# E-səhiyyə: İnformasiya Təhlükəsizliyinin Aktual Problemləri

Yadigar İmamverdiyev
AMEA İnformasiya Texnologiyaları İnstitutu
*yadigar@lan.ab.az*

***Xülasə*— E-səhiyyə keyfiyyətli tibbi xidmətlərin və məlumatların bütün cəmiyyətə əlyetərliyi sahəsində müxtəlif perspektivlər vəd edir. Bununla yanaşı, şəxsi həyatın toxunulmazlığı və informasiya təhlükəsizliyi baxımından bir sıra təhlükələrə də yol açır. Bu işdə e-səhiyyə sahəsində əsas inkişaf tendensiyalarına qısa nəzər salınır, əsas informasiya təhlükəsizliyi təhdidləri potensial risk baxımından xarakterizə olunur və informasiya təhlükəsizliyinin təmin edilməsinin vacib mexanizmləri analiz edilir. E-səhiyyə sistemlərində, o cümlədən simsiz bədən sensorları şəbəkələrində informasiya təhlükəsizliyinin təmin edilməsinin aktual elmi-praktiki problemləri identifikasiya edilir.**

***Açar sözlər— e-səhiyyə; m-səhiyyə; fərdi tibbi məlumatlar; informasiya təhlükəsizliyi; gizlilik; de-identifikasiya; WSBN.***

## I. GİRİŞ

İnsanın sağlamlığı əhəmiyyətli sosial dəyərdir və hər hansı bir ölkənin inkişaf və rifah səviyyəsi barəsində ölkə əhalisinin sağlamlıq vəziyyətinə və səviyyəsinə görə fikir yürütmək olar. Əhalinin sağlamlığının yüksək səviyyədə təmin edilməsi ciddi sosial-siyasi problemdir və onun həlli bütün cəmiyyətin səylərini birləşdirməyi tələb edir. Səhiyyə sistemi ölkənin sosial-iqtisadi yüksəlişi üçün fundament yaradan əmək resurslarının istehsalını və keyfiyyətini təmin edir.

Müasir informasiya və kommunikasiya texnologiyaları (İKT) səhiyyədə innovasiyalar üçün prinsipal yeni imkanlar yaradır. Elektron səhiyyə (e-səhiyyə, *ing.* eHealth) İKT-dən istifadə edərək xəstəliklərin qarşısının alınması, diagnostikası, müalicəsi, monitorinqi və səhiyyənin menecmentini yaxşılaşdıra bilən alətləri və xidmətləri bildirir (1990-cı illərin ortalarına kimi teletibb termini geniş işlədilirdi) [1]. E-səhiyyə səhiyyə xidmətlərinin əlyetərliyini və keyfiyyətini yaxşılaşdırmaqla və səhiyyə sektorunu daha effektiv etməklə bütün cəmiyyətə fayda verir.

E-səhiyyə 2003-cü ildə informasiya cəmiyyəti üzrə Cenevrə sammitində müzakirə edilmişdi, 2005-ci ildə isə ÜST (Ümumdünya Səhiyyə Təşkilatı) e-səhiyyə üzrə müvafiq qətnamə qəbul etmişdi. Həmin dövrdən ölkələr e-səhiyyənin inkişafı üzrə öz milli strategiyalarını formalaşdırmağa və həyata keçirməyə başlayırlar [2].

E-səhiyyənin formalaşdırılması və inkişafı bir sıra siyasi (strategiya), qanunvericilik (standartlaşdırma), sosial, iqtisadi, texnoloji və s. problemlərlə müşahidə edilir [3]. Bu sahədə əhəmiyyətli problemlərdən biri də informasiya təhlükəsizliyinin təmin edilməsidir [4]. Tibb müəssisələrində əhəmiyyətli həcmdə konfidensial informasiya emal edilir, burada həm pasiyentlərin və tibb işçilərinin fərdi məlumatları, həm də müalicə sirri vardır. Bu öz növbəsində tibbi informasiya sistemlərinin informasiya təhlükəsizliyinin yüksək səviyyədə təmin edilməsini tələb edir, çünki belə sistemlərdə informasiya təhlükəsizliyinin pozulması birbaşa insan həyatına təhdidlər törədə bilər [4-7].

Bu işin məqsədi e-səhiyyə mühitində informasiya təhlükəsizlliyi və fərdi məlumatların konfidensiallığı üzrə elmi-praktiki tədqiqatların müasir vəziyyətini analiz etmək və aktual tədqiqat istiqamətlərini müəyyən etməkdir.

## II. E-SƏHİYYƏ: ƏSAS TENDENSİYALAR

Dünya ölkələri e-səhiyyənin inkişafında müəyyən mərhələləri keçiblər, bunu ÜST-nin hesabatları əks etdirir [8]. Bir sıra ölkələrdə müvafiq qanunvericilik bazasının yaradılması istiqamətində işlər aparılır, e-səhiyyənin arxitekturası müəyyən edilib, infrasturukturun bir sıra komponentləri yaradılıb, istismara müxtəlif tibbi informasiya sistemləri və servislər daxil edilib. E-səhiyyədə informasiya təhlükəsizliyi problemlərini identifikasiya etmək üçün e-səhiyyədə hazırki mərhələdə baş verən əsas tendensiyaları analiz etmək zəruridir. Bu məqsədlə aşağıda əsas tendensiyaların qısa təhlili verilir.

### *Tibbi məlumatların rəqəmsallaşdırılması*

E-səhiyyə vətəndaşlar üçün tibbi yardımın maksimal əlyetərliyininə yönəlib və həkimə onun və pasiyentin yerləşdiyi məkandan asılı olmayaraq bütün zəruri informasiyanın verilməsini və məsafədən məsləhət imkanını nəzərdə tutur. Təsadüfi deyil ki, e-səhiyyənin mərkəzi konsepsiyası elektron sağlamlıq kartı sistemidir [9]. Əvvəllər kağız üzərində olan məlumatlar rəqəmsallaşdırılaraq paylanmış verilənlər bazalarından ibarət olan informasiya sistemində toplanır. Elektron sağlamlıq kartı özündə şəxsi, tibbi (xəstəlik tarixi, müayinə, müalicə, cari istifadə edilən dərman preparatları, qan qrupu, peyvəndlər və s.) və sığorta məlumatlarını cəmləşdirir və kart sahibinə keyfiyyətli, effektiv və operativ tibbi xidmət almaq imkanı verir.

