Rəqəmsal Tibb İnfrastrukturunda Kiber İnsidentlər, Təhdidlər, Risklər və Onların İntellektual Analizi

Babək Nəbiyev[1], Könül Daşdəmirova [2]
ETN İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*babek.nabiyev@gmail.com*, [2]*konulahmed@gmail.com*

***Xülasə*— Tezisdə səhiyyə sektoruna yönəlmiş kibertəhlükələr və onların yaratdığı problemləri təhlil edir. Tibbi kibertəhlükələrin əsas növləri araşdırılır, onların pasiyent təhlükəsizliyinə, fərdi və klinik məlumatların məxfiliyinə, səhiyyə infrastrukturunun stabil fəaliyyətinə təsiri araşdırılır. Rəqəmsal səhiyyə sistemlərinə yönəlmiş qlobal miqyaslı kiberhücumlar və onların nəticələri təhlil edilir. Tibbi infrastrukturlarda kibertəhlükəsizliyin təmin edilməsi üçün həyata keçiriləcək tədbirlər və yanaşmalar təqdim olunur. Səhiyyə sektorunda kibertəhlükələrin effektiv idarə olunması və pasiyent etimadının qoruması məqsədilə milli səviyyədə ixtisaslaşmış Tibbi CERT-nin yaradılması təklif edilir.**

Açar sözlər—Səhiyyə sektorunda kibertəhlükəsizlik; tibbi məlumatların qorunması; fidyə (ransomware) hücumları; fişinq; DDoS; məlumat sızıntısı; pasiyent təhlükəsizliyi; GDPR; HIPAA; rəqəmsal tibb infrastrukturu; Tibbi CERT

I. GIRIŞ

Rəqəmsal texnologiyaların geniş tətbiq olunduğu müasir dövrdə səhiyyə sektoru kiberhücumların hədəfinə çevrilmiş əsas sahələrdən biridir. Elektron sağlamlıq sistemlərinin, rəqəmsal pasiyent məlumat bazalarının və onlayn tibbi xidmətlərin tətbiqi səhiyyə sahəsində yeni imkanlar yaratsa da, eyni zamanda informasiya təhlükəsizliyi risklərini əhəmiyyətli dərəcədə artırır. Tibbi məlumatların yüksək həssaslığı, səhiyyə infrastrukturunun fasiləsiz fəaliyyəti və pasiyent təhlükəsizliyi ilə birbaşa bağlılığı bu sahəni kibercinayətkarlar üçün cəlbedici hədəfə çevirir [1]. Nəticədə, xəstəxana sistemlərinin fəaliyyətində fasilələr yaranması, pasiyent məlumatlarının oğurlanması, tibbi avadanlıqların funksionallığının pozulması və tibbi xidmətin keyfiyyətinin kəskin şəkildə aşağı düşməsi kimi ciddi fəsadlar müşahidə olunur. Bəzi hallarda kiberhücumlar birbaşa pasiyent həyatına təhlükə yaratmaqla yanaşı, səhiyyə müəssisələrinin nüfuzuna və ictimai etimada da zərbə vurur. Bundan əlavə, sistemlərin bərpası və itkilərin aradan qaldırılması böyük maliyyə və texniki resurslar tələb edir ki, bu da səhiyyə sektorunun davamlı fəaliyyətinə mənfi təsir göstərir [2].

Hazırda səhiyyə sektorunda baş verən kiberinsidentlər təkcə texniki deyil, həm də etik, hüquqi və sosial nəticələrə səbəb olan çoxşaxəli problemlər yaradır. Bu səbəbdən səhiyyə sistemlərində informasiya təhlükəsizliyi siyasətinin gücləndirilməsi, kibertəhlükəsizlik standartlarının tətbiqi və bu sahədə ixtisaslı kadr potensialının artırılması prioritet istiqamətlərdən birinə çevrilmişdir. Səhiyyə təşkilatları üçün kiber risklərin düzgün idarə edilməsi, pasiyent məlumatlarının qorunması və xidmət davamlılığının təmin olunması getdikcə daha vacib məsələlərə çevrilir.

II. RƏQƏMSAL TIBB INFRASTRUKTURUNDA BAŞ VERƏN QLOBAL KIBERTƏHLÜKƏLƏRIN NÖVLƏRI

Tədqiqat çərçivəsində rəqəmsal tibbi infrastrukturlarında müşahidə edilən əsas kibertəhlükələr kompleks və çoxistiqamətli yanaşma ilə araşdırılmışdır [3]. İlk növbədə, səhiyyə sahəsində rast gəlinən əsas kibertəhlükə kateqoriyaları müəyyən edilərək, hər bir hücum növünün pasiyentlərin təhlükəsizliyinə, məlumatların məxfiliyinə və səhiyyə xidmətlərinin davamlı fəaliyyətinə təsirləri təhlil olunmuşdur. Bundan əlavə, son illərdə qlobal miqyasda baş vermiş irimiqyaslı tibbi kiberinsidentlər araşdırılaraq onların əməliyyat fəaliyyətində yaratdığı pozuntular, maliyyə itkiləri və digər ciddi nəticələr qiymətləndirilmişdir. Sonda isə mövcud kibertəhlükələrin qarşısının alınması və insidentlərin effektiv idarə edilməsi məqsədilə mövcud yanaşmalar və tətbiq edilən texnologiyalar – xüsusən CERT (Computer Emergency Response Team) kimi xüsusi cavab qrupları və SIEM (Security Information and Event Management) sistemlərinin tətbiqi nəzərdən keçirilmişdir [4].

