UOT 004.056:351 DOI: 10.25045/jpis.v11.i2.02

İmamverdiyev Y.N.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@iit.science.az

COVID-19 PANDEMİYASI DÖVRÜNDƏ KİBERTƏHLÜKƏSİZLİK PROBLEMLƏRİNİN ANALİZİ

Hazırda dünya bu əsrin ən pis pandemiyalarından birini yaşayır. Bu dövrdə kibertəhlükəsizlik daha böyük əhəmiyyət qazanır, çünki pandemiya zamanı kibermühit bədniyyətli aktorlar üçün olduqca əlverişlidir. Cəmiyyət bu pandemiya zamanı kiberhücumların böyük artımı ilə qarşılaşır. Bu məqalədə COVID-19 pandemiyası zamanı kibertəhlükəsizlik təhdidlərinin ümumi mənzərəsi analiz edilir, fərdi məlumatların təhlükəsizliyinin qanunvericilik və texnoloji aspektlərinə baxılır, pandemiyanın rəqəmsal monitorinqi sistemlərində meydana çıxan yeni kibertəhdidlər diqqətə çatdırılır və qısa təsvir edilir. İnfodemiya ilə mübarizə tədbirləri və bu məsələdə sosial medianın rolu araşdırılır. Nəhayət, evdən iş konsepsiyasının tətbiqi ilə əlaqəli kibertəhlükəsizliyin təmin edilməsi üzrə istifadəçilər və təşkilatlar üçün tövsiyələr və kibertəhlükəsizlik infrastrukturunun modernləşdirilməsi üzrə təkliflər işlənir. Məqalədə sistemləşdirmə, ümumiləşdirmə, təsnifləndirmə və müqayisəli kritik analiz metodları istifadə edilmişdir. Alınmış nəticələrin COVID-19 pandemiyası və postpandemiya dövründə təşkilatlarda kibertəhlükəsizlik sistemlərinin yeni tələblər baxımından təkmilləşdirilməsi işində olduqca faydalı olacağı gözlənilir.

Açar sözlər: *COVID-19, pandemiya, koronavirus, kibertəhlükəsizlik, gizlilik, infodemiya.*

Giriş

2019-cu ilin dekabr ayının sonlarında Çinin Hubei əyalətinin Uhan şəhərində aşkarlanmış naməlum təbiətli sətəlcəm tezliklə bütün dünyada indiyədək görünməmiş müqyasda yayıldı. (Uhan 11 milyondan çox əhali ilə Mərkəzi Çində ən çox əhalisi olan şəhərdir.) Xəstəliyin törədicisinin yeni növ koronavirus olduğu müəyyən edildi və ona Ümumdünya Səhiyyə Təşkilatı (ÜST) tərəfindən COVID-19 adı verildi (ing. COrona VIrus Disease 2019). İlk vaxtlar bu xəstəlik "2019 yeni koronavirus", yaxud "2019-nCoV" olaraq da adlandırılmışdı. COVID-19 koronavirus xəstəliyi dünyada sürətlə asimmetrik olaraq yayıldı, qlobal böhrana çevrildi və ÜST 11 mart 2020-ci ildə bu xəstəliyi pandemiya elan etdi [1, 2].

COVID-19 koronavirus xəstəliyinin qarşısının alınması üçün müxtəlif məhdudlaşdırıcı tədbirlərin görülməsi ilə İnternet insanların əsas əlaqə vasitəsinə çevrilib. Təşkilatların əməkdaşları fiziki olaraq öz iş yerlərindən kənarda işləyirlər və minimal kibertəhlükəsizlik təminatına malikdirlər [3]. Kibercinayətkarlar da COVID-19 pandemiyasının yaratdığı şəraitdən "faydalanmağa" çalışırlar. İşlərin əsas hissəsinin onlayn yerinə yetirilməsini və insanların pandemiya qorxusunu istismar edən kiberhücumların sayı getdikcə artır [4].

Məqalədə COVID-19 pandemiyası dövründə kibertəhlükəsizlik problemləri analiz edilir, daha çox rast gəlinən kiberhücumlar müzakirə edilir və onlayn təhlükəsizliyi təmin etmək üçün tövsiyələr verilir.

COVID-19 koronavirusu

Koronaviruslar ilk dəfə virusları adi soyuqdəymə xəstələrindən yetişdirən D. A. Tyrell və M. L. Bynoe tərəfindən 1966-cı ildə təsvir edilmişdi [5]. Onları nüvəsi və səthdəki çıxıntıları ilə sferik virionlar şəklindəki formasına görə günəş tacına oxşadıqları üçün koronavirus adlandırmışdılar (latınca Corona – tac deməkdir). *Koronaviruslar adi soyuqdəymədən tutmuş* Şiddətli Kəskin Tənəffüs Sindromu (Severe Acute Respiratory Syndrome, SARS) və Yaxın Şərq Tənəffüs Sindromu (Middle East Respiratory Syndrome, MERS) *kimi daha ağır xəstəliklərə səbəb olan geniş bir virus ailəsidir*. Onların dörd altailəsi mövcuddur: alfa-, beta-, qamma- və delta-koronavirusları. Güman edilir ki, alfa- və beta-koronavirusları məməlilərdən, xüsusən də

yarasalardan, qamma- və delta-koronavirusları donuz və quşlardan qaynaqlanır [6]. COVID-19 ilə SARS və MERS koronavirusları arasında genetik oxşarlıq vardır. COVID-19 aşağı tənəffüs yollarına təsir edən və insanlarda sətəlcəm kimi özünü göstərən SARS-CoV-2 adlı bir beta-koronavirusdan qaynaqlanır [7].

Əksər hallarda COVID-19 xəstəliyi yüngül keçir, lakin bəzi insanlarda bu xəstəlik olduqca ağır keçir və bəzi hallarda xəstəlik ölümlə nəticələnə bilər. Risk qrupuna yaşlı insanlar, həmçinin somatik xəstəlikləri (məsələn, ürək xəstəliyi və ya diabet) olan şəxslər aiddir. Hazırki məlumatlara görə, COVID-19-un ölümlə nəticələnmə faizi (dünya ortalaması) SARS üçün 9.6 % və MERS üçün 34.4% ilə müqayisədə təxminən 3.4%-dir (təəssüf ki, bu qiymət yüksələ bilər) [6]. COVID-19-un inkubasiya dövrü – yoluxmadan xəstəliyin kliniki əlamətlərinin yaranmasına qədər olan müddəti uzundur (təxminən 1-14 gün), SARS ilə müqayisədə o daha yoluxucudur və olduqca sürətlə yayılır.