Qeyd edək ki, ingilis dilli mənbələrində daha çox "Electronic Health Record (EHR)", "Electronic Medical Record (EMR)" və "Electronic Case Record (ECR)" terminləri istifadə edilir [10]. Elektron tibb kartları üzrə rus dilində terminologiya məsələləri [11]-də müzakirə edilir. Bir sıra ölkələrdə EHR sistemlərinin yaradılmasını və istifadəsini təşviq edən qanunlar qəbul edilmişdir. ABŞ-da səhiyyənin informasiyalaşdırılmasının indiki mərhələsində müəyyən tələblərə cavab verən EHR-sistemlərinin qurulması tələb edilir. Həkimləri EHR tətbiqinə stimullaşdırmaq üçün 2014-cü ildə

14,6 milyard dollar sərf edilmişdi, hazırda isə tətbiqin gecikdirilməsinə görə cərimələr nəzərdə tutulur.

1996-cı ildə ABŞ-da qəbul olunmuş "Tibbi sığortanın varisliyi və hesabatlılığı haqqında Qanun" (Health Insurance Portability and Accountability Act, HIPAA) müəyyən edir ki, pasiyentlər öz məlumatlarına girişə və ondan istifadə üsullarına nəzarət etmək hüququna malikdirlər [12]. Belə qanunlar pasiyentlərin öz xəstəlikləri və müalicə üsulları haqqında məlumat tapmaq üçün İnternetdən istifadə etməyə artan maraqları ilə birlikdə *fərdi tibbi kartlara* (Personal Health Record, PHR) ehtiyac yaradır, bu kartlar tətbiqi veb proqramlara əsaslanır, insanlara öz tibbi məlumatlarına müraciət etməyə, onları idarə etməyə və digər insanlara təqdim etməyə imkan verir .

EHR-sistemlərin daha bir imkanı pasiyent və elektron reseptlər haqqında informasiyanın təşkilatlar arasında, o cümlədən transsərhəd ötürülməsi ilə bağlıdır [13], bu sahədə ən tanınmış layihə 2014-cü ildə başa çatma epSOS Avropa layihəsi olmuşdur (http://www.epsos.eu/).

***Mobil səhiyyə (m-səhiyyə)***

Mobil telefonlar həm səs, həm də video və multimedia məlumatları vasitəsilə səhiyyə xidmətləri göstərilməsinin yeni vasitəsinə çevrilir [14]. Mobil səhiyyə (ing. mHealth) – səhiyyə məsələlərinin həlli üçün mobil qurğuların istifadəsini nəzərdə tutur və bir sıra üstünlüklərə malikdir (mobil telefonlar bəzi yerlərdə yeganə rabitə vasitəsidir, bir çox halda həkim briqadasının göndərilməsinə ehtiyac olmur, həkimin pasiyentlə ünsiyyəti üçün telekommunikasiya texnologiyalarından maksimal istifadə etməyə imkan verir).

M-səhiyyə hələlik başlanğıc mərhələsindədir, öz potensialını reallaşdıra bilməyib. M-səhiyyə sahəsində lider Yaponiyadır, dünya dövriyyəsinin 6 %-i onun payına düşür. ÜST-nin e-səhiyyə üzrə qlobal hesabatında qeyd edilir ki, m-səhiyyənin dominant forması hazırda kiçikmiqyaslı eksperimental layihələrlə xarakterizə olunur, onlarda da informasiyanın ortaq istifadəsinin və informasiyaya girişin bəzi məsələlərinə baxılır [15].

***Fərdiləşdirilmiş tibb***

Hesablama texnologiyalarında və genom məlumatlarının öyrənilməsində inkişafın fərdiləşdirilmiş tibdə böyük innovasiyalara gətirəcəyi gözlənilir. ABŞ Milli Onkologiya İnstitutu fərdiləşdirilmiş tibbi "tibbin xəstəliyin profilaktikası, diaqnostikası və müalicəsi üçün genlər, zülallar və insanı əhatə edən mühit haqqında informasiyadan istifadə edən forması" kimi müəyyən edir. Fərdiləşdirilmiş tibb xəstəliklərin erkən diaqnostikası, yüksək dərəcədə fərdiləşdirilmiş müalicə üsulları və dərmanların mənfi yan təsirlərini öncədən görmək və onlardan yan keçmək sahəsində geniş imkanlar yaradır [16].

***Sosial şəbəkə servisləri və səhiyyə texnologiyaları 2.0***

Sosial şəbəkə servisləri (Web 2.0 texnologiyaları) – interaktiv ünsiyyət və istifadəçi tərəfindən yaradılan kontent üçün nəzərdə tutulmuş texnologiyalar səhiyyə sahəsinə də daxil olur. Meydana çıxan texnologiyalardan biri pasiyentlərin öz sağlamlıq vəziyyəti və ya yaşlı valideynlərinin və ya uşaqlarının sağlamlıq vəziyyəti barədə verilənlərə onlayn rejimdə nəzarət etməsidir. Daha bir tendensiya tibbi xidmətlərin reytinqi üçün onlayn reputasiya sistemlərinin istifadə edilməsidir [17].

Pasiyentlər tibbi informasiya üçün veb-saytlara və sosial şəbəkə servislərinə müraciət edirlər. Belə sosial şəbəkə saytlarının bir çoxu səhiyyə ilə bağlı müsbət davranışı təşviq edir. Bəzən saytlar pasiyentlərə diaqnozlar və müalicə haqqında sual vermək və onlara cavab almaq imkanı da verir. Bu qeyri-dəqiq və qeyri-peşəkar onlayn tibbi məsləhətlərin geniş yayılması barədə ciddi narahatlıqlar doğurur.

Məsafədən klinik müalicə üçün sosial şəbəkə saytlarından istifadə edildikdə əsas narahatlıq tibbi yardımın göstərilməsi üçün hüquqi məsuliyyətlə bağlı məsələlər, müalicə sirrini qorumaq üçün zəruri olan texniki və sosial xarakterli məsələlər, həmçinin sosial şəbəkə servisləri ilə İnternet üzərindən ötürülən informasiyanın adekvat təhlükəsizliyinin və etibarlılığının təmin edilməsi ilə bağlı məsələlərdir [16, 17].

***E-səhiyyədə bulud texnologiyaları***

EHR-sistemləri fərdi məlumatların konfidensiallığını pozmadan və müvafiq təhlükəsizliyi dəstəkləməklə müxtəlif səhiyyə təşkilatları arasında informasiya mübadiləsini təmin edir. Belə sistemlərin qurulması üçün bulud platformaları ideal seçimdir, onlar əhəmiyyəli miqyaslama və tələblər dəyişdikdə çeviklik təmin edirlər, [18]-də bu məqsədlə Fusion platforması təklif edilir. Fusion – tibbi informasiyadan böyük miqyaslarda birgə istifadə edilməsi və informasiya təhlükəsizliyinin idarə edilməsi üçün açıq eksperimental bulud platformasıdır. Bu platformanın məqsədi EHR-in tətbiqinə çəkilən xərclərin azaldılmasıdır. Bundan başqa, Fusion tibbi məlumatların istifadə edildiyi yeni servislərin yaradılması üçün yeni imkanlar da yaradır.

