən (db) və ya mütləq qiymətlərdə 2·10-5 paskaldan (Pa) böyük olmalıdır. Qeyd edək ki, müəyyən şərait üçün normativ sənədlərlə müəyyənləşdirilmiş həddən yüksək intensivliyə malik səslər küy adlanır. Yuxarıda qeyd edilən bu səviyyə sağlam qulağın eşitdiyi ən zəif səsi xarakterizə edir (eşitmə həddi). Digər tərəfdən səviyyəsi 120 db (və ya 1 Pa) olan küylər qulaqda ağrı hissi yaradır və ağrı həddi adlanır.



Şəkil 1. Səs dalğalarının maneə ilə qarşılıqlı təsiri

1-əks edən, 2-udulan, 3-nüfuz edən hissələr, 4-maneə (divar), 5-səs mənbəyi

150 db səviyyəli küylər qulaq pərdəsini deşir, 180-200 db isə insana öldürücü təsir edir. Normal ucalıqda aparılan danışıqların yaratdığı səslər 30-40 db intensivliyinə uyğun gəlir. Normadan artıq hər 12 db səviyyəli səs norma ilə müəyyənləşdirilmiş səs ucalığını (qulağa təsirini) 2 dəfə artırır [8]. Məsələn, qapalı musiqili əyləncə mərkəzlərində (şadlıq sarayları və s.) maksimal ekvivalent səs səviyyəsi 70 db həddində müəyyənləşdirilib, lakin real vəziyyətdə 100-105 db səviyyəsində olur (normadan 7-8 dəfə çox).

IV. NİTQ İNFORMASİYASININ QORUNMASI PROBLEMLƏRİ HAQQINDA

İnformasiya təhlükəsizliyi və məlumatların, o cümlədən fərdi məlumatların əldə edilməsi məsələləri milli qanunvericiliklə tənzimlənir. "AR-in Konstitusiya Qanunu"-na görə şəxsin razılığı olmadan və ya xəbərdar edilmədən onun danışıqlarının yazılması, foto, video çəkilişlərinin aparılması qadağandır (xüsusi hallar istisna olmaqla). Bu, məxfi və dövlət sirri daşıyan məlumatlara da şamil edilir. "Dövlət sirri haqqında" AR-in Qanunu dövlət sirri təşkil edən məlumatlarını üç məxfilik dərəcəsi ilə: xüsusi əhəmiyyətli, məxfi və tam məxfi kimi müəyyənləşdirir (maddə 7) və dövlət sirrinə aid edilən məlumatların qanunla müəyyən edilən təsnifatını təsbit edir (maddə 4). Qanunla belə məlumatların yayılması və qorunması məsuliyyəti vəzifəli şəxslərin, o cümlədən elmi tədqiqat müəssisələrinin rəhbərliyinin üzərinə qoyulur. Məsul şəxslər məxfiliyin pozulmasına görə qanunvericiliyə müvafiq olaraq cinayət, mülki-hüquq və ya inzibati məsuliyyət daşıyırlar (maddə 28) [9].

Şəkil 1-dən göründüyü kimi danışıqlardan yaranan səs rəqsləri dalğalarının bir hissəsi otağın bir çox konstruktiv inşaat elementlərindən nüfuz edərək xaricə yayıla və adi dinləmə yolu ilə əldə edilə bilər. Bu halda pəncərələr (xüsusilə açıq halda), qeyri-metal materiallardan hazırlanmış qapılar, hava tənzimləyici nəfəsciklər, tavan və döşəmə, eləcə də qaz, su, otağı qızdıran isitmə borularının, elektrik kommunikasiya xətlərinin divarlardan keçid yerlərində yaranmış boşluqlar və s. nüfuzedici tərkibin sızma kanalı rolunu oynaya bilər.

Qeyd edək ki, hal-hazırda nitq informasiyasının istər akustik, istərsə də yuxarıda qeyd edilən digər texniki kanallardan icazəsiz əldə edilməsinə qarşı çoxsaylı qorunma vasitələri mövcuddur. Qorunan danışıqların məxfilik statusundan, otaqların inşa konstruksiyasından, təşkilatın maliyyə imkanlarından və s. amillərdən asılı olaraq qiyməti və funksional imkanları kəskin fərqlənən çox sadə və ucuz, eləcə də xüsusi təyinatlı mürəkkəb və baha olan texniki vasitələrdən istifadə edilə bilər.