COVID-19 ilə əlaqəli kibertəhdidlərin ümumi mənzərəsi

Kibertəhlükəsizlik təhdidlərinin mənzərəsi COVID-19-un başlaması ilə, praktiki olaraq dəyişməyib. Pandemiya dövrünün kiberhücumları təbiətlərinə görə əvvəlki hücumlara bənzəyir, yeganə fərq odur ki, onlar yeni "libas" geyiniblər. Bədniyyətlilərin kiberhücum motivləri, hədəfləri ssenariləri və alətləri olduqca rəngarəngdir. Onlar COVID-19 ilə əlaqəli daha çox sosial mühəndislik və girov proqramları (ing. ransomware) hücumlarına cəhd edirlər [6]. Pandemiya dövründə kiberhücumların sayında kəskin artım müşahidə edilir, insanlar gərgin emosional vəziyyətdədirlər və beləliklə, kiberhücumlar daha uğurlu alınır. Analiz [4] göstərir ki, Çində pandemiyanın ilk yayılması və COVID-19 ilə əlaqəli ilk kiberhücum arasından xeyli müddət keçmişdir, sonra hücumlar davamlı olaraq artmış və bəzi günlərdə 3 və ya 4 unikal kiberhücum haqqında məlumat verilmişdir.

Sosial mühəndislik hücumları. Bir çox tədqiqatçıya görə, sosial mühəndislik metodları XXI əsr hakerlərinin əsas alətlərindən biridir [9]. Sosial mühəndislik metodları insanı aldatmaq üçün psixoloji fəndlərdən istifadə edir, bu da insanları hərəkətlər etməyə və ya şəxsi və korporativ konfidensial məlumatları bilmədən yaymağa vadar edir. Bədniyyətlilər maliyyə fırıldaqçılığı etmək və zərərli proqramları yaymaq üçün pandemiya dövründə və digər böyük miqyaslı hadisələr zamanı insanların narahatlığından, qorxusundan, marağından və digər zəifliklərindən istifadə edirlər [10].

Sosial mühəndislik metodlarından daha çox fişinq istifadə edilir, onu təkcə veb üzərindən deyil, SMS xidmətləri (Smishing), səsli zəng xidmətləri (Vishing) vasitəsi ilə də həyata keçirirlər. Bu çətin dövrdə fişinq hücumları əhəmiyyətli dərəcədə artmışdır. İnsanlar informasiyaya və ya köməyə möhtacdırlar, buna görə fişinq hücumu belə zamanlarda daha uğurludur. Ən təsirli fişinq hücumları emosiyalara və narahatlıqlara hesablanır və koronavirus barədə təcili informasiya aclığı ilə birləşdikdə belə məlumatlara müqavimət göstərmək olduqca çətin olur [8, 10].

Adətən, fişinq məktublarında istifadəçinin nəyisə klikləməyi, məsələn, COVID-19 haqqında ən son məlumatı öyrənmək üçün və ya ödəmə rekvizitlərini yeniləmək üçün tələb edilir. Fişinq məktublarında ÜST adından tez-tez istifadə edilir [8].

Girov proqramları ilə hücumlar. COVID-19 pandemiyasının yaratdığı fürsətlərdən istifadə edərək kibercinayətkarlar xəstəxanalara, sağlamlıq mərkəzlərinə, təhsil və ictimai qurumlara girov proqramları ilə hücumlar edirlər [4, 8, 10]. Girov proqramları kompüterin bloklanması (verilənlərin girov götürülməsi) üçün zərərli proqram təminatıdır; bədniyyətli belə proqram vasitəsilə hədəf kompüterdə verilənləri şifrələyir və deşifrələmə açarı qarşılığında müəyyən müddətdə ödəniş edilməsini tələb edir. Cinayətkarlar mövcud vəziyyətə görə sistemlərinin bloklanmasını istəməyən təşkilatların girov pulu verə biləcəyinə ümid edirlər. Girov proqramları sistemlərə e-poçt qoşmaları, yoluxdurma linkləri və ya identifikasiya məlumatları ələ keçirilmiş əməkdaşların kompüterləri vasitəsilə yoluxdurulur. Hazırda kibercinayətkarlar, hətta "yeraltı vebdə" (ing. *dark web*) girov proqramı xidmətləri (ing. ransomware-as-a-service) təklif edirlər.

Çoxsaylı girov proqramları mövcuddur. Onlardan bəzilərini qısa təsvir edək.

Winlocker adlı zərərli proqram yoluxmuş kompüterləri bloklayır, işə düşdükdə bəzi faylları silir və Windows reyestrində dəyişiklik edir. Daha sonra səs siqnalı verir və sistemin bloklandığı məlumatını göstərir, sistem yenidən yüklənir və sonra kilidi açmaq üçün parol tələb olunur [11].

CoronaVirus adlı girov proqramı saxta Wise Cleaner (sistemin optimallaşdırılması üçün proqram təminatı) veb saytı vasitəsilə yayılırdı. Qurbanları saxta setap faylını saytdan yükləməyə təşviq edirdilər. Bu zərərli proqram kompüterə quraşdırıldıqdan sonra parolu oğurlaya, məlumatları şifrələyə və sistemdən məlumatları oğurlaya bilər [11].

Mobil telefonlar üçün də xeyli girov proqramı mövcuddur. CovidLock adlı tətbiq, guya COVID-19 hadisələrini izləməyə kömək edən zərərli bir Android tətbiqi ilə gəlir. Girov proqramı qurbanlarının telefonlarını kilidləyir və bərpa üçün bitkoinlə 100 ABŞ dolları ödəmələri üçün 48 saat vaxt verir. Təhdidlərdə telefondakı məlumatların silinməsi və sosial mediada hesab məlumatlarının sızması da yer alır. Başqa bir halda, Android tətbiqi insanlara üz maskası və təhlükəsizlik dəstləri təklif edir. İstifadəçi tətbiqi quraşdıran kimi bu tətbiq SMSTrojan-ı yükləyir, bu troyan qurbanın telefon əlaqə siyahısını açır və özünü yaymaq üçün avtomatik SMS-lər göndərir [10].