***E-səhiyyə və Big Data***

E-səhiyyə sistemləri Big Data ilə müşaiyət olunur: böyük həcmdə verilənlər, genom məlumatları, diaqnostika təsvirləri, test nəticələri, tədqiqat nümunələri, sığorta və maliyyə məlumatları və olduqca çox sayda müxtəlif növ məlumatlar daxildir. Big data tibbi məlumatların aqreqasiyası və intellektual analizi üçün böyük imkanlar açır [19].

***E-səhiyyə sahəsində standartlaşdırma***

E-səhiyyənin gələcəyini müəyyən mənada tibbi informasiya sistemlərinin interoperabelliyi müəyyən edir. Lakin e-səhiyyə standartlaşdırma üçün ən mürəkkəb və problemli sahələrindən biridir, burada bir sıra özünəməxsus çətinliklər mövcuddur [17]. Əsas çətinliklərdən biri ondan ibarətdir ki, burada bir deyil, onlarla texnologiya sahəsi əhatə olunmalıdır. Kontent səviyyəsində − tibbi məlumatlar, diaqnostika təsvirləri, tibbi tədqiqatlar sahəsində standartlaşdırma tələb edilir. Digər standartlaşdırma geniş çeşiddə tibbi cihazları, proqram təminatı sistemləri, verilənlər bazalarını idarəetmə sistemlərini əhatə etməlidir. Başqa bir geniş standartlaşdırma sahəsinə e-səhiyyə infrastrukturu və telekommunikasiya sistemləri, informasiya təhlükəsizliyi, tibbi məlumatların mübadiləsi protokolları daxildir. Semantik operabellik də tibbi sorğu kitabları və terminologiya standartları (ICD, LOINC, SNOMED CT) ilə təmin edilməlidir.

E-səhiyyə sahəsində standartlaşdırma sahəsində vəziyyəti mürəkkəbləşdirən digər bir cəhət standartlaşdırma fəaliyyətinə cəlb olunan təşkilatların çoxluğu və onların fəaliyyətinin əlaqələndirilməsi və standartlar arasında interoperabelliyin təmin edilməsidir. Qeyd edək ki, e-səhiyyə sahəsində standartlaşdırma ilə ISO/TC 215, CEN/TC251, ITU-T, IEEE 11073, HL7, epSOS, DICOM, GS1 Healthcare, Continua Health Alliance kimi qurumlar fəaliyyət göstərir.

## III. E-SƏHİYYƏDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ TƏHDİDLƏRİ

**Zərərli proqram təminatı**. E-səhiyyənin yan təsirlərindən biri də zərərli proqramların kritik tibbi sistemləri və qurğuları yoluxdurmasıdır. ABŞ Veteran İşləri Nazirliyi 2013-cü ildə bildirmişdi ki, nazirliyin xəstəxanalarında 2009-cu ildən bəri ən azı 327 qurğu virusla yoluxmuşdu. 40-dan artıq virus növü rentgen maşınları və laboratoriya avadanlığı daxil olmaqla General Electric Co., Philips N.V. və Siemens AG kimi şirkətlərin istehsal etdiyi qurğuları yoluxdurmuşdu.

Bir halda, 2010-cu ildə, infarktdan sonra tıxanmış arteriyaların açılması prosedurları üçün lazım olan kompüter avadanlığı virusla yoluxmuşdu və laboratoriyanı müvəqqəti bağlamaq lazım gəlmişdi. Başqa bir halda, özəl xəstəxanada virus bir cihazdan konfidensial pasiyent məlumatlarını kənar serverə göndərirdi. Tibbi avadanlığın zərərli proqramlarla yoluxması halları çoxdur və bu barədə [20]-də geniş məlumat tapmaq olar.

**Tibbi identifikasiya məlumatlarının itkisi.** Təhdidlərdən biri də tibbi identifikasiya məlumatlarının oğurlanmasıdır. Pokemon-un tədqiqatlarına görə 2013-cü ildə 1.8 milyon amerikalının tibbi identifikasiya məlumatları oğurlanmışdı. Bu zaman onların 36%-nə yazılmış hesabları ödəməyə imkanları olmamışdır. Bəziləri sığorta müddətlərinin başa çatmasına görə dərmanların və tibbi xidmətlərin xərclərinin tam ödəməyə məcbur olmuşlar. Digərləri dələduzların aldıqları tibbi xidmətlərə görə ödəməli olmuşdur. Bu zaman hesabın orta həcmi 18.660 dollar olmuşdur.

2014-cü il Healthcare Breach Report-a görə 2010-cu ildən bəri bütün səhiyyə verilənlərinin 68 %-i qurğuların itirilməsi və ya oğurlanması səbəbindən baş verib [21]. 2014-cü ildə təxminən 2 milyon amerikalının tibbi identifikasiya məlumatları oğurlanmışdı. Lakin 2015-ci ildə hakerlərin tibbi məlumat bazalarına hücumları ilə əlaqədar bu rəqəm 112 milyona çatmışdı (hər 3 amerikalıdan birinin tibbi identifikasiya məlumatları oğurlanmışdı). Verilənlərin ən böyük itkisi 2015-ci ilin fevralında sığorta şirkəti Anthem tərəfindən açıqlanmışdı, hakerlər şirkətin serverlərini sındıraraq 78,8 milyon insanın fərdi identifikasiya edilə bilən məlumatlarını oğurlamışdır. Anthem tibbi məlumatların və maliyyə məlumatlarının oğurlanmadığını bildirmişdi. Qeyd etmək lazımdır ki, oğurlanmış məlumatlar şifrlənməmişdi, qanun (HIPPA) bunu məcburi tələb etmir [22].

Lakin bu baş verə bilənlərdən ən pisi deyil. Əgər kiminsə sizin tibbi identifikatora girişi olarsa və onu tibbi xidmətlərin reseptlərin alınması üçün istifadə edərsə, bütün müvafiq məlumatlar da sizin şəxsi tibb kartınıza yazılacaq. Və sizin məlumatlar dələduzun məlumatları ilə qarışacaq. Ora əvvəlcə yazılmış bütün informasiya yalan olacaq. Anthem sistemində baş verən insident 80 milyon pasiyentə toxunmuşdur və belə hallar baş vermişdi. Anthem şirkətinin məlumatına görə oğurlanmış verilənlərdə pasiyentin adı, doğum tarixi, üzvlük identifikatorları və sosial sığorta kartının nömrələri, ünvan, telefon nömrələri, e-poçt ünvanı və iş yeri haqqında məlumatlar olmuşdur. Bu verilənlərdən müəyyən qədər dələduzluq hesabları üçün istifadə etmək olar.