Aparılmış təhlillər nəticəsində rəqəmsal tibb sahəsində əsas kibertəhlükə kateqoriyaları aşağıdakı kimi təsnif edilmişdir [5, 6]:

- Fidyə proqramı hücumları (ransomware): Hakerlər tərəfindən zərərli fidyə proqramının tibbi müəssisələrin serverlərinə və elektron qeyd sistemlərinə yerləşdirilərək məlumatların şifrələnməsi və sonradan açılması üçün fidyə tələb olunması ilə xarakterizə olunur. Belə hücumlar tibbi xidmətin fasiləsizliyini pozur və pasiyent təhlükəsizliyi baxımından ciddi təhdid yaradır.
- Məlumat oğurluğu: Xəstəxana və klinikalarda saxlanılan fərdi və klinik məlumatlar kibercinayətkarlar tərəfindən oğurlanaraq ya qara bazarda satılır, ya da şantaj və digər bədniyyətli məqsədlərlə istifadə olunur. Nəticədə pasiyent məxfiliyi pozulur və hətta hüquqi müstəvidə ciddi risklər meydana çıxır.
- Fişinq hücumları: Klinika əməkdaşlarına göndərilən saxta elektron məktublar və ya mesajlar vasitəsilə onların sistem giriş məlumatlarının ələ keçirilməsinə yönəlmiş hücumlardır. Bu yolla kiberdələduzlar sanki legitim görsənən məlumatlar vasitəsilə işçiləri aldataraq

DOI: 10.25045/SPCDH4.0.2025.17

sistemə daxil olur və həssas tibbi məlumatlara icazəsiz çıxış əldə edirlər.

- DDoS hücumları (xidmətdən imtina hücumları): Tibbi müəssisələrin veb-saytlarının və onlayn xidmətlərinin eyni anda çoxlu sayda sorğu ilə yüklənməsi nəticəsində sistemin fəaliyyətinin dayanmasına və xidmətlərin əlçatmaz olmasına səbəb olan hücumlardır. Bu, xüsusilə onlayn təcili xidmətlər və məlumat mübadiləsi üçün kritik əhəmiyyət daşıyan resursları iflic vəziyyətinə sala bilər.
- Zəifliklərin istismarı: Tibbi avadanlıqların və proqram təminatının məlum texniki boşluqlarını (zəifliklərini) hədəfə alan hücumlardır. Kibercinayətkarlar mövcud boşluqlardan istifadə edərək tibbi cihazların funksionallığını pozur və ya onları öz nəzarətinə keçirə bilirlər. Nəticədə həyati əhəmiyyətli tibbi aparatların (məsələn, süni tənəffüs cihazlarının) işi dayana və ya yanlış yönləndirilə bilər.
- İnsider təhdidlər: Səhiyyə müəssisəsinin daxilindən qaynaqlanan təhlükələrdir. Bura bilərəkdən və ya bilməyərəkdən işçilər tərəfindən məlumatların sızdırılması, sistemlərin pozulması kimi hallar daxildir. Daxili nəzarət mexanizmlərinin zəifliyi səbəbindən ortaya çıxan bu cür insidentlər informasiya təhlükəsizliyi baxımından xüsusi diqqət tələb edir.

Yuxarıda qeyd olunan kibertəhlükə formaları səhiyyə sisteminin dayanıqlığına, pasiyentlərin hüquqlarına və ümumən cəmiyyətin informasiya təhlükəsizliyinə ciddi mənfi təsir göstərir. Aparılmış təhlillər göstərir ki, belə hücumlar nəticəsində tibbi informasiya sistemlərinin fəaliyyətinin pozulması və dayanması, təcili tibbi xidmətlərin gecikməsi və ya tamamilə dayandırılması, eləcə də kritik tibbi cihazların işləməməsi hallarına rast gəlinir. Bu kimi vəziyyətlər birbaşa pasiyentlərin həyatı və sağlamlığını risk altına qoyur. Məlumat oğurluğu nəticəsində pasiyent məxfiliyinin pozulması ilə yanaşı, təşkilatlar GDPR və HIPAA kimi beynəlxalq normativ aktların tələblərini pozmuş olurlar, bu da hüquqi sanksiyalara və cərimələrə səbəb olmaqla yanaşı, səhiyyə müəssisələrinin nüfuzuna xələl gətirir [7]. Bundan əlavə, kiberhücumların fəsadlarının aradan qaldırılması böyük maliyyə itkiləri ilə müşayiət olunur: bəzi hallarda qurumlar sistemi bərpa etmək və ya şifrələnmiş məlumatları açmaq üçün fidyə ödəməyə məcbur qalırlar, xidmətlərin dayanması isə əlavə iqtisadi zərərlər doğurur. Beləliklə, tibbi kibertəhlükələr həm birbaşa tibbi xidmətin keyfiyyətini və pasiyent təhlükəsizliyini, həm də dolayısı ilə hüquqi və maliyyə dayanıqlığını təhdid edir.