Koronavirusla əlaqəli daha bir məşhur zərərli proqram Emotetdir, o, bank troyan proqramıdır, Microsoft Word sənədlərinə zərərli proqram kodu yerləşdirir, istifadəçilərin konfidensial maliyyə məlumatlarının oğurlanmasına imkan verir.

Saxta veb-saytlar və domenlər. 2020-ci ilin fevral-mart aylarında COVID-19 ilə əlaqəli saxta URL-ünvanların alınmasında böyük artım müşahidə edilmişdi [8]. Adətən, burada hədəf COVID-19 ilə əlaqəli xeyli sayda «yaxşı» domen əldə etməkdir ki, sonra fırıldaqçılar onları zərərli proqramları yayan saytlara çevirirlər və «koronavirus» əvəzinə «koronovirus» kimi səhv yazılmış sözlərdən istifadə edərək istifadəçiləri bu domenlərə yönləndirməyə çalışırlar.

Kibertəhdid aktorları koronavirusla əlaqəli informasiyanı reklam edən zərərli veb saytlara keçidlər olan fişinq e-poçtları göndərmək üçün pandemiya mövzusundan da istifadə edirlər. Bu veb saytlarda zərərli proqramlar ola bilər və ya giriş parollarını tələb edən fişinq saytları olması mümkündür. Bəzi zərərli spamlarda da zərərli proqramlara keçidlər və ya zərərli proqram quraşdırılmış qoşmalar ola bilər. Bu keçidləri və ya zərərli qoşmaları açan qurbanların öz kompüterlərini bədniyyətli aktorların istifadəsinə vermək riski var.

Johns Hopkins Universitetində yeni koronavirus haqqında informasiyanı və ölüm hallarını göstərmək üçün onlayn interaktiv xəritə hazırlanmışdır [12]. Hakerlər ona java əsaslı zərərli proqram yerləşdirmişdilər, əksər qurbanlar təkcə xəritəni açmaqla kifayətlənməmiş, həm də xəritəni paylaşmışdılar, yəni həm özləri yoluxmuş, həm də zərərli proqramı yaymışdılar [10].

DDoS hücumları. Ən pis hal ssenarisində qəddar, heç bir etika gözləməyən hakerlər səhiyyə sektorunu hədəfə alırlar, onlar tibbi resursları istismar edirlər və intensiv terapiya sistemlərinə girişlərin qarşısını alırlar, bu ölümə səbəb ola bilər [13].

Kibercasusluq. ABŞ və Böyük Britaniya səlahiyyətli orqanları milli səhiyyə siyasətinə dair kəşfiyyat və COVID-19 ilə əlaqəli araşdırmalara dair sensitiv məlumatlar da daxil olmaqla zərərli kiber fəaliyyətə qarşı xəbərdarlıq etmişdi [14]. Bu xəbərdarlıq COVID-19 üzrə tədqiqatlar sahəsində intellektual mülkiyyət oğurluğu ilə bağlı sualları da meydana çıxarmışdı.

Hibrid hücumlar. COVID-19-un yaratdığı fəsadların miqyası, şübhəsiz ki, bioterroristlərin də diqqətini cəlb edəcəkdir [15]. İqtisadi fəaliyyətlərin reallaşdırılmasında rəqəmsal texnologiyaların rolu getdikcə artır və bu şəraitdə hibrid hücumlar (bioloji və rəqəmsal) dünya iqtisadiyyatı üçün ölümcül ola bilər. Kiberhücumların çoxunun hibrid (hərbi və mülki) olması barədə məlumatlar artmaqdadır və çoxvektorlu hücumların başvermə ehtimallarının analizi metodları işlənilməlidir. Hibrid hücumlar nəticəsində yarana bilən katastrofik (fəlakətli) risklərin qarşısının alınması üçün ölkələrdə dinamik, çevik və dayanıqlı mərkəzlər yoxdur. Belə mərkəzlər müxtəlif növ insidentlərin idarə edilməsi ilə məşğul olan qurumların fəaliyyətini koordinasiya etməlidir, onu mövcud informasiya infrastrukturları, yüksək texnologiyalar və qabaqcıl risk analizi üsulları əsasında minimal investisiyalar cəlb etməklə qurmaq olar.

COVID-19 və fərdi məlumatların təhlükəsizliyi

COVID-19 pandemiyasını dayandırmaq üçün dünyanın hər yerində hökumətlər və özəl şirkətlər virusun yayılmasını yavaşıtmaq niyyətilə süni intellektin köməyi ilə nəzarət, hesabatlılıq və izləmə texnologiyalarından istifadə edirlər. Bu texnologiyalar ictimai nəzarət və vətəndaşların təhlükəsizliyi üçün fərdi məlumatları toplayır, analiz edir və paylaşırlar, bu dövlət orqanları ilə vətəndaşların əməkdaşlığına kömək edir. Bir çox müəllif epidemiyaya nəzarət üçün olan bu texnoloji infrastrukturun fərdi məlumatların təhlükəsizliyi, insan ləyaqəti, vətəndaş azadlıqları, şəffaflıq baxımından orta və uzunmüddətli dövrdə ciddi etik və tənzimləmə nəticələrinin ola biləcəyini iddia edir [16].

Avropa İttifaqının 2018-ci ilin mayından qüvvəyə minmiş fərdi məlumatların konfidensiallığının təmin edilməsi üzrə yeni qanunu GDPR (General Data Protection Regulation) bu sahədə ciddi tədbirlər nəzərdə tutur. Fərdi məlumatların qorunması tənzimləyiciləri və bəzi hüquqşünaslar bildirirlər ki, GDPR qanunu COVID-19-a qarşı mübarizədə zəruri olan məlumatların emalı yolunda maneə olmayacaq [17]. Bu texniki baxımdan doğrudur, çünki GDPR pandemiya kimi çox ciddi vəziyyətlərdə məlumatların qorunması qaydalarının yumşaldılmasına imkan verir. Qanuna uyğunluq məsələsində irəliləyiş əldə etmək üçün milli qanunların təfərrüatlarını və nüanslarını başa düşmək lazımdır. Bunlar ölkədən-ölkəyə fərqlənir və real istifadə variantlarına baxıldıqda, qanun ilkin tələblərdə göstərildiyi kimi icazəverici olmaya bilər [18].