Tibbi identifikasiya məlumatları kredit kartı və ya sosial sığorta kartları ilə müqayisədə daha dəyərli hesab olunur. World Privacy Forum-un məlumatlarına görə qara bazarda onun qiyməti 50 dollardır, kredit kartının və ya sosial sığorta kartının nömrəsi təxminən 1 dollardır [23]. Bir tibb kartından orta qazanc 20 min dollar, adi identifikasiya məlumatlarının oğurluğundan isə 2 min dollar qiymətləndirilir .

Ponemon İnstitutunun məlumatına görə səhiyyə sahəsində kibercinayətkarlığın artmasının səbəblərindən biri ondadır ki, burada dələduzluğun aşkarlanmasına daha çox vaxt gedir, vəziyyəti düzəltmək isə xeyli mürəkkəb olur [24]. Bank hesablarını bağlamaq, yeni kredit kartı almaq olar, electron tibbi məlumatları korreksiya etmək isə daha çətindir.

**Tibbi cihazlara kiber hücumlar.** Bir çox tibbi cihazda geniş yayılmış əməliyyat sistemləri istifadə edilir, buna görə onlar da adi kompüterlər kimi hücumlara həssasdırlar. Lakin xüsusi əməliyyat sistemləri olan cihazlar da kiber hücumlara məruz qala bilər, çox zaman bunun üçün proqram təminatının yenilənməsi mexanizmi istifadə edilir [25, 26].

Naqilsiz texnologiyalar tibbi cihazları kiber-hücumlara olduqca həssas edir. ABŞ Milli Təhlükəsizlik Nazirliyi 2012-ci ildə müasir tibb qurğularının istifadə üzrə tövsiyələrini nəşr etmişdir [27]. Bülletendə nazirliyin mütəxəssisləri etiraf edirlər ki, yeni texnologiyalar işin nəticəliliyini yüksəltməyə, xərcləri azaltmağa və pasiyentlərə xidmətin keyfiyyətini yaxşılaşdırmağa kömək edir, lakin bu zaman təhlükəsizlik baxımından risklər yaranır ki, ona səhiyyə sahəsi hazır olmaya bilər. Tibbi cihazlarda kommunikasiya təhlükəsizliyi ciddi narahatlıq doğurur, buna görə bədniyyətlilərin müdaxilələrindən və tibbi verilənlərin oğurlanmasından qorunmaq üçün əlavə təhlükəsizlik tədbirlərinin lazım olduğu nazirliyin hesabatında bildirilir.

2011-ci ildə Black Hat təhlükəsizlik konfransında tədqiqatçılardan biri insulin nasosuna icazəsiz qoşulmağın və istifadəçinin xəbəri olmadan onun parametrlərini dəyişdirməyin mümkünlüyünü göstərmişdir. Həmin tədqiqatçı qanda qlükozanın səviyyəsini göstərən sensorun ötürdüyü verilənlərin osilloqrafın köməyi ilə ələ keçirilməsini də göstərmişdir.

2009-cu ildə Massaçusets Universitetinin (Amherst) tədqiqatçılarından biri implant qurğuya – defibrilyatora icazəsiz qoşulmağın mümkünlüyünü nümayiş etdirmişdir, defibrilyator - elektrik impulslarının köməyi ilə ürəyin işini sabitləşdirir. O, cihazı yenidən elə proqramlaşdırılmışdır ki, ürəyi cərəyan vursun. Bundan başqa, tədqiqatçı defibrilyatorda enerjiyə qənaət rejimini söndürməyə də nail olmuşdu, bunun nəticəsində batareyanı ştat rejimindəki bir neçə il əvəzinə bir neçə saatda boşaltmaq olar.

Bütün xəstəxanaların təxminən 25%-i pasiyentlərin verilənlərinin təhlükəsizliyinin illik yoxlanılmasını yerinə yetirmirlər. Bunu 2011-ci ildə səhiyyədə informasiya təhlükəsizliyi üzrə ixtisaslaşan tibbi informasiya və idarəetmə sistemləri cəmiyyətinin keçirdiyi rəy sorğusu göstərmişdir ki, informasiya təhlükəsizliyinə öz İT- büdcələrinin 3%-indən az sərf edirlər.

Hesabatda xatırladırlar ki, pasiyentlər haqqında məlumatların itirilməsinə görə xəstəxanaları məsuliyyətə cəlb etmək olar. Məsələn, bir USB daçıyıcısında 25-minə yaxın pasiyentin tibb kartını saxlamaq olar. Belə daşıyıcının itirilməsi xəstəxanaya 6 milyon dollara başa gələ bilər, bura cərimələr, hüquqi xərclər, pasiyentlərə xəbər verilməsi xərcləri və zərərçəkmişlərin şəxsi məlumatlatlarının monitorinqinə çəkilən xərclər daxildir.

**Digər təhdidlər.** ABŞ-da tibbi cihazların layihələndirilməsi, istehsalı və satışının tənzimlənməsi ilə Qida və dərman məhsullarına Nəzarət İdarəsi məşğul olur, lakin bu idarə tibbi cihazların kommunikasiya qurğularına qoşulmasını tənzimləyən sənədləri hələlik işləməyib. Buna görə pasiyentlərin tibbi məlumatlarına girişi olan cihazları hakerlərdən qorumaq qayğısına tibbi müəssisələrin əməkdaşlarının özləri qalmalı olur.

Adətən tibbi cihazlarda təhlükəsizlik vasitələri nəzərdə tutulsa da, onlar mürəkkəblik və ya məlumatsızlıq səbəbindən heç də həmişə istifadə edilmirlər. E-səhiyyədə istifadə edilən texnologiyaların əksəriyyəti yeni olduğundan istifadəçilər bu texnologiyalarda təhlükəsizliyin təmin edilməsi üsulları ilə tanış olmaya bilərlər və nəticədə bədniyyətlilər istifadəçi səhvlərindən yaralana bilərlər.

«Yaxşı düşünülmüş təhlükəsizlik proqramının olmaması təşkilatın pasiyentlərin tibbi məlumatlarını oğurlanmaqdan, itirilməkdən və zədələnməkdən qorumaq imkanlarına mənfi təsir göstərə bilər.»

İnformasiya təhlükəsizliyinə ayrılan büdcə kiçik olduqda problem daha da dərinləşə bilər: vəsaitləri məhdud olan müəssisə prioriteti təhlükəsizliyin təmin edilməsinə deyil, başqa məsələlərə üstünlük verə bilər. Lakin bu növ çətinliklərə baxmayaraq, təhlükəsizliyə «olsaydı, yaxşı olardı» funksiya kimi yanaşmaq olmaz.