Kibertəhlükələrin sürətlə yayıldığı bir şəraitdə tibbi müəssisələrdə kiberrisklərin qiymətləndirilməsi mühüm əhəmiyyət kəsb edir. Hazırda elektron tibbi infrastrukturlarda kiber risklərin qiymətləndirilməsi üçün NIST, ISO/IEC 27005, OCTAVE və FAIR kimi tanınmış beynəlxalq metodologiyalardan istifadə olunur [8].

ABŞ Milli Standartlar və Texnologiya İnstitutu (NIST) tərəfindən təqdim edilən NIST Risk Management Framework (RMF) metodologiyası ən çox tətbiq edilən yanaşmalardan biridir. Bu metodologiya tibbi infrastrukturun fəaliyyət dövrü boyunca risklərin idarə olunmasına imkan verir. Xüsusilə, NIST SP 800-30 və SP 800-37 sənədləri risklərin müəyyənləşdirilməsi, ehtimal və nəticələrin təhlili, riskin qiymətləndirilməsi və onun azaldılması proseslərini əhatə edir.

ISO/IEC 27005 standartı da geniş istifadə olunan yanaşmalardan biridir. Bu standart, ISO/IEC 27001 və 27002 ilə inteqrasiya edilə bilən informasiya təhlükəsizliyi idarəetmə sistemləri çərçivəsində risklərin müəyyən edilməsi, təhlili, qiymətləndirilməsi və idarə olunması üçün əlverişli mexanizm təqdim edir.

Məhdud resurslara malik kiçik təşkilatlar üçün isə OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) metodologiyası daha uyğun sayılır [9]. Bu yanaşma təşkilat üçün kritik əhəmiyyət daşıyan informasiya resurslarını, onlara qarşı mövcud təhlükələri və zəiflikləri müəyyən etməyə imkan verir.

Səhiyyə sektoru üçün ISO/IEC 27005 və NIST SP 800-30 metodlarının birgə tətbiqi, xüsusilə fərdi tibbi məlumatların mühafizəsi sahəsində daha effektiv və praktik hesab olunur.

III. DÜNYA ÜZRƏ BAŞ VERMIŞ ƏSAS TIBBI KIBERTƏHLÜKƏLƏR VƏ INSIDENTLƏR

Rəqəmsal tibbi infrastrukturlara yönəlmiş təhdidlərin analizi göstərir ki, tibbi informasiya sistemlərinə qarşı kiberhücumların həm sayı, həm də təsir dairəsi əhəmiyyətli dərəcədə artmaqdadır. 2017-ci ilin may ayında baş vermiş WannaCry fidyə proqramı hücumu 150-dən çox ölkəni əhatə edən qlobal kiberinsidentə çevrilmişdir [10]. Bu hücumdan ən çox zərər çəkən qurumlardan biri Böyük Britaniyanın Milli Səhiyyə Xidməti (NHS) olmuşdur. Minlərlə xəstəxana kompüteri şifrələnmiş, təcili tibbi yardım da daxil olmaqla bir çox xidmət iflic vəziyyətinə düşmüş və 19 minə yaxın tibbi görüş ləğv edilmişdir. Hadisə nəticəsində NHS milyonlarla funt sterlinq dəyərində maliyyə itkisinə uğramış və milli səhiyyə sistemində ciddi əməliyyat pozuntuları yaranmışdır.

2020-ci ildə ABŞ-da fəaliyyət göstərən və 400-dən çox xəstəxana və klinikanı birləşdirən Universal Health Services (UHS) şəbəkəsi genişmiqyaslı fidyə hücumuna məruz qalmışdır [11]. Hücum nəticəsində UHS-in elektron sistemləri tamamilə sıradan çıxmış, tibb personalı müvəqqəti olaraq kağız əsaslı sənəd dövriyyəsinə keçməyə məcbur olmuşdur. Nəticədə təcili tibbi yardım da daxil olmaqla bir çox kritik xidmətlərin göstərilməsində gecikmələr baş vermiş və sistemlərin bərpası təşkilata 67 milyon ABŞ dollarından çox zərər vurmuşdur. Digər bir əhəmiyyətli hadisə 2018-ci ildə Sinqapurun ən iri səhiyyə təminatçısı olan SingHealth qurumunda baş vermiş məlumat sızıntısıdır. Bu hücum zamanı 1,5 milyon pasiyentin (o cümlədən Sinqapur Baş nazirinin) fərdi tibbi məlumatları oğurlanmış və bir qismi qara bazarda satışa çıxarılmışdır. Hadisədən sonra xəstəxananın bütün informasiya təhlükəsizliyi protokolları yenidən nəzərdən keçirilmiş və ciddi islahatlar aparılmışdır.