Fərdi məlumatların gizliliyi və ictimai təhlükəsizlik mövzusunda "köhnə" mübahisə hələ də bitməyib. Pandemiya böhranında ictimai təhlükəsizlik əsas prioritetdir və dövlətlər müəyyən məlumatların təxirəsalınmaz ictimai məqsədlər üçün qanuni istifadəsinə nail olmağa çalışırlar, lakin bu zaman gizlilik hüquqları risk altına düşə bilər [19, 20]. Xüsusilə, fərdi məlumatlar COVID-19 kimi pandemiya böhranını idarə etmək üçün vacib olduqda, "qeyri-aşkar" razılıq gözlənilən olacaq [20].

Bir çox ölkə yoluxmuş insanların əhəmiyyətli bir hissəsinin yaşadığı xüsusi şəhər və rayonları tapmaq üçün insanların mobil telefonlarına görə yerlərini və digər məlumatlarını izləməyə başlayır. Məsələn, Çin hökuməti virusla yoluxmuş insanları izləyir, məqsəd başqa insanların yoluxmaması üçün onların evdə qalmalarından əmin olmaqdır. İnsanlar evlərindən çıxmaq üçün QR kodu skan etməlidirlər və COVID-19 test nəticələri əsasında aldıqları rəng koduna görə hərəkət edirlər, yəni yaşıl – sağlamdır, qırmızı – karantin edilir və çölə çıxa bilməz.

İctimai təhlükəsizliyi təmin etmək üçün, Koreya fərdi məlumatları fəal şəkildə istifadə edir, Fransa isə ictimai təhlükəsizlik riskində könüllü əməkdaşlığı təşviq edir. [21]-də epidemioloji araşdırmalarda bu iki fərqli yanaşmanın müsbət və mənfi tərəfləri araşdırılır.

Mühüm məqamlardan biri də, COVID-19-a qarşı mübarizə və vaksinlərin hazırlanması üçün fərdi məlumatların istifadə edilməsidir. Məsələn, Almaniyada Telekom adlı telekommunikasiya provayderi COVID-19 ilə mübarizədə vətəndaşların mobilliyini monitorinq etmək üçün mobil telefonların hərəkət məlumatlarını Robert Koch İnstitutuna (RKİ) təqdim etmişdi (ümumilikdə, 46 milyon müştərinin anonimləşdirilmiş verilənləri) [22]. Qeyd edək ki, Avropa Verilənlərin Mühafizəsi Şurası COVID-19 epidemiyası kontekstində fərdi məlumatların emalı üzrə bəyanat yaymışdır [23].

Fərdi məlumatların elmi tədqiqatlar üçün açıq edilməsi zamanı bu məlumatların təhlükəsizliyinə cavabdeh təşkilatlar, adətən, de-identifikasiya metodlarından istifadə edirlər [24]. Fərdi məlumatların de-identifikasiyasına müxtəlif yanaşmalar mövcuddur. HIPAA (Health Insurance Portability and Accountability Act) gizlilik qaydalarında fərdi tibbi məlumatların de-identifikasiyasına dair iki yanaşma təklif olunur: təhlükəsiz liman metodu və ekspert təyini metodu [24]. Təhlükəsiz liman metodu ad, sosial təhlükəsizlik nömrəsi, əlaqə məlumatları, IP ünvanı, barmaq izi, foto və ünvan məlumatları kimi 18 fərdi identifikasiya məlumatını silir. Ekspert təyini metodunda isə silinəcək fərdi məlumatları ekspertlər müəyyən edirlər.

Açıqlamaq və unutmaq modeli, məlumatların istifadəsi müqaviləsi modeli və anklav modeli də fərdi məlumatların saxlanması və istifadəsi proseslərində istifadə edilir [25].

Toplanmış fərdi məlumatların elmi istifadə dəyərini qorumaq və eyni zamanda fərdi məlumatları de-identifikasiya etmək asan deyil. Bu iki amil bir-biri ilə ziddiyyətdədir [21]. Başqa sözlə, tədqiqatçılar fərdi məlumatların minimum de-identifikasiya səviyyəsinə malik orijinal məlumatlardan istifadə edərək daha dəqiq analiz nəticələri almaq istəyirlər. Digər tərəfdən, məlumatları təqdim edən qurumlar məlumatların anonimliyini təmin etməklə fərdi gizlilik tələblərini ödəməyə çalışırlar. De-identifikasiyanın səviyyəsi artdıqca məlumatların keyfiyyəti və tədqiqat nəticələrinin dəqiqliyi aşağı düşür. Əksinə, de-identifikasiyanın səviyyəsi aşağı olarsa, məlumatların keyfiyyəti və nəticələrin dəqiqliyi daha yüksək olur [21].

De-identifikasiya texnologiyaları geniş yayılsa da, de-identifikasiya edilmiş verilənlərdən şəxslərin re-identifikasiya edilməsinin qarşısını almaq çətindir. Tədqiqatçılar qrupu de-identifikasiya edilmiş verilənlərdən istifadə edərək müəyyən əlamətləri dəqiq tapa bilmişdir [26]. Onların maşın öyrənmə modeli yalnız 15 demoqrafik əlamətdən (yaş, cins, ailə vəziyyəti və s.) istifadə edərək istənilən anonim verilənlərdən şəxsləri 99.98% dəqiqliyi müəyyən edə bilər.

Alternativlərdən biri de-identifikasiya ideyasından müvafiq texnologiyaların tətbiqinə keçməkdir. Verilənlərin istifadəsi və fərdi gizlilik arasında balans tapmaq lazımdır. Son zamanlar bu sahədə təhlükəsiz çoxtərəfli hesablamalar və homomorf şifrələmə kimi texnologiyalar ortaya çıxır [27].

Pandemiya və e-səhiyyə sistemlərinin kibertəhlükəsizliyi problemləri

Müasir informasiya və kommunikasiya texnologiyaları (İKT) səhiyyədə innovasiyalar üçün prinsipial yeni imkanlar yaradır. Elektron səhiyyə (e-səhiyyə, ing. eHealth) İKT-dən istifadə edərək xəstəliklərin qarşısının alınması, diaqnostikası, müalicəsi, monitorinqi və səhiyyənin menecmentini yaxşılaşdıra bilən alətləri və xidmətləri bildirir [24].