## IV. E-SƏHİYYƏDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ MEXANİZMLƏRİ

Fərdi tibbi məlumatlar konfidensial informasiya kateqoriyasına aiddir, belə informasiyanın əldə edilməsi, emalı və istifadəsi onun toplandığı məqsədlər ilə məhdudlaşdırılır. E-səhiyyə informasiya sistemləri fərdi tibbi məlumatların saxlanmasını, onlara girişi və istifadəsini yalnız tibbi yardımın göstərilməsi məqsədləri üçün və yalnız tibbi yardımın göstərildiyi müddətdə təmin edir.

Fərdi tibbi məlumatların mühafizəsi hüquqi, təşkilati və texniki tədbirlər kompleksinin tətbiqi yolu ilə həyata keçirilir və aşağıdakı məqsədləri güdür:

- şəxsi həyatın toxunulmazlığı, şəxsi və ailə sirri hüquqlarının reallaşdırılması;
- fərdi tibbi məlumatların tamlığının və konfidensiallığının təmin edilməsi;
- fərdi məlumatlara giriş hüququnun reallaşdırılması;
- onların qanunsuz toplanmasının və emalının qarşısının alınması.

Şəbəkələrin sərhədində şəbəkə ekranları qoymaq, şəbəkə monitorinqi və müdaxilələrin aşkarlanması sistemlərindən istuifadə etmək, mümkün olduqca cihazları şəbəkənin ayrıca seqmentində yerləşdirmək tövsiyə olunur. Həmçinin girişə ciddi nəzarət siyasəti, kommunikasiya kanallarının hər iki ucunda şifrləmə və autentifikasiya tətbiq etmək məsləhət görülür.

**Girişə nəzarət.** E-səhiyyə sistemlərində girişin rol əsasında idarə edilməsi (Role based access control, RBAC) istifadə edilməsi tövsiyə olunur [28, 29]. E-səhiyyə sistemlərinə yalnız tibb müəssisəsinin rəhbərliyi tərəfindən müvafiq icazəsi olan şəxslər təşkilatda icra etdikləri funksiyalar (rollar) çərçivəsində daxil ola bilərlər. Məsələn, pasiyentin xəstəlik tarixçəsinə tibb işçisinin yalnız öz səlahiyyətləri çərçivəsində giriş hüququ var. Qeydiyyatçı tibb bacısı xəstənin qeydiyyatı zamanı xəstənin pasport məlumatlarını, ona nə zaman həkim qəbulu və analizlər təyin edildiyini görə və yalnız öz səlahiyyətləri daxilində dəyişikliklər edə bilər.

**Autentifikasiya və avtorizasiya.** Məsafədəki istifadəçilərin terminal serverin resurslarına girişini idarə etmək üçün terminal rejimdə işləyən aparat-proqram vasitəsi istifadə edilə bilər. Məsələn, Rusiya Səhiyyə Nazirliyinin tibb müəssisələrinin kompüter avadanlığı və proqram təminatı ilə təchiz edilməsi haqqında metodiki tövsiyələrinə müvafiq olaraq fərdi kompüterdən fərqli olan xüsusi qurğu – aparat nazik kliyenti tətbiq etmək tövsiyə edilir. Tövsiyə olunan nazik kliyent xüsusi lokal əməliyyat sistemindən isifadə edir ki, onun da yeganə vəzifəsi istifadəçinin işləməsi üçün terminal serverdə sessiyanı təşkil etməkdir.

Nazik kliyentdə istifadəçilərin lokal avtorizasiyası fərdi identifikator təqdim edildikdən və PIN-kod daxil edildikdən sonra həyata keçirilir. PIN-kod düzgün daxil edildikdə nazik kliyentin əməliyyat sistemi yüklənir. Nazik kliyentin əməliyyat sisteminin etibarlı yüklənməsi zamanı əməliyyat sisteminin obrazının tamlığı yoxlanır.

**E-imza.** Sağlamlıq haqqında fərdi məlumatlara bütün dəyişikliklər və əlavələr tibb işçisinin gücləndirilmiş elektron imzası ilə təsdiqlənir. E-imzanın yaradılması və yoxlanması üçün nazik kliyent bazasında veb-giriş rejimində işləyən xüsusi aparat-proqram vasitələri mövcuddur. Burada xüsusi brauzerin köməyi ilə sənədlərə baxmaq və imzalamaq olar.

**Audit.** Fərdi tibbi məlumatlara əlavə və dəyişikliklərin auditini təmin etmək üçün edilmiş əlavə və dəyişikliklərin təsviri, onların edildiyi zaman və tarix, məlumatlara əlavə və dəyişikliyi edən, məlumata baxan, kopyalayan və ya çap edən tibb işçisinin identifikatoru xüsusi loq-faylda avtomatik qeydə alınır. Audit fərdi məlumatlara girişin qarşısını almaq mümkün olmadıqda və icazəsiz giriş şübhələri olduqda belə icazəsiz giriş faktlarını vaxtında aşkarlamağa imkan yaradır.

**Ehtiyat surətçıxarma.** Fərdi tibbi məlumatların mütəmadi olaraq ehtiyat surətləri yaradılaraq qorunmalıdır.

**Sertifikatlaşdırma.** E-səhiyyə həllərində istifadə edilən informasiya təhlükəsizliyi üzrə həm proqram, həm də aparat-proqram vasitələri qanunvericiliyə uyğun şəkildə sertifikatlaşdırılmalıdır.

**Fərdi məlumatların de-identifikasiyası (fərdisizləşdirmə).** Səhiyyə üzrə statistik, sosial və elmi tədqiqatların aparılması zamanı fərdi məlumatlardan istifadə edilərək fərdisizləşdirilmiş verilənlərdən istifadə etmək zəruridir [30]. Statistik və analitik sistemlərin istifadəsi zamanı müxtəlif hesabatların alınması zamanı da fərdisizləşdirilmiş verilənlərdən istifadə edilməlidir.

Fərdi məlumatların fərdisizləşdirilməsi üçün anonimlik (*anonymization*), təxəllüs (*pseudonymization*), şifrləmə (*encryption*), açarla kodlaşdırma (*key-coding*) və s. üsullar istifadə edilə bilər. HIPAA ***təhlükəsiz liman mexanizmi:*** fərdin və ya qohumlarının, ailə üzvlərinin və ya işə götürənlərin 18 spesifik identifikatorunun silinməsi tələb edilir:

- adlar, ünvanlar, tarixlər, telefon nömrələri, faks nömrələri,
- tibbi sığorta nömrələri, sosial sığorta nömrələri, tibbi sənədləşmə nömrələri,elektron poçt ünvanları, hesab nömrələri,
- lisenziya/sertifikat nömrələri, maşın identifikatorları və seriya nömrələri, qurğu identifikatorları və seriya nömrələri,
- URL (universal resource locator), IP-ünvanlar, biometrik identifikatorlar, üzün tam fotoşəkilləri və identifikasiyanın başqa unikal nömrəsi, xarakteristikası və ya kodu.