V. XİDMƏTİ DANIŞIQLARIN BƏZİ KRİPTOQRAFİK QORUNMA ÜSULLARI HAQQINDA

Təcrübə göstərir ki, xidməti danışıqlara aidiyyatda digər qorunma üsullarına (hüquqi, təşkilati, fiziki, texniki və s.) nisbətən kriptoqrafik üsullar daha etbarlıdır. Kriptoqrafik üsulların əsasını qorunan informasiyanın maskalanması prinsipi təşkil edir: informasiya – məqalədə xidməti danışıqlar – səs (nitq) informasiyası müəyyən çevirmələr vasitəsiə bədniyyətli tərəfindən ilkin kontent halında ələ keçirilməsi mümkün olmayan və ya çətin olan hala salınır. Bu məqsədlə istifadə edilən üsullardan bir çoxu qorunan informasiyanın və aparılan danışıqların ətrafa yayılmasını (gücləndirilməsi, filtrasiyası və s.) təmin edən akustik avadanlıqların generasiya edilən akustik küy sahələri ilə maskalanmasına əsaslanır. Ən sadə qorunma metodlarından biri danışıq mühitinin akustik maneə siqnalları ilə küyləndirilməsidir. Bu halda danışıqlarla eyni vaxtda musiqinin, radio-televiziya verilişlərinin səsləndirilməsindən istifadə etmək olar. Belə ki, qulaq, maneə yaradan müxtəlif səs axınlarından faydalı nitqi seçmək kimi psixi-akustik xüsusiyyətə malikdir. Bu zaman kənar səslərlə qarışmış nitq dalğaları otaqdan kənara yayılsa və eşidilsə də anlaşılmaz olur. Metodun çatışmayan cəhəti kənar səslər fonunda iştirakçılar tərəfindən danışıqların dərk edilməsinin çətinləşməsi, müəyyən inamsızlıq və yorğunluq hissinin yaranmasıdır. Digər variantda nitq rəqsləri enerjisinin nüfuzedici tərkibinin azaldılması məqsədilə otağın bütün səthinin səsuducu materiallarla üzlənməsidir (fiziki üsul). Bu məqsədlə səsuducu əmsalı böyük olan mineral pambıq, şüşəlifli və bazalt əsaslı materiallardan, köpükləndirilmiş poliamiddən (paralondan) və s. inşaat üzlük materiallarından istifadə etmək olar. Tavan və döşəmədən xaricə nüfuz edən səs dalğalarını zəiflətmək üçün asma tavan və ikinci qat döşəmə qurmaq olar. Bu halda nüfuzedici tərkibin zəiflədilməsi qeyd edilən maneələrdə səs enerjisinin bir hissəsinin udulması (maneələrin daxilində istilik enerjisinə çevrilməsi) hesabına baş verir. Kriptoqrafik qorunma üsullarından biri kimi otağın konstruktiv elementlərində akustik səs dalğalarının yaratdığı vibrasiyaların xaricdən qəbul edilməsini aradan qaldırmaq üçün xüsusi texniki vasitələrdən istifadə etmək lazım gəlir. Məsələ ondadır ki, danışıqlardan yaranan akustik dalğalar otaq daxilindəki kommunikasiya xətlərində və otağın digər konstruktiv elementlərində (divarlar, tavan, döşəmə, pəncərə, qapı və s.) nitq siqnallarının amplitudasına uyğun vibrasiya yaradır. Bu siqnallar nə qədər zəif olsa da qonşu otaqlardan, divarların xarici səthlərindən xüsusi qurğular vasitəsilə qəbul edilərək ilkin səs siqnallarının bərpa edilməsi üçün istifadə edilə bilər [10]. Bu, xüsusilə pəncərə şüşələrinə, polad borulara və divarlara aiddir. İnformasiyanın bu vibrokanallardan sızmasının qarşısını almaq üçün vibroküyləmə yaradan qurğulardan istifadə edilir: qurğular eşidilən səs diapazonu tezliklərində vibrasiya rəqsləri generasiya edərək qeyd olunan konstruktiv elementlərə nüfuz etdirilir. Bu halda vibrasiyanın həmin elementlərdə yaratdığı rəqslər nitq rəqslərini maskalayaraq bədniyyətlinin əldə etdiyi siqnallardan nitq informasiyasını sintez etmək imkanını aradan qaldırır. Bu məqsədlə qurğunun generasiya etdiyi siqnal konstruksiyalara bərkidilmiş elektrik vibratorlarına verilir və onları müəyyən intensivlikdə rəqsə gətirir. Bu məqsədlə məsələn, “Sonata-AB” markalı vibroküyləyicidən istifadə etmək olar [11].