E-səhiyyədə tətbiq edilən 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 (Internet of Things) və s. daxildir [24].

E-səhiyyədə əhəmiyyətli problemlərdən biri kibertəhlükəsizliyin təmin edilməsidir. 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 sistemlərində kibertəhlükəsizliyin yüksək səviyyədə təmin edilməsini tələb edir, çünki belə sistemlərdə informasiya təhlükəsizliyinin pozulması birbaşa insan həyatına təhdidlər törədə bilər [24]. E-səhiyyədə əsas kibertəhdidlərə zərərli proqramların kritik tibbi sistemləri və qurğuları yoluxdurması, tibbi məlumatların oğurlanması, tibbi cihazlara kiber hücumlar, kibertəhlükəsizlik tələblərinə cavab verməyən tibbi cihazların istifadəsi daxildir. Pandemiya ilə əlaqədar yeni kibertəhlükəsizlik təhdidləri də meydana çıxır.

Səhiyyə sənayesi dünyanın ən böyük və ən inkişaf etmiş sahələrindən biridir və tibbi məlumatların sensitiv təbiəti onları kibercinayətkarlar üçün qiymətli və cəlbedici edir, kibercinayətkarlar gizli məlumatları oğurlamaq, manipulyasiya etmək və səhiyyə ekosistemində əməliyyatları pozmaq üçün boşluqları olan şəbəkələrə və sistemlərə əhəmiyyətli kapital qoyurlar. Tibbi xidmətlərin keyfiyyəti və e-səhiyyə sistemlərində idarəetmənin effektivliyi etibarlı məlumatlardan asılıdır. Kibertəhlükəsizlik e-səhiyyə verilənlərinin konfidensiallığını, tamlığını və əlçatanlığını qorumaq və məlumat sızmasının təsirini minimuma endirmək üçün etibarlı bir yoldur.

Bütün dünyada COVID-19 pandemiyası tibbi diaqnoz, xəstəxanaya yerləşdirmə statistikası, infeksiya nisbəti, xəstələrin xəritəsinin tərtibi, dərman allergiyası, ölüm dərəcəsi və digər incə metadata daxil olmaqla birbaşa böhran mənbəyindən böyük həcmdə tibb məlumatların yaranmasına səbəb olur. Bəzi məlumatlar açıq olsa da, digərləri həssasdır və düzgün idarəetmə və təhlükəsizlik tələb edir. Pis qorunan tibbi məlumatlar səbəbindən səhv diaqnoz qoyula və ya, hətta COVID-19-un yayılmasına qarşı edilən cəhdlər heçə endirilə bilər.

COVID-19 pandemiyası ona gətirib çıxarır ki, pandemiyanın idarə edilməsi üçün müxtəlif ölkələrdə rəqəmsal nəzarət sistemləri işlənilir [28], onların bəziləri verilənləri toplamaq, analiz etmək və mübadilə etmək üçün avtonom işləyirlər, yəni kiber-fiziki sistemlərdir (KFS). Nəzərə almaq lazımdır ki, KFS-lərin e-səhiyyə sistemlərinə inteqrasiyası zamanı gözlənilməyən və çox vaxt görünməyən kiberrisklər yaranır, onlar hazırda tənzimlənmirlər və çox zaman nəzərə alınmırlar. Bunların çox sürətlə inkişaf edən yeni texnologiyalar olduğunu nəzərə alsaq, demək olar ki, hər bir yeni dizaynda rəqəmsal pandemiya monitorinq sistemləri yüksək risk kateqoriyasına aiddirlər. Tibbi sistemlərin rəqəmsallaşdırılması pandemiyanın idarə edilməsi üçün böyük əhəmiyyət kəsb etsə də, səylər fərdi məlumatları kiberriskə məruz qoya və vəziyyəti daha da pisləşdirə biləcək sistemlərin yaradılmasına deyil, pandemiya idarəçiliyinə dəyər qatacaq həllərə yönəldilməlidir [28].

Bundan başqa, riskin ötürülməsi üçün müvafiq kibersığorta siyasətləri yoxdur, həm də bu yeni tibbi sistemlərin idarə olunması üçün standartlar və qaydalar mövcud deyil. Bu şərtləri nəzərə alaraq risklərin siniflərə bölünməsi aktuallaşır. Sistemlərin potensial risklərə uyğun olaraq ayrılması ilə, tibb mütəxəssisləri kiberhücumlar və ya verilənlərin konfidensiallığının pozulması zamanı ən azı pandemiya idarəetmə sisteminin hissələrini işlədə bilərlər.

Video konfrans və teleiş bəzi sənaye sahələrində geniş tətbiq olunsa da, bu texnologiyaların e-səhiyyə sistemlərində tətbiqi HIPAA tələblərinin tibbi kommunikasiya proqramlarına qismən təsiri səbəbindən geridə qalır [29].

Bir çox telekonfrans sistemlərində şifrələmə kimi etibarlı konfidensiallıq elementləri tətbiq edilir; lakin konfidensiallıq qaydasında tələb olunan audit yoxlamaları göstərilmədikdə bunlar HIPAA tələblərinə cavab vermir: qorunan tibbi məlumatlar yaradıldıqda, dəyişdirildikdə, giriş edildikdə, paylaşıldıqda və ya silindikdə sistem administratorlarının audit jurnallarını yazmaq və izləmək imkanı olmalıdır [29]. Buraya pasiyentlərlə şifrələnmiş rabitə də daxildir. Bu səbəbdən, telekonfrans və gizli mətn mesajlaşma sistemləri HIPAA ilə uyğun deyil.

HIPAA-nın diqqətlə nəzərdən keçirilməsi və düzəlişlər edilməsi tibb işçilərinə COVID-19 fəlakəti zamanı və ondan sonra pasiyentlərin xeyrinə teletibb xidmətlərini optimallaşdırmağı davam etdirməyə imkan verə bilər [30].

İnfodemiya ilə mübarizə

Dünya COVID-19-un yayılmasını cilovlamaq üçün mümkün bir müalicə və ya vasitə gözlədiyi üçün, "koronavirus" sözünə birbaşa və ya dolayı istinad edən hər bir məlumat internet istifadəçilərinin diqqətini cəlb edir. Nəticədə kibercinayətkarlar koronavirusun yayılması ətrafındakı qorxu və qeyri-müəyyənlikdən dezinformasiya yaymaq üçün istifadə edirlər.