Microsoft şirkətinin təklif etdiyi fərdisizləşdirmə üsulunda fərdisizləşdirilmiş məlumatlar informasiya sisteminin bir seqmentində, bu məlumatların sahibini identifikasiya etməyə imkan verən məlumatlar isə başqa bir seqmentində saxlanır. Bu iki məlumat yalnız pasiyent haqqında məlumatlar bilavasitə istifadə edildikdə, məsələn, pasiyent həkim qəbulunda olduğu anda birləşdirilir. Pasiyent getdikdən sonra verilənlər yenidən “parçalanır”, bu onların təhlükəsizliyini təmin etməyə imkan verir.

## V. SİMSİZ BƏDƏN SENSORLARI ŞƏBƏKƏSİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ

Təcili yardım həkimləri, tibb bacıları, feldşerlər naqilsiz tibbi cihazlardan diaqnostika, müalicə və pasiyentin vəziyyətini monitorinq etmək üçün istifadə edirlər. Bu cihazlar cibdə daşınan, səyyar və ya implant ola bilər (məsələn, kardiomonitor).

Simsiz bədən sensorları şəbəkəsi (Wireless Body Sensor Network, WBSN) pasiyentlərin sağlamlıq vəziyyətinin monitorinqi məqsədilə simsiz şəbəkə ilə transiverə və ya kiçik qoşma kompüterə (məsələn, mobil telefona) birləşdirilmiş fizioloji sensorlar çoxluğudur. WBSN-nin arxitekturasını 3 yaruslu şəbəkə şəklində göstərmək olar [31].

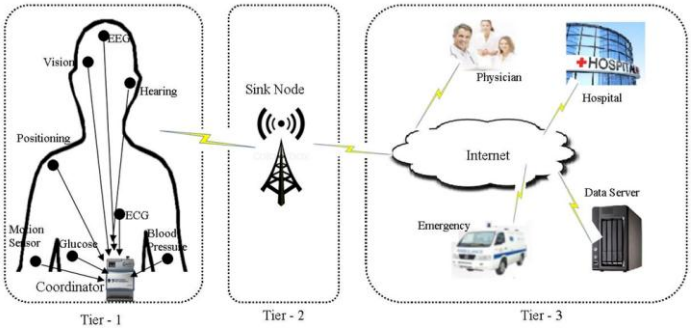
Hər bir sensor qovşağı mikrokompüter (hesablama komponenti), transiver (kommunikasiya komponenti), enerji mənbəyi (adətən, batareya) və tətbiq sahəsindən asılı olaraq müəyyən sensorlardan ibarətdir. Bəzi smart-sensorlara sistemin müxtəlif komponentlərini idarə etmək üçün aktuator – elektromexaniki qurğu da daxildir. Sensorlar müəyyən fəaliyyəti ölçür və informasiya toplayır və informasiyanı baza stansiyası (ing. sink node) adlanan xüsusi stansiyaya göndərir. Bu bio-tibbi sensorlar ölçdükləri verilənləri bədənin yaxınlığında yerləşən koordinatora göndərir, koordinator verilənlərin emalını və aqreqasiyasını yerinə yetirir. Baza stansiyası isə məlumatları İnternet vasitəsilə səhiyyə müəssisəsinə və ya digər təyinat yerinə göndərir.

Baza stansiyası həm də daxili şəbəkə ilə xarici şəbəkə arasında şlüz rolunu oynaya bilər. Autentifikasiya, şəbəkə ekranı və s. kimi təhlükəsizlik mexanizmlərini bu idarəetmə qurğusunda tətbiq edərək trafiki monitorinq etmək mümkündür.

Spesifik xüsusiyyətlərinə görə WBSN-lərin təhlükəsizlik arxitekturası şəbəkələrin digər növlərindən fərqlidir [32]. Sensor şəbəkələrinin enerji, hesablama və kommunikasiya imkanları məhduddur və bu şəbəkələri fiziki mühitlə və insanlarla sıx qarşılıqlı əlaqədədir, bu fiziki hücum imkanlarını artırır və yeni təhlükəsizlik problemləri yaradır.

WBSN-ə kiber hücumlarla bədniyyətli paketlərin təyinat ünvanını dəyişə, marşrutlamanı poza bilər, simsiz kommunikasiya mühitini gizli dinləməklə tibbi məlumatları oğurlaya bilər, pasiyentin yerini müəyyənləşdirə və onun hərəkətlərini izləyə bilər, verilənlərə dəyişikliklər edə, tibbi verilənlərdə saxta həyəcan siqnalları yarada bilər, DoS-hücumlar (Denial of Service – xidmətdən imtina), fiziki qurğulara müdaxilə və “jamming” hücumları, yan kanal hücumları, enerji mənbəyinin – batareyanın boşaldılması, analoq sensor inyeksiyası və s. hücumları həyata keçirə bilər [32, 33].

IEEE 802.15.6 standartında WBSN üçün üç təhlükəsizlik səviyyəsi müəyyən edilir: səviyyə 0, səviyyə 1 və səviyyə 2. Səviyyə 0 (Qorunmayan) qorunmayan kommunikasiya üçün istifadə edilir. Paketlər şifrlənmədən ötürülür və məlumatların tamlığı, təkrarlama hücumundan müdafiə, autentifikasiya və s. yoxdur. Səviyyə 1-də (Autentifikasiya) verilənlər autentifikasiya edilən şəkildə ötürülür, lakin verilənlər şifrlənmir və onların tamlığı yoxlanmır. Səviyyə 2 (Şifrləmə və autentifikasiya) təhlükəsizliyi ən yüksək səviyyədə təmin edir, tamlıq, autentifikasiya, verifikasiya və s. tədbirləri həyata keçirilir. Səviyyələr tətbiq sahəsinin tələbləri əsasında seçilir [34].




Şəkil 1. WBSN arxitekturası

## VI. E-SƏHİYYƏDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN MENECMENTİ STANDARTI

ISO 27799 [35] xüsusi olaraq səhiyyə üçün adaptasiya edilmiş standartdır və ISO/IEC 27002 standartının səhiyyə sahəsində interpretasiyasını və həyata keçirilməsini dəstəkləmək üçün rəhbər prinsipləri müəyyən edir. Bu standart səhiyyə sektorunda informasiya təhlükəsizliyinin menecmenti tələblərinə ünvanlanıb. Bu rəhbər prinsiplərin həyata keçirilməsi səhiyyə təşkilatlarına təhlükəsizlik insidentlərinin sayını və təsirini azaltmağa və fərdi tibbi məlumatların konfidensiallığının, tamlığının və əlyetərliyinin minimal səviyyəsini təmin etməyə imkan verir.