2021-ci ildə ABŞ-da Scripps Health adlı səhiyyə təşkilatı kiberhücuma məruz qalaraq dörd həftə ərzində fəaliyyətini qismən dayandırmalı olmuşdur. Ransomware hücumu nəticəsində Scripps-in elektron sağlamlıq qeydləri (EHR) sistemləri işləməz hala düşmüş, pasiyentlərin müalicə prosesində ciddi fasilələr yaranmış və 113 mindən çox pasiyent

məlumatı sızmışdır. Bu insidentin təşkilata vurduğu maliyyə zərəri 112 milyon ABŞ dollarını keçmişdir.

Avropa ölkələri də oxşar təhlükələrlə üzləşmişdirlər. 2021-2022-ci illərdə Fransanın bir sıra xəstəxanalarına qarşı ardıcıl DDoS və fidyə hücumları həyata keçirilmişdir. Xüsusilə, 2022-ci ildə baş vermiş bir hadisədə Paris regionundakı Corbeil-Essonnes xəstəxanası kiberhücum səbəbindən fəaliyyətini tamamilə dayandırmalı olmuş və bəzi pasiyentlərin digər tibb müəssisələrinə təxliyə edilməsi tələb olunmuşdur. Hücumun yaratdığı birbaşa zərər 10 milyon avrodan çox dəyərləndirilmişdir.

Baş vermiş qlobal insidentlər göstərir ki, kibertəhlükələr səhiyyə sistemi üçün beynəlxalq miqyasda real təhdid təşkil edir və hər bir ölkənin səhiyyə infrastrukturu bu cür hücumlardan ciddi şəkildə zərər görə bilər. Nəticədə, tibbi kibertəhlükələrlə mübarizə mövzusu bütün dünyada səhiyyə sektorunun gündəmində olan kritik məsələlərdən birinə çevrilmişdir. Belə şəraitdə səhiyyə infrastrukturunda kibertəhlükəsizliyin təmin olunması kompleks və çoxşaxəli yanaşma tələb edir. Rəqəmsallaşma prosesinin sürətlənməsi və tibbi xidmətlərin elektron resurslardan asılılığının artması şəraitində tibbi məlumatların və sistemlərin mühafizəsi strateji əhəmiyyət kəsb edir. Effektiv kibermüdafiə üçün həm hər bir səhiyyə müəssisəsi səviyyəsində, həm də sektoral (milli) səviyyədə ardıcıl tədbirlər həyata keçirilməlidir.

İlk növbədə, hər bir səhiyyə təşkilatı daxilində proaktiv təhlükəsizlik tədbirləri planlaşdırılmalıdır. Rəqəmsal tibb infrastrukturu üçün təhlükəsizlik strategiyasının hazırlanması əsas şərtlərdəndir. Müəssisələr öz kiber risk profillərini dəyərləndirməli, mövcud texnoloji infrastrukturu nəzərə alaraq uyğun təhlükəsizlik siyasəti formalaşdırmalıdır. Bu istiqamətdə atılacaq başlıca addımlar aşağıdakılardır:

- Risk əsaslı təhlükəsizlik siyasəti: Hər bir tibb müəssisəsi informasiya təhlükəsizliyi siyasətini və prosedurlarını tərtib etməlidir. Potensial təhdid və zəiflikləri öncədən müəyyən etmək üçün mütəmadi risk analizləri aparılmalı, insidentlərə qarşı fövqəladə hallara cavab planları hazırlanmalıdır. Risklərin davamlı izlənməsi və yenidən qiymətləndirilməsi sayəsində qurum mümkün hücumlardan əvvəlcədən xəbərdar olub müvafiq qabaqlayıcı addımlar ata bilər.
- Texniki infrastrukturun gücləndirilməsi: Tibbi sistemlərdə informasiya texnologiyalarının müdafiəsi ən müasir tələblərə uyğun qurulmalıdır. Xüsusilə, şəbəkə mühiti güclü firewall və müdafiə divarları, antivirus və antispyware proqramları ilə qorunmalıdır. Kritik server və məlumat bazaları real vaxt rejimində monitorinq edilərək Security Information and Event Management (SIEM) kimi platformalar vasitəsilə loqların analizi həyata keçirilməlidir. Elektron Sağlamlıq Qeydləri (EHR) kimi kritik məlumat sistemləri mütləq şəkildə şifrələnməli, müntəzəm ehtiyat nüsxələri alınmalı və etibarlı mühitlərdə saxlanılmalıdır. Köhnəlmiş və dəstək almayan tibbi avadanlıq və proqramlar vaxtında yenilənməli və ya müasir ekvivalentlərlə əvəzlənməlidir ki, texniki boşluqlar minimal olsun.
- İnsan amilinə qarşı tədbirlər: Tədqiqatlar göstərir ki, səhiyyə sektorunda kiberinsidentlərin əhəmiyyətli bir qismi insan səhvlərindən qaynaqlanır. Bu səbəbdən, səhiyyə personalının kiber gigiyena qaydaları barədə məlumatlılığını artırmaq vacibdir. Mütəmadi olaraq bütün səviyyələrdə – həkimlər, tibbi heyət, inzibati personal və İT mütəxəssisləri üçün kibertəhlükəsizlik üzrə təlimlər və maarifləndirmə sessiyaları keçirilməlidir. Belə proqramlar fişinq hücumlarına qarşı ayıq-sayıqlığı, güclü parol siyasətinə riayət etməyi, sosial mühəndislik cəhdlərini tanıma bacarığını aşılayır. Nəticədə istifadəçilərin fərdi məsuliyyəti yüksəlir və ümumilikdə təşkilatın təhlükəsizlik mədəniyyəti formalaşır.