ÜST fevralın ortalarında bildirmişdi ki, onlar pandemiya ilə mübarizə ilə yanaşı, koronavirusdan daha asan və sürətlə yayılan infodemiya (ing. infodemics) – yalan məlumatların geniş yayılması ilə də mübarizə aparırlar.

ÜST-ə görə, infodemiya – səhiyyə sahəsində fövqəladə vəziyyət zamanı problem haqqında böyük həcmdə yalan, saxta informasiya, dezinformasiya və şaiələrin yayılmasıdır. İnfodemiya həll axtarışını çətinləşdirə, effektiv ictimai səhiyyə tədbirlərinə manea ola, insanlar arasında çaşqınlıq və inamsızlıq yarada bilər. Bu problemi həll etmək üçün ÜST Facebook, Google, Pinterest, Tencent, Twitter, TikTok, YouTube və digər axtarış və media şirkətləri ilə birgə işləyir və dezinformasiya da daxil olmaqla şaiələrin qarşısını almağa çalışır. Məlumatlara görə, bu şirkətlər əsaslandırılmamış tibbi məsləhətlərin, yalan məlumatların və əhalinin sağlamlığına qarşı risk yaradan digər yalan informasiyanın qarşısını fəal şəkildə alırlar [31].

İnsanlar COVID-19 pandemiyasına qarşı mübarizə tədbirləri səbəbindən fiziki ictimai məkanları tərk edirlər, buna görə onlayn platformalar sosial müzakirələri başa düşmək üçün daha məşhur vasitə olurlar. Böyük qlobal hadisələr və pandemiyalar zamanı dezinformasiyanın potensialı böyükdür və istifadəçilər sosial mediada gördükləri yazılara etibar etməzdən və reaksiya

verməzdən əvvəl bu məlumatları yoxlamalıdırlar. Bədniyyətli aktorlar tez-tez yalan məlumatları və ya zərərli saytlara keçidləri yerləşdirmək üçün sosial mediadan istifadə edirlər.

Sosial media platformalarında çox sayda botlar, avtomatlaşdırılmış hesablar da vardır, onlar müəyyən müzakirə mövzularını başqalarının hesabına gücləndirə bilirlər. [32]-də COVID-19 haqqında toplanmış 43.3 milyon ingilisdilli tvit botların davranışı və müzakirələrin əsas mövzusu baxımından analiz edilir. Bu analizin nəticəsində botların ABŞ-da siyasi sui-qəsd fikirlərini təşviq etmək üçün istifadə olunduğuna dair ilkin sübutlar əldə edilmişdir, botlar ictimai sağlamlıq problemlərinə fokuslanan insanlardan kəskin fərqlənirlər.

COVID-19 pandemiyası, həm də ölkələrin informasiya qarşıdurması alətinə çevrilmişdir [33]. Bəzi ölkələr COVID-19-un yayılmasında ABŞ kəşfiyyatını günahlandırırlar. ABŞ və Böyük Britaniya hökumətləri bəzi ölkələr tərəfindən yalnış məlumatların qəsdən yayılması ilə bağlı ittihamlar irəli sürürlər [34], bunlar pandemiya ilə mübarizədə beynəlxalq əməkdaşlığı daha da çətinləşdirir.

Evdən iş zamanı kibertəhlükəsizliyin təmin edilməsi məsələləri

Əksər ölkələrin tətbiq etdiyi karantin tədbirləri və sosial məsafəni saxlamaq zəruriyyəti "evdən iş" konsepsiyasının geniş tətbiqinə səbəb oldu. Evdən iş zamanı fərdlər mobil və ya digər rəqəmsal platformalardan geniş istifadə sayəsində öz işlərini evdən yerinə yetirirlər. Hazırkı COVID-19 pandemiyası zamanı müəssisələr fəaliyyətlərini davam etdirmək üçün öz əməkdaşlarını mümkün olduqca evdən iş rejiminə keçirməyə məcbur olurlar.

Beləliklə, COVID-19 pandemiyası qlobal miqyasda çox sayda işçinin uzaqdan işləmək məcburiyyətində qalmasına səbəb olur. Lakin evdən işləyən işçilər normal şəraitdə malik olduqları ilə müqayisədə minimal kibertəhlükəsizlik resurslarına malikdirlər [8]. Kiber təcavüzkarlar da zərərli proqramları yerləşdirmək və məsafədən işləyən yeni qüvvələrdən faydalanmaq üçün bütün bacarıqları ilə koronavirusdan istifadə edirlər.

Çox sayda konfidensial müştəri məlumatları ilə işləyən təşkilatlar evdən iş zamanı işçilərin etibarlı mühitdə işləmələrini təmin etməlidirlər. Burada ilk addım yalnız noutbuklarda deyil, ağıllı telefonlarda və ya işçilərin müştəri məlumatlarına daxil olmaq üçün istifadə edə biləcəkləri hər hansı digər şəxsi qurğularda da düzgün təhlükəsizlik proqram təminatını quraşdırmaq və avtomatik yeniləmələri təmin etməkdir.

İstifadəçilərin kiberhücum qurbanına çevrilməsinin əsas səbəbləri pis qorunan qurğular və istifadəçinin kiber məlumatlılığının olmamasıdır [35]. Buna cavab olaraq, bir çox təşkilat əlavə kibertəhlükəsizlik tədbirləri tətbiq edir (məsələn, ikifaktorlu autentifikasiya, antivirus və zərərli proqramlardan mühafizə, VPN (Virtual Private Network) təşkilatın təmin etdiyi qurğular, şifrələmə və s.). Evdən işləyən istifadəçilərin gizlilik və kibertəhlükəsizlik təhdidləri barədə maarifləndirilməsi və təlimatlandırılmasına xüsusi diqqət verilməlidir. Onlar koronavirus qorxusundan istifadə edən fişinq hücumlarından məlumatlı və bilikli olmalı, onları və kiberhücumların digər növlərini necə aşkarlamağı və onlara necə reaksiya verməyi bilməlidirlər.

COVID-19 dövründə hakerlərin diqqət mərkəzində olan populyar hədəflərdən biri də onlayn video konfrans və birgə iş platformalarıdır [10].