Standart səhiyyə məlumatlarının qorunması üçün təhlükəsizlik tədbirlərinin seçilməsi və həyata keçirilməsi üzrə aydın, dəqiq və səhiyyəyə spesifik tövsiyələr verir və səhiyyədə rastlanan çox geniş diapazonda miqyaslara, yerlərə və xidmət göstərilməsi modellərinə adaptasiya edilə bilər. ISO 27799 standartı 11 təhlükəsizlik sahəsinə baxır, onlar ümumilikdə 39 əsas təhlükəsizlik kateqoriyasını əhatə edirlər. Hər bir kateqoriyada bir və ya bir neçə təhlükəsizlik tədbirinin təsviri verilir.

ISO 27799 standartında 1) informasiya təhlükəsizliyi siyasəti, 2) informasiya təhlükəsizliyinin təşkili, 3) aktivlərin menecmenti, 4) insan resurslarının təhlükəsizliyi, 5) fiziki və ətraf mühit təhlükəsizliyi, 6) kommunikasiyaların və əməliyyatların menecmenti, 7) girişə nəzarət, 8) informasiya sistemlərinin alınması, yaradılması və istismarı, 9) informasiya təhlükəsizliyi insidentlərinin menecmenti və 10) fəaliyyətin fasiləsizliyinin menecmentində informasiya təhlükəsizliyi aspektləri və 11) tələblərə uyğunluq kimi təhlükəsizlik sahələrinə baxılır.

## VII. E-SƏHİYYƏDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN AKTUAL PROBLEMLƏRİ

İKT-əsaslı texnologiyalar səhiyyə sistemlərinin yükünü azaltmağa və səhiyyə xidmətlərinin keyfiyyətini yüksəltməyə kömək edir. Bu texnologiyalara bio-sensorlar, kompüter vasitəsilə diaqnoz, bədən sensorlarının simsiz şəbəkəsi, mobil tibb, radiotezliklə identifikasiya (Radio Frequency Identification, RFID), bulud texnologiyaları, kommunikasiya protokolları, elektron tibb məlumatları, Big data, Əşyaların İnterneti və s. daxildir. Bunun nəticəsində səhiyyə sistemlərinin mürəkkəbliyi son illər dramatik şəkildə artmışdır. Lakin bu texnologiyaların səhiyyə sistemlərinə inteqrasiyasında səhvlər yolverilməzdir, çünki insan həyatı bahasına başa gəlir. Bundan əlavə, belə sistemlərdə səhvlər baş verdikdə sistemlərin yenilənməsi və bərpası əhəmiyyətli səylər və zaman tələb edir. Nəticədə, e-səhiyyə sistemləri istifadə edilməzdən əvvəl ciddi şəkildə test edilməlidirlər.

Səhiyyə sistemlərinin test edilməsi və verifikasiyası üçün bir neçə yanaşmanın işlənməsinə baxmayaraq, bir sıra itkilərə səbəb olan İKT ilə əlaqəli tibb insidentləri hələlik tez-tez baş verir. Buna görə, tibbi informasiya sistemlərinin və tibbi cihazların adekvat test və verifikasiya edilməsi üçün aşağıdakı istiqamətlərdə elmi-praktiki tədqiqatların aparılması vacibdir:

- e-səhiyyə sistemlərinin test edilməsi və verifikasiyası metodları;
- e-səhiyyə proqram təminatının və avadanlığının verifikasiyası metodları;
- tibbi sensorların, m-tibbin, WBSN-in etibarlığının qiymətləndirilməsi metodları;
- e-səhiyyə sistemlərinin imtinalara dayanıqlığının qiymətləndirilməsi;
- EHR-sistemlərin və fərdi tibbi məlumatların etibarlılığının qiymətləndirilməsi metodları.

M-tibbin reallaşdırılması ilə bağlı bir çox problem mövcuddur: pasiyentlə tibbi xidmət provayderi arasında simsiz rabitə şəbəkəsində kommunikasiyanın təhlükəsizliyi, distant tibbi nəzarət funksiyalarının yetərli etibarlılığının təmin edilməsi, simsiz şəbəkə qurğuları ilə alınmış tibbi məlumatların dəqiqliyinin təmin edilməsi və s.

E-səhiyyə sistemlərində verilənlərin təhlükəsizliyini təmin etmək üçün bütün kommunikasiya infrastrukturunda informasiya təhlükəsizliyi müvafiq səviyyədə təmin edilməlidir. Bu sahədə aşağıdakı istiqamətlərdə elmi-praktiki tədqiqatların aparılması vacibdir:

- e-səhiyyə sistemlərində informasiya təhlükəsizliyi boşluqlarının qiymətləndirilməsi;
- e-səhiyyə sistemlərində və tibbi cihazlarda informasiya təhlükəsizliyi risqlərinin qiymətləndirilməsi metodları;
- e-səhiyyə sistemlərində girişin idarə edilməsi metodları;
- e-səhiyyə üçün təhlükəsiz şəbəkə arxitekturaları;
- fərdi tibbi məlumatların təhlükəsiz ötürülməsi, email və saxlanması metodları
- e-səhiyyə sistemlərində müdaxilələrin və dələduzluğun aşkarlanması metodları;
- e-səhiyyə sistemlərində təhlükəsizlik üzrə məhkəmə ekspertizası üsulları.

*Gizliliyi saxlamaqla verilənlərin intellektual analizi* (Privacy Preserving Data Mining) üsullarının işlənməsi. E-səhiyyə sahəsində analitika üçün verilənlərin anonimləşdirilməsi istifadəçi məxfiliyini qorumaq üçün kifayət deyil. Buna görə də, fərdi məlumatları intellektual analizi zamanı məxfiliyinin pozulması hallarının qarşısını almaq üçün müvafiq yanaşmalar, metodlar və texnologiyaların işlənilməsi vacibdir. Geniş istifadə edilən data mining və ya maşın təlimi üsullarından fərqli olaraq, PPDM giriş verilənlərinin modifikasiya edilməsini tələb edir. İlkin verilənlərin

modifikasiya edilməsi fərdi verilənlərdə həssas məlumatların açıqlanmasının və ya fərdlərin məxfiliyinin pozulmasının qarşısını almağa xidmət edir. Ədəbiyyatda rast gəlinən PPDM üsullarını iki istiqamətdə qruplaşdırmaq olar randomizasiya üsulları və kriptoqrafik üsullar [36].

PPDM alqoritmlərinin əksəriyyəti nəzəri olaraq təklif edilib və onların yalnız kiçik bir qismi real praktiki situasiyalar üçün realizə edilmişdir və ya real verilənlərdən istifadə edilərək test edilmişdir. Bu isə onların istifadəçilərə təmin edəcəyi təhlükəsizlik səviyyəsini birqiymətli müəyyən etməyi çətinləşdirir.