Lakin bir çox hallarda danışıq iştirakçıları, o cümlədən dəvət edilənlər müasir miniatür yazma qurğularından (ardınca, diktofon) istifadə etməklə nitq informasiyasını gizli yazmaqla əldə edə bilərlər. Bu məqsədlə bədniyyətli miniatür radioötürücü qurğu vasitəsilə nitq siqnallarını otaqdan xaricdə yerləşdirilmiş radioqəbuledici qurğulara ötürə bilər. Ötürmə üçün radio/optik (infraqırmızı tezlik diapazonlu dalğalarla), elektromaqnit və s. kanallardan istifadə etmək olar. Başqa bir halda qurğunun miniatür mikrofon və radioötürücü hissəsini stolda, stulda, otağın digər əşyalarında və ya özünə aid əşyalarda (qələmində, qeyd dəftərində, eynəyində və s.) gizlədə, yazma hissəsini isə bədənində yerləşdirə bilər. Diktofonun bədəndə (geyimdə) gizlədilməsi halından daha çox istifadə olunur. Ona görə də danışıqların məxfiliyinin qorunmasının ən etibarlı yolu maskalanma üsulları ilə onların yazılması imkanının aradan qaldırılmasıdır. Qeyd edək ki, hal-hazırda köhnə tip maqnit kasetli analoq diktofonlardan demək olar ki, istifadə edilmədiyindən mətndə yazma qurğusu dedikdə nitq informasiyasının yazılması üçün sərt disklər, Smart Media, Memory Stick kimi daşıyıcılarla təchiz edilmiş miniatür rəqəmsal diktofonlar nəzərdə tutulur.

Otaqda gedən danışıqların icazəsiz (gizli) yazılmasının qarşısının alınması əsasən iki istiqamətdə aparılır:

- yazma qurğusunun otağa gətirilməsinin aşkarlanması və kənarlaşdırılması (fiziki və texniki üsullar) [12];
- diktofonun elektron sxem dövrəsinin (radioelektron elementlərinin) normal işinin pozulmasına imkan yaradan qurğular qruplarına bölünür (kriptoqrafik və texniki üsullar);
- otağa gətirilmiş diktofonların yazılarının maskalanması (kriptoqrafik üsullar).

Burada maskalanma dedikdə səs (nitq) dalğalarının akustik yayılma mühitinin küy siqnalları ilə qarışdırmaqla yazıların güclü təhrifə uğradılması prosesi başa düşülür. Təhrifə uğradılmış nitq yazıları dinlənilmə rejimində anlaşılmaz səs yazıları kimi (küy kimi) qavranır: mövcud texniki üsullarla nitqi küydən (maneələrdən) ayırmaq mümkün olmur.

İkinci qrup qurğular generasiya etdikləri akustik küy səsləri ilə diktofonun normal işinə əngəl yaratma prinsipinə (akustik küyləmə prinsipi) əsaslanır və əsasən iki alt qrupa bölünür:

- ultrasəs diapazonunda maneə küy siqnallarının yaradılması;
- eşidilən səs diapazonunda maneə küy siqnallarının yaradılması.