Zoom, Microsoft Teams və Google Meet kimi onlayn videokonfrans proqramlarının istifadəçilərinin sayı pandemiya dövründə kəskin artmışdır. Videokonfrans və digər oxşar əməkdaşlıq alətlərinə yüksək tələbat səbəbindən bu alətlərdə hakerlərin istismarı üçün bir çox boşluqlar üzə çıxa bilər. Hazırda populyarlığı sürətlə artan Zoom ciddi neqativ reaksiya ilə üzləşir, çünki təhlükəsizlik mütəxəssisləri, fərdi məlumatların müdafiəçiləri və hətta FTB (Federal Təhqiqat Bürosu) Zoom-un standart parametrlərinin təhlükəsiz olmadığı barədə xəbərdarlıq edirlər. Nəticədə NASA (National Aeronautics and Space Administration), SpaceX kimi bir çox şirkət, Tayvan, ABŞ və Avstraliya kimi bəzi ölkələr Zoom-u kommunikasiya üçün qadağan etmişlər [10].

Bir hesabatda Google Meet, Microsoft Team və Zoom kimi tətbiqlərin gizlilik siyasətləri analiz edilmiş və onların insanların güman etdiklərindən daha çox məlumat topladıqları qənaətinə gəlinmişdi [30].

Şəbəkə təhlükəsizliyinə ənənəvi yanaşmada təşkilatlar diqqəti ilk növbədə güclü şəbəkə perimetrinin qurulmasına yönəldirdilər, hazırda bu sahədə paradiqma dəyişikliyi baş verib və "sıfır etibarlı arxitektura" tətbiq edilir.

"Sıfır etibar" terminini 2010-cu ildə Forrester Research John Kindervag daxil etmişdi [36]. Sıfır etibar modeli (Zero Trust) yeni şəbəkə təhlükəsizliyi paradiqmalarının çoxluğudur, onların əsasında "heç kimə heç nəyi etibar etmə" prinsipi dayanır. Perimetrin müdafiəsinə böyük diqqət yetirən klassik yanaşmalardan fərqli olaraq Zero Trust modeli şəbəkə seqmentlərinin deyil, resursların təhlükəsizliyi üzərində fokuslanır. Zero Trust arxitekturasının fərqləndirici xüsusiyyəti təşkilatın hər bir resursuna giriş vermək üçün autentifikasiya və avtorizasiyaya böyük diqqət verilməsidir. Həm də autentifikasiya mexanizmlərində zaman gecikmələrinin minimallaşdırılması tələb edilir.

2020-ci ilin əvvəlində ABŞ Milli Standartlar və Texnologiyalar İnstitutu (NIST) tərəfindən nəşr edilmiş sənəddə sıfır etibarlı arxitekturanın əsas məntiqi komponentlərinə baxılır [37]. Artıq bəzi təşkilatların korporativ infrastrukturunda sıfır etibarlı arxitektura elementləri vardır. NIST təşkilatlara sıfır etibar modelini tədricən tətbiq etmələrini tövsiyə edir. Korporativ infrastrukturların əksəriyyətinin hələ uzun müddət sıfır etibar/perimetr hibrid rejimində işləyəcəyi gözlənilir [38].

Kompüter virusları da bioloji viruslar kimi çox asan və sürətli yayıla bilir. Koronovirusdan qorunmaq üçün şəxsi gigiyena qaydalarına da əməl edilməlidir. [39]-da COVID-19 pandemiyası dövründə kibercinayət təhlükələrini aradan qaldırmağa kömək edə biləcək gigiyena protokolları təqdim edilir. Təhsil protokolu, təlim protokolu və siyasət protokolları təsvir edilir. Məqalədə, həmçinin teleiş (məsafədən görülən iş) üzrə NIST standartları və İnformasiya Texnologiyaları Laboratoriyasının (ITL, 2020) rəhbər prinsipləri nəzərdən keçirilir [40].

Kiberhücumların aşkarlanması və qarşısının alınması üçün tətbiq olunan təhlükəsizlik sisteminin gücünə baxmayaraq, uğurlu kiberhücumlardan sonra bərpa planının olması vacibdir ki, başvermə halında onların nəticələri minimallaşdırılsın. Bərpa planları, bütün mobil və məsafədəki onlayn sistemlərdə gündəlik məlumatların ehtiyat nüsxəsi strategiyası, kiber məlumatlılıq və xüsusilə, mobil cihazlarda və İnternet tətbiqlərində etibarlı rəqəmsal etikaya riayət etməklə gözlənilir.

Koronavirus, demək olar ki, hər bir şirkətin işləmə metodunu dəyişmiş, kibertəhlükəsizlik və əməliyyat risklərini ağırlaşdırmışdır. Pandemiya dövründə kibersığorta şirkətlərin sığorta portfelində belə yüksək riskləri nəzərə alan və yumşaldan əsas təklif ola bilər [41]. Kibersığorta – müəssisələri və onlara xidmət göstərən şəxsləri İnternet əsaslı risklərdən qorumaq üçün nəzərdə tutulmuş xüsusi bir sığorta məhsuludur.

Nəticə

Bütün dünyanı sarmış COVID-19 pandemiyasına qarşı ölkələrdə bir çox təşəbbüslər həyata keçirilir. Bu tədbirlər özləri ilə müəyyən təhlükəsizlik və gizlilik riskləri də gətirir, COVID-19 müxtəlif bədniyyətli təşəbbüslərdə istifadə edilir. Bu koronavirusa yoluxanların sayı artdıqca bu xəstəliyi cəlbedici tələ kimi istifadə edən bədniyyətli kampaniyaların sayı da artır.

COVID-19 pandemiyası zamanı dəqiq və etibarlı tibbi məlumatlara artan tələbatla əlaqədar olaraq səhiyyə sənayesi görünməmiş sayda və miqyasda kibertəhlükəsizlik problemləri ilə üzləşir. Bu kibertəhlükəsizlik problemlərinin miqyasını düzgün anlamaq onların pis mühafizəsi ilə əlaqəli ciddi nəticələrdən qaçmaq üçün lazımdır.