Hazırda bir çox sahələrdə olduğu kimi, səhiyyə sektorunda da, xüsusilə rəqəmsal tibbi infrastrukturların kibertəhlükəsizliyinin təmin edilməsində süni intellekt (Sİ) texnologiyalarından geniş istifadə olunur. Süni intellekt alqoritmləri real vaxt rejimində şəbəkə trafikini, istifadəçi davranışlarını və sistem hadisələrini analiz edərək şübhəli fəaliyyətləri vaxtında aşkarlamaq imkanına malikdir. Bu texnologiyalar eyni zamanda həssas tibbi məlumatların şifrələnməsini təmin edir və elektron tibbi qeydlərə icazəsiz girişlərin qarşısını almaqda mühüm rol oynayır.

Maşın təlimi əsaslı yanaşmalar fişinq hücumları və qeyri-normal davranışları yüksək dəqiqliklə müəyyən edərək, potensial məlumat sızmaları barədə qabaqlayıcı xəbərdarlıqlar təqdim edir. Sİ əsaslı sistemlər tibbi İT infrastrukturunu davamlı şəkildə təhlil edir, zəif parolları, qorunmamış və ya düzgün konfiqurasiya olunmamış IoT cihazlarını müəyyənləşdirərək potensial hücum vektorlarını proqnozlaşdırır və bu risklərə qarşı avtomatlaşdırılmış cavab tədbirləri həyata keçirir.

Xüsusilə pasiyentlərin təhlükəsizliyi təmin olunması baxımından kritik əhəmiyyətə malik olan IoT cihazların qorunması sahəsində süni intellekt texnologiyalarının tətbiqi prioritet təşkil edir. Bu texnologiyalar cihazların davranış modellərinə nəzarət edir, məsələn, məlumatların icazəsiz olaraq xarici resurslara ötürülməsi kimi şübhəli halları aşkar edir və bu cür zərərli fəaliyyətləri dərhal bloklayır [12].

Bununla yanaşı, süni intellekt səhiyyə işçiləri üçün təlim və maarifləndirmə platformalarının hazırlanmasında da istifadə olunur. Belə platformalar işçilərin rəqəmsal savadlılığını artırmaq, onların kibertəhlükəsizlik sahəsində bilik və bacarıqlarını qiymətləndirmək və fərdi inkişaf planları təklif etmək üçün effektiv alətə çevrilmişdir.

Yuxarıdakı tədbirlər hər bir müəssisə səviyyəsində tətbiq edilməli olsa da, səhiyyə sektorunun kibertəhlükələrə qarşı dayanıqlılığını təmin etmək üçün sektoral (ölkə miqyasında) koordinasiyalı yanaşmaya ehtiyac vardır.

Bu kontekstdə, milli səviyyədə ixtisaslaşmış Tibbi CERT (Computer Emergency Response Team) strukturunun yaradılması vacib hesab olunur (şəkil 1).

Tibbi CERT – səhiyyə sahəsinə yönəlmiş kibermühitin qorunması üçün ixtisaslaşmış operativ cavab və koordinasiya qrupudur.