Birinci qrup qurğularda akustik küy siqnalı kimi eşidilməyən diapazonlu ultrasəs siqnallarından (20-22 kHs) istifadə edilir. Bu siqnallar diktofonun gücləndiricisinin

amplitud-tezlik xarakteristikasını dəyişərək onun normal yazı rejiminə mane olur. Mikrofonun korpusunun metal materialdan olması (ekranlanması) ehtimalını nəzərə alaraq küy siqnallarının intensivliyini artırmaq lazım gələ bilər. Bu qrup qurğuların (məsələn, VNG 012-U Savesa) təhlükəsizliyi qoruma səviyyəsi daha yüksəkdir.

İkinci qrup qurğularda eşidilən səs diapazonlu tezliklərdə a) “nitqəbənzər” (bir neçə nitq fraqmentlərinin qarışığından alınan səs) küy siqnalları; b) “ağ” küy (səs diapazonunda intensivliyi bərabər paylanan küy siqnalları) və ya c) “narıncı” küy (səs diapazonunda, tezliyin artması istiqamətində, hər növbəti oktava zolağında intensivliyi 3 db azalan səs siqnalları) səsləri yayan generatorlardan istifadə edilir [13]. Danışıqlar bu küy səslərinin fonunda aparılır. Küy səsinin intensivliyi elə seçilir ki, qulağın nitqi küy səsindən ayırmaq xüsusiyyəti öz təsirini itirməsin. Küy səsi ilə nitq səsi qarışığı kiçik ölçülü ucadandanışanlardan səsləndirilir. Çıxış gücü əllə tənzimlənən (“ANG-2000”, “Kabinet”) və danışıq səslərinin intensivliyindən asılı olaraq avtomatik tənzimlənən (“Барон”, “Шорох-1”) olmaqla iki variantda hazırlanır. Sadə və ucuz olmaqla istənilən tip mikrofonun işini əngəlləyir. Bu qrupa daxil olan qurğuların ümumi çatışmayan cəhəti informasiya təhlükəsizliyi tədbirinin aşkar aparılmasıdır. Digər çatışmayan cəhət tədbir təşkilatçıları tərəfindən danışıqların texniki vasitələrlə həyata keçirdikləri yazılışların anlaşıqlıq və fərdi tembr (ahəng) göstəricilərinin pisləşməsidir [14].

NƏTİCƏ

Məqalədə akustik kanallarla ötürülən nitq informasiyasının (danışıqların) təhlükəsizliyi məsələləri və bəzi kriptoqrafik qorunma metodları araşdırılır. Qorunma predmeti otaq daxilində aparılan danışıqlardır. Danışıqların gizli əldə edilməsinin iki variantına baxılır: tədbir iştirakçılarının diktofonla danışıqları gizli yazması və eyni məqsədilə akustik sızma kanalları ilə xaricə yayılan vibroakustik siqnalların qəbulu. Nitq informasiyasının akustik sızma kanalları kimi a) xaricdən danışıqların bilavasitə dinlənilməsinə imkan yaradan konstruktiv elementlər (giriş qapısı, havalandırma sistemləri, kommunikasiya xətlərinin otaqdan çıxış yerləri ilə divar arasındakı boşluqlar və s.); b) vibrosızma kanalları – pəncərə şüşələri, su, qaz, isitmə sistemlərinin metal boru xətləri, divarlar və s. konstruktiv elementlər nəzərdə tutulur. Bu metodlar əsasında yaradılmış bəzi texniki qurğular və onların iş prinsipləri izah edilir. Aparılan danışıqların konfidensiallıq dərəcəsindən, otağın inşaat-konstruktiv xüsusiyyətlərindən, maliyyə imkanlarından və s. amillərdən asılı olaraq xidməti danışıqların təhlükəsizliyini təmin etmək məqsədilə təklif və tövsiyələr verilir.

ƏDƏBİYYAT

[1] C. Thanapat, “Interplay of international law and cyberspace: State sovereignty violation, extraterritorial effects, and the paradigm of cyber sovereignty Chinese,” *Chinese Journal of International Law*, vol. 23, no. 1, pp. 25–72, Mar. 2024, doi: 10.1093/chinesejil/jmae005.