## NƏTİCƏ

Elektron səhiyyə keyfiyyətli tibbi xidmətlərin və tibbi məlumatların bütün cəmiyyətə əlyetərliyi sahəsində müxtəlif perspektivlər vəd edir. Bununla yanaşı, tibbi xarakterli məlumatların toplanması, saxlanması, emalı və mübadiləsi sahəsində informasiya və kommunikasiya texnologiyalarının geniş istifadəsi şəxsi həyatın toxunulmazlığı və informasiya təhlükəsizliyi baxımından bir sıra təhlükələrə də yol açır. Bu təhlükələrə adekvat tədbirlərin görülməsi və zəruri mexanizmlərin işlənməsi elektron səhiyyə üzrə istənilən təşəbbüsün vacib komponenti olmalıdır.

## ƏDƏBİYYAT


[1] V. Della Mea “What is e-Health (2): The death of telemedicine?”Journal of Medical Internet Research, vol. 3, no.2, 2001 :e22. doi:10.2196/jmir.3.2.e22.

[2] Building Foundations for eHealth - Progress of Member States. World Health Organization, 2006. 339 p.

[3] C. George , D. Whitehouse, P. Duquenoy (eds.), “eHealth: Legal, Ethical and Governance Challenges.” Springer, 2013. 396 p.

[4] М.Г.Мамедова. “Информационная безопасность персональных медицинских данных в электронной среде” İnformasiya texnologiyaları problemləri, №2, s.16-30, 2015.

[5] S. Sabnis, D. Charles “Opportunities and challenges: Security in eHealth,” Bell Labs Technical Journal, vol. 17, no. 3, pp. 105–111, 2012.

[6] K.K. Agbele, H.O Nyongesa, & A.O. Adesina “ICT and information security perspectives in e-health systems,” Journal of Mobile Communication, vol. 4, no. 1, pp. 17-22, 2010.

[7] Y. M. Mohammad, Information security strategy in telemedicine and e-health systems: A case study of England’s shared electronic health record system. PhD. Brunel University. 2010. http://bura.brunel.ac.uk/handle/2438/4669

[8] Atlas of eHealth country profiles. WHO Global Observatory for eHealth. World Health Organization 2016, 392 p.

[9] D. Fridsma “Electronic Health Records: The HHS Perspective,” IEEE Computer, vol. 45, no.11, pp.24-26, 2012.

[10] J. L. Fernández-Alemán, I.C. Secor, P.Á.O. Lozoya, A. Toval “Security and privacy in electronic health records: A systematic literature review,” Journal of Biomedical Informatics, vol. 46, pp. 541–562, 2013.

[11] Б. В. Зингерман, Н.Е. Шкловский-Корди “Электронная медицинская карта и принципы ее организации,” Врач и информационные технологии, №2, с.37-58, 2013.

[12] B. K. Atchinson, D.M. Fox “The politics of the Health Insurance Portability And Accountability Act,” Health Affairs, vol. 16, no. 3, pp. 46–150, 1997.

[13] M. Azarm-Daigle, C. Kuziemsky, L. Peyton “A review of cross organizational healthcare data sharing,” Procedia Computer Science, vol. 63, pp. 425 – 432, 2015.

[14] S.-P. Lin, Determinants of adoption of mobile healthcare service, International Journal of Mobile Communications, vol. 9, no. 3, pp. 298-315, 2011.

[15] mHealth: New horizons for health through mobile technologies. Global Observatory for eHealth series - Volume 3. World Health Organization. 2011. 112 p.

[16] ITU-T Technology Watch Report: Standards and eHealth. January 2011. http://itu.int/en/ITU-T/techwatch/Pages/ehealth-standards.aspx.

[17] ITU-T Technology Watch Report: E-health Standards and Interoperability. April 2012.

[18] S. Basu, A. Karp, J. Li, J. Pruyne, J. Rolia, S. Singhal, J. Suermondt, R. Swaminathan, “Fusion: Managing Healthcare Records at Cloud Scale,” IEEE Computer Society, vol. 45, no. 11, pp. 42-49, 2012.

[19] R. Alguliyev, Y. Imamverdiyev “Big Data: Big Promises for Information Security,” 8th IEEE International Conference on Application of Information and Communication Technologies (AICT), pp. 1-4, 2014.

[20] C. Weaver “Patients put at risk by computer viruses,” Wall Street Journal, 13 June, 2013. www.wsj.com/articles/SB10001424127887324188604578543162744943762

[21] The 2014 Bitglass Healthcare Breach Report. www.bitglass.com/company/news/press_releases/healthcare-data-breach-report

[22] D. Munro “Data breaches in healthcare totaled over 112 millionr in 2015,” 31 December, 2015.

[23] L .J. Camp, M.E. Johnson “The Economics of Financial and Medical Identity Theft.” 2012.

[24] Fifth Annual Study on Medical Identity Theft. Ponemon Institute, February 2015, 38 p.

[25] TrapX Security, “Anatomy of an Attack MEDJACK (Medical Device Hijack),” May 2015.

[26] D. Storm “MEDJACK: hackers hijacking medical devices-to create backdoors in hospital networks,” Computerworld, June 8, 2015 http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

[27] National Cybersecurity and Communications Integration Center. Attack Surface: Healthcare and Public Health Sector. 2012, 10 p.

[28] ISO/TS 22600-1 Health informatics – Privilege management and access control – Part 1: Overview and policy management. ISO 2006.

[29] ISO/TS 22600-2 Health informatics – Privilege management and access control – Part 2: Formal models. ISO 2006.

[30] B. Eze, L. Peyton “Systematic literature review on the anonymization of high dimensional streaming datasets for health data sharing,” Procedia Computer Science, vol. 63, pp. 348-355, 2015.

[31] J. I. Bangash, A.H. Abdullah, M.H. Anisi, A.W. Khan “A survey of routing protocols in üireless body sensor networks,” Sensors, vol. 14, no. 1, pp. 1322-1357, 2014.

[32] M. Al Ameen, J. Liu, and K. Kwak, “Security and privacy issues in Wireless Sensor Networks for Healthcare Applications,” J Med Syst, vol. 36, no. 1, pp. 93–101, 2012.

[33] M. Rushanan, D.F. Kune, C.M. Swanson, A.D. Rubin “Sok: Security and privacy in implantable medical devices and body area networks,” Proc. 35th Annual IEEE Symp. on Security and Privacy, pp. 524-539, 2014.

[34] K. S. Kwak, S. Ullah, N. Ullah, “An overview of IEEE 802.15.6 standard,” Proc. of the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL), pp. 1-6, 2010.

[35] International Organization for Standardization (ISO). ISO 27799-2008 Health informatics – Information security management in health using ISO/IEC 27002. 2008.

[36] C. C. Aggarwal and P.S. Yu. Privacy-preserving data mining: models and algorithms. New York: Springer, 2008.