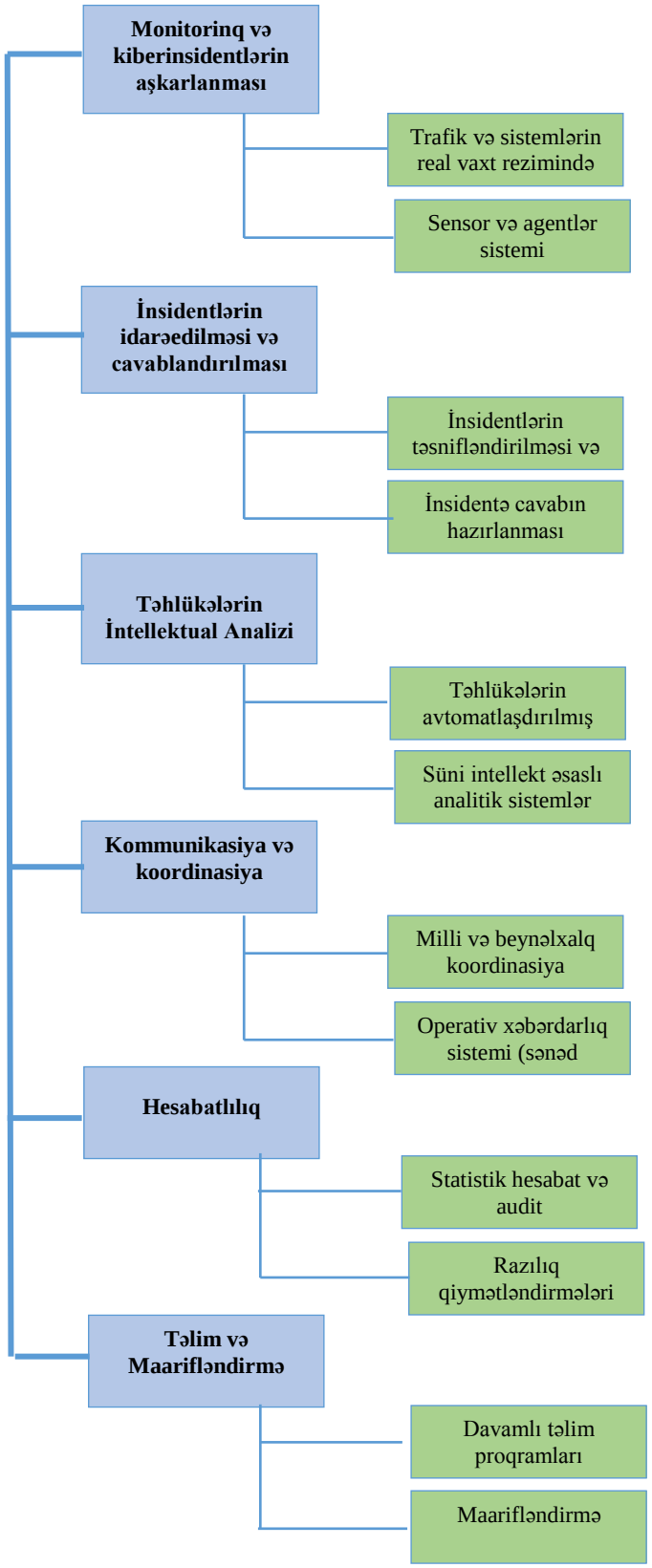
Belə bir qurum səhiyyə sektorunda baş verən kiberinsidentlərə qarşı vahid mərkəzdən, koordinasiyalı şəkildə cavab verilməsini təmin edə bilər.

Tibbi CERT eyni zamanda sektorda kiber təhlükə kəşfiyyatı (threat intelligence) funksiyasını icra edərək, aktual təhdidlər barədə məlumat mübadiləsini sürətləndirər və zəruri xəbərdarlıqları bütün səhiyyə şəbəkəsinə çatdırar. Bu cür milli koordinasiya qurumu səhiyyə sektorunda kibertəhlükəsizliyin idarə olunmasında mərkəzi rol oynayaraq, ayrı-ayrı tibb müəssisələrinin resurs və bilgi mübadiləsini də asanlaşdırar.

IV. KIBERTƏHLÜKƏSIZLIYIN TƏMIN OLUNMASIMDA TIBBI CERT-IN ƏSAS FUNKSIYALARI

Təklif olunan Tibbi CERT-in əsas funksional istiqamətlərini aşağıdakı kimi ümumiləşdirmək olar:

- Real vaxt rejimində monitorinq və insident reaksiyası: Tibbi CERT səhiyyə təşkilatlarının şəbəkə və sistemlərini 24/7 rejimində izləyərək kiberinsidentləri erkən mərhələdə aşkarlamalı və təsnif etməlidir. Aşkarlanmış hücumlara (istər fidyə, istər fişinq, DDoS və s.) operativ texniki cavab tədbirləri görülməlidir – zərərverici fəaliyyətlər dərhal bloklanmalı, yoluxmuş sistemlər təmizlənməli, və zəruri hallarda müvəqqəti alternativ həllər tətbiq olunmalıdır. Bu cür operativ reaksiya sayəsində hücumların təsiri minimuma endirilər və tibbi xidmətlərin fasiləsizliyi mümkün qədər tez bərpa olunar.
- Təhlükələrin intellektual analizi və zəifliklərin aşkarlanması: Tibbi CERT kibertəhlükə kəşfiyyatı (Cyber Threat Intelligence) mərkəzi rolunda çıxış edərək səhiyyə sektoruna yönəlmiş aktual təhdid vektorlarını, yeni ortaya çıxan zəifliklərı və hücum metodlarını izləyir. Topladığı məlumatları təhlil edərək aidiyyəti təşkilatlarla paylaşır. Bu prosesdə SIEM texnologiyalarının tətbiqi xüsusi əhəmiyyət daşıyır – SIEM platforması vasitəsilə müxtəlif sistemlərin loqları toplanıb korelyasiya olunur, anomaliyalar avtomatik aşkarlanır, risklərin dərəcəsi qiymətləndirilir və xəbərdaredici siqnallar yaradılır. Beləliklə, mümkün hücumlar baş vermədən öncə müəyyən edilə və qabaqlayıcı texniki tədbirlər həyata keçirilə bilər. Bu intellektual analiz komponenti rəqəmsal tibb infrastrukturunun dayanıqlığını təmin etmək baxımından mühüm rol oynayır.
- Kibertəhlükəsizlik üzrə təlim və maarifləndirmə: Tibbi CERT, həm səhiyyə işçilərinin (həkimlər, tibb bacıları və s.), həm də İT heyətinin kibertəhlükələrə qarşı bilik və bacarıqlarını artırmaq üçün müntəzəm təlim proqramları həyata keçirməlidir. Simulyasiya edilmiş kiberhücum ssenariləri, praktiki seminarlar və maarifləndirmə kampaniyaları vasitəsilə tibbi personalın kibertəhdidlərə hazırlıq səviyyəsi yüksəldilir. Nəticədə, sektordakı insan amilindən qaynaqlanan risklər azalır və insidentlərə qarşı institusional kollektiv immunitet güclənir.
- Beynəlxalq və sektorarası əməkdaşlıq: Tibbi CERT yalnız lokal səhiyyə müəssisələri ilə deyil, həm də qlobal kibertəhlükəsizlik şəbəkələri ilə sıx əməkdaşlıq qurmalıdır. Dünyada fəaliyyət göstərən FIRST (Forum of Incident Response and Security Teams), US-CERT, WHO Health CERT kimi insident cavab şəbəkələri və Avropa İttifaqının ENISA