[2] A. Nawazish, A. Afzaal, and I. Z., “Sovereignty and cyber security: Re-thinking state power in the 21st century,” *Indus Journal of Social Sciences*, vol. 3, no. 4, pp. 397–407, Nov. 2025, doi: 10.59075/ijss.v3i4.1995.

[3] А. Я. Капустин, “Суверенитет государства в киберпространстве: международно-правовое измерение,” *Журнал зарубежного законодательства и сравнительного правоведения*, т. 18, № 6, с. 99–108, 2022, doi: 10.12737/jflcl.2022.079.

[4] K. Blind, “Standardization and standards: Safeguards of technological sovereignty?” *Technological Forecasting and Social Change*, vol. 210, p. 123873, 2025, doi: 10.1016/j.techfore.2024.123873.

[5] А. А. Афанасьев, “Технологический суверенитет: сущность, цели и механизм достижения,” *Вопросы инновационной экономики*, т. 15, № 2, с. 469–488, 2025, doi: 10.18334/vinec.15.2.122986.

[6] Н. Ш. Козлова и В. А. Довгаль, “Кибербезопасность и информационная безопасность: сходства и отличия,” *Вестник АГУ*, вып. 3 (286), с. 88–97, 2021, doi: 10.53598/2410-3225-2021-3-286-88-97.

[7] Е. В. Потапцева и В. В. Акбердина, “Технологический суверенитет: понятие, содержание и формы реализации,” *Вестник Волгоградского государственного университета. Экономика*, т. 25, № 3, с. 5–16, 2023, doi: 10.15688/ek.jvolsu.2023.3.1.

[8] “Теоретические основы физической акустики.” [Online]. Available: http://userdocs.ru/fizika/4987/index.html

[9] Azərbaycan Respublikası, “Dövlət sirri haqqında” AR Qanunu. [Online]. Available: http://www.e-qanun.az/framework/3731

[10] V. V. Grishachev, “Detecting threats of acoustic information leakage through fiber optic communications,” *Journal of Information Security*, no. 3, pp. 149–155, 2012.

[11] “Система виброакустической и акустической защиты ‘Соната-АВ’. Руководство по эксплуатации.”

[12] “Система виброакустической и акустической защиты ‘Соната-АВ’.” [Online]. Available: http://www.cbi-info.ru/files/sonata-av3m.pdf

[13] В. Л. Каргашин, “Защита от утечки речевой информации из помещений. Практические аспекты реализации.”

[14] В. Л. Каргашин, “Защита от утечки речевой информации из помещений.” [Online]. Available: http://www.bnti.ru/showart.asp?aid=1024&lvl=04.02.03

[15] ГОСТ 12.1.003-83 (СТ СЭВ 1930-79), *Шум. Общие требования безопасности*.

[16] L. Reva, V. A. Trushin, A. A. Ivanov, and T. V. Borbotko, “Truthfulness of estimation of voice information protection from leakage through technical canals,” in *Proc. Int. Conf. Information Technologies in Business and Industry*, 2016.

[17] L. Reva *et al.*, “Truthfulness of estimation of voice information protection from leakage through technical canals.” [Online]. Available: https://iopscience.iop.org/article/10.1088/1742-6596/803/1/012128/pdf

Cryptographic protection of official negotiations in the context of state cyber sovereignty

Bikas Aghayev, Shakir Mehdiyev, Lale Aliyeva
Institute of Information Technology, Baku, Azerbaijan

Abstract - This article examines and compares related concepts such as "state cyber sovereignty," "technological sovereignty," "ınformation security," "cybersecurity," and others. citing a number of sources, it is argued that information containing varying levels of confidentiality and state secrets, as well as official communications of important government agencies and organizations, can be considered an integral part of a multi-level structured system of state and technological cyber sovereignty. Based on this approach, several cryptographic methods for protecting confidential official communications conducted indoors from secret recording by participants and from obtaining information via vibroacoustic signals leaking outside the premises are considered. To this end, proposals and recommendations are provided.

Keywords - state cyber sovereignty; technological cyber sovereignty; information security; protection of confidential and proprietary negotiations; methods of cryptographic protection.