Şəkil 1. Tibbi CERT-in strukturu.

(European Union Agency for Cybersecurity) kimi qurumları ilə informasiya mübadiləsi aparmaq vacibdir. Bu əməkdaşlıqlar sayəsində transsərhəd xarakterli kibertəhdidlər barədə operativ məlumat alına bilər və beynəlxalq hücum kampaniyalarına qarşı çevik reaksiya verilməsi mümkün olar. Həmçinin, Tibbi CERT vasitəsilə ölkədaxili müxtəlif sektorlar (məsələn, enerji, telekommunikasiya və s.) arasında da kiber təhdidlərə dair koordinasiya aparıla bilər ki, səhiyyə ilə əlaqəli infrastrukturun qorunması daha hərtərəfli təmin edilsin.Standartların və siyasətlərin formalaşdırılması: Tibbi CERT səhiyyə müəssisələrinə kibertəhlükəsizlik sahəsində metodoloji dəstək göstərərək sektorda vahid standartların formalaşdırılmasına yardım edə bilər. Bu, tibb sektorunda informasiya təhlükəsizliyi üzrə normativlər, protokollar və ən yaxşı təcrübələrin hazırlanmasını və tətbiqini əhatə edir. Belə texniki-məsləhət dəstəyi nəticəsində səhiyyə təşkilatlarının informasiya təhlükəsizliyi üzrə uyğunluq (compliance) səviyyəsi yüksəlir və milli kibertəhlükəsizlik strategiyalarına sektorial inteqrasiya güclənir.

Beynəlxalq təcrübə də göstərir ki, səhiyyə sektoruna özəl kibertəhlükəsizlik qurumlarının yaradılması effektiv nəticələr verə bilər. Məsələn, Amerika Birləşmiş Ştatlarında səhiyyə sektorunun kibertəhlükələrə qarşı müdafiəsi Health Sector Cybersecurity Coordination Center (HC3) adlı ixtisaslaşmış mərkəz tərəfindən əlaqələndirilir [13]. ABŞ Səhiyyə və İnsan Xidmətləri Departamentinin (HHS) nəzdində fəaliyyət göstərən HC3 xəstəxana və klinikalara kibertəhdidlər barədə operativ bildirişlər göndərir, analitik hesabatlar hazırlayır və sektor daxilində informasiya mübadiləsini təşkil edir. Almaniyada səhiyyə sahəsində kiber müdafiə üçün De.CERT Gesundheit adlı xüsusi CERT strukturundan istifadə olunur [14]. Bu qurum ölkənin səhiyyə sisteminə aid təşkilatlara insidentlərin aşkarlanması, texniki müdaxilə, zəifliklərin analizi və personalın təlimi sahələrində dəstək verir. Avropa İttifaqı miqyasında isə ENISA agentliyi səhiyyə də daxil olmaqla müxtəlif kritik sektorlar üzrə kibertəhlükəsizlik strategiyalarının hazırlanmasına töhfə verir və üzv ölkələr arasında informasiya təhlükəsizliyi mexanizmlərinin uzlaşdırılmasına yardım edir [15]. Bu nümunələr göstərir ki, tibbi sahədə ixtisaslaşmış kibertəhlükəsizlik komandalarının fəaliyyəti beynəlxalq miqyasda artıq praktikaya çevrilməkdədir və ölkəmiz üçün də belə bir strukturun formalaşdırılması aktualdır.

NƏTICƏ

Rəqəmsal tibbi infrastrukturların sürətli inkişafı fonunda kibertəhlükəsizlik səhiyyə sektorunun ən vacib çağırışlarından birinə çevrilmişdir. Tədqiqatda aparılan təhlillər göstərir ki, rəqəmsal tibb mühitində kiber insidentlərin potensial təsiri çox ağır ola bilər. Pasiyentlərin həyati təhlükəsizliyi, məlumat məxfiliyi, xidmətlərin fasiləsizliyi və s. kimi sahələri ətahə edən geniş spektrli risklər mövcuddur. Səhiyyə təşkilatlarının bu təhdidlərə qarşı dayanıqlı olması üçün sistemli və inteqrasiya edilmiş yanaşma zəruridir. Əldə olunan nəticələrə əsasən, tibbi kibertəhlükələrə qarşı mübarizədə həm texnoloji, həm təşkilati, həm də insan faktorunu əhatə edən kompleks tədbirlər görülməlidir. Hər bir tibb müəssisəsində güclü informasiya təhlükəsizliyi mədəniyyəti formalaşdırılmalı, qabaqlayıcı texniki həllər tətbiq olunmalı və personal mütəmadi təlimləndirilməlidir. Bununla yanaşı, sektoral səviyyədə vahid koordinasiya mexanizminin – Tibbi CERT-in yaradılması – səhiyyə şəbəkəsində məlumat mübadiləsinin sürətləndirilməsi, insidentlərə operativ cavab verilməsi və ümumi kiberdayanıqlığın artırılması baxımından mühüm addımdır. Nəticə etibarilə, təklif edilən yanaşmaların həyata keçirilməsi rəqəmsal tibb infrastrukturunda baş verən kiber insidentlərin sayını və təsirini minimuma endirməyə imkan verəcək. Bu isə pasiyentlərin etimadının qorunmasını, tibbi xidmətlərin fasiləsizliyini və rəqəmsal səhiyyə innovasiyalarının davamlı olaraq təhlükəsiz şəkildə tətbiqini təmin edəcək. Səhiyyə sektorunda kibertəhlükəsizliyin gücləndirilməsi üçün davamlı səylər göstərilməli və yeni ortaya çıxan təhdidlərə uyğun olaraq strategiyalar mütəmadi şəkildə yenilənməlidir. Yalnız bu halda rəqəmsal səhiyyənin verdiyi imkanlardan tam faydalanmaqla yanaşı, həmin infrastrukturun təhlükəsizliyini və dayanıqlılığını təmin etmək mümkün olacaqdır.

İSTINADLAR

[1] А. А. Попкова, К. В. Парфенов, А. Р. Алборов, “Угрозы информационной безопасности в государственном секторе России,” Известия высших учебных заведений. Социология. Экономика. Политика. 2024,Т. 17. №. 4. pp.77-93.

[2] K. S. Bhosale, M. G. A Nenova, G. Iliev, “A study of cyber attacks: In the healthcare sector //2021 sixth junior conference on lighting,” IEEE, 2021, pp. 1-6.

[3] P. Yeng et al, “SecHealth: Enhancing EHR Security in digital health transformation,” Proceedings of the 8th International Conference on Sustainable Information Engineering and Technology. 2023, pp.538-544.

[4] R. Alguliyev, B. Nabiyev, K. Dashdamirova, “CTI Challenges and Perspectives as a Comprehensive Approach to Cyber Resilience,” 2023 5th International Conference on Problems of Cybernetics and Informatics (PCI). IEEE. 2023, pp.1-5.

[5] M. Nandan et al, “Telemedicine (e-Health, m-Health): Requirements, Challenges and Applications,” Designing Intelligent Healthcare Systems, Products, and Services Using Disruptive Technologies and Health Informatics. 2022, pp.1-25.

[6] E. A. Al-Qarni, “Cybersecurity in healthcare: A review of recent attacks and mitigation strategies,” International Journal of Advanced Computer Science and Applications. 2023, pp.135-140

[7] R. Preston, “Stifling innovation: how global data protection regulation trends inhibit the growth of healthcare research and start-ups,”Emory Int'l L. Rev. 2022, T. 37. pp. 135.

[8] S. Memon et al., “Cyber security risk assessment methods for smart healthcare,” 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC). IEEE, 2024., pp. 1-6.

[9] C. J. Alberts et al., “Operationally critical threat, asset, and vulnerability evaluation (OCTAVE) framework,” version 1.0, 1999.

[10] M. A. Branquinho, “Ransomware in industrial control systems. What comes after Wannacry and Petya global attacks?,” WIT Trans. Built Environ. 2018, pp. 329-334.

[11] T. I. Adeyinka, K. I. Adeyinka, “Reducing the Carbon Footprint in Healthcare Cybersecurity Threats in AI-Powered Healthcare Systems Data Privacy in AI-Driven Diagnostics,” AI-Driven Healthcare Cybersecurity and Privacy. IGI Global Scientific Publishing, 2025, pp. 283-326.

[12] A. H. Ameen, M. A. Mohammed, A. N. Rashid, “Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions,” Journal of Intelligent Systems, 2023, T. 32, №. 1. p. 20220267.

[13] Health Sector Cybersecurity Coordination Center (HC3), https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

[14] Internetpräsenz der WIESO CERT, http://www.wieso-cert.de/

[15] ENISA is the EU agency dedicated to enhancing cybersecurity in Europe, https://www.enisa.europa.eu/