Texnologiyalardan asılılığın atrması və kiberhücumların mürəkkəbləşməsi səbəbindən kibertəhlükəsizlik riski təşkilatlar üçün gələcək 20 ildə ən böyük risk adlandırılırdı. COVID-19

pandemiyası korporativ mənzərəni köküdən dəyişdi və indi təşkilatların çoxu başa düşür ki, gələcək 20 il ərzində gözlədikləri kiberrisklər cəmisi bir neçə həftə ərzində onların qapılarına çatıbdır.

İnternet mövcud olduqca kibertəhlükəsizlik də çox vacib olacaq. Kibertəhlükəsizlik sahəsində təhsil, təlim və maarifləndirmə həmişə olduğu kimi, COVID-19 pandemiyası dövründə də və ondan sonra da kibertəhlükəsizlik təhdidlərinin qarşısının alınması üçün bir nömrəli vasitə olaraq qalacaqdır.

Ədəbiyyat

1. The World Health Organization (WHO). Coronavirus disease (COVID-2019) situation reports, https://www.who.int/emergencies/diseases/novel-coronavirus-2019/situation-reports
2. Sohrabi C., Alsafi Z., O'Neill N., Khan M., Kerwan A., Al-Jabir A., Iosifidis C. & Agha R. World Health Organization declares global emergency: A review of the 2019 novel coronavirus (COVID-19) // International Journal of Surgery, 2020, vol. 76, pp. 71-76.
3. Ahmad T. Corona virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity, 2020, DOI: 10.2139/ssrn.3568830.
4. Lallie H. S., Shepherd L. A., Nurse J. R., Erola A., Epiphaniou G., Maple C., & Bellekens X. Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv preprint arXiv:2006.11929, 2020, 20 p.
5. Tyrrell D.A., Bynoe M.L. Cultivation of viruses from a high proportion of patients with colds // Lancet, 1966, Vol. 1 (7428), pp. 76–77.
6. Velavan T. P., Meyer C. G. The COVID-19 epidemic // Tropical medicine & international health, 2020, vol. 25, no. 3, pp. 278-280.
7. Wang L.S., Wang Y.R., Ye D.W., & Liu Q.Q. A review of the 2019 novel coronavirus (COVID-19) based on current evidence // International Journal of Antimicrobial Agents, 2020, vol. 55, no. 6, 105948, pp. 1-7, DOI: 10.1016/j.ijantimicag.2020.105948.
8. Fontanilla M.V. Cybercrime pandemic // Eubios Journal of Asian and International Bioethics, 2020, vol. 30, no. 4, pp. 161-165.
9. Krombholz K., Hobel H., Huber M., & Weippl E. Advanced social engineering attacks // Journal of Information Security and applications, 2015, vol. 22, pp. 113-122.
10. Khan N. A., Brohi S. N., & Zaman N. Ten deadly cyber security threats amid COVID-19 pandemic. TechRxiv. Preprint. 2020, 6 p. DOI: 10.36227/techrxiv.12278792.v1
11. Trend Micro, Developing Story: COVID-19 Used in Malicious Campaigns. 2020, https://www.trendmicro.com/vinfo/us/security/news/cybercrimeand-digital-threats/coronavirus-used-in-spam-malware-file-namesand-malicious-domains
12. Johns Hopkins University, Coronavirus COVID-19 Global Cases by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU), 2020, https://coronavirus.jhu.edu/map.html.
13. Stein S., and Jacobs J. Cyber-attack hits U.S. health agency amid Covid-19 outbreak, 2020, https://www.bloomberg.com/news/articles/2020-03-16/u-s-healthagency-suffers-cyber-attack-during-covid-19-response.
14. National Cyber Security Centre Advisory: APT groups target healthcare and essential services. 5 May, 2020, https://www.ncsc.gov.uk/les/Joint%20NCSC%20and%20CISA%20Advisory%20APT%20groups%20target%20healthcare%20and%20essential%20services.pdf
15. Bruno D. COVID-19 and cybercrime: How rogue nations and cyber criminals are exploiting a global crisis. Northern Policy Institute: Briefing Note No. 17, May 2020, 13 p.
16. Ienca M., and Vayena E. On the responsible use of digital data to tackle the COVID-19 pandemic // Nature Medicine, 2020, No. 26, pp. 463–464. DOI: 10.1038/s41591-020-0832-5.
17. Renda A., & Castro R. Towards stronger EU governance of health threats after the COVID-19 pandemic // European Journal of Risk Regulation, 2020, pp. 1-10.

18. Goniewicz K., Khorram-Manesh A., Hertelendy A.J., Goniewicz M., Naylor K., & Burkle F.M. Current response and management decisions of the European Union to the COVID-19 outbreak: a review // Sustainability, 2020, vol. 12(9), 3838.
19. Mouton F., de Coning A. COVID-19: Impact on the cyber security threat landscape (pre-print), March 2020, 18 p.
20. Remolina L.N., & Findlay M. Regulating personal data usage in COVID-19 control conditions. SMU Centre for AI & Data Governance Research Paper No 2020/04, 2020, 42 p.
21. Ahn N.Y., Park J.E., Lee D.H., & Hong P.C. Balancing personal privacy and public safety in COVID-19: Case of Korea and France. arXiv preprint arXiv:2004.14495. 2020, 9 p.
22. Daubenschuetz T., Kulyk O., Neumann S., Hinterleitner I., et al. SARS-CoV-2, a Threat to Privacy? arXiv preprint arXiv:2004.10305. 2020, 7 p.
23. EU: Statement on the processing of personal data in the context of the COVID-19 outbreak. 2020, https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en
24. İmamverdiyev Y.N. E-səhiyyə: İnformasiya təhlükəsizliyinin aktual problemləri / "Elektron tibbin multidissiplinar problemləri" I respublika elmi-praktiki konfransı, 2016, pp. 32-38.
25. Garfinkel S.L. De-identification of personal information (NISTIR 8053). National Institute of Standards and Technology, 2015, DOI: 10.6028/NIST.IR.8053.
26. Rocher L., Hendrickx J.M., and Montjoye Y.D. Estimating the success of re-identifications in incomplete datasets using generative models // Nature Communications, vol. 10, no. 3069, 2019, DOI: 10.1038/s41467-019-10933-3.
27. İmamverdiyev Y.N. Konfidensiallığı qorumaqla fərdi məlumatların intellektual analizi üçün Deep Learning metodları / "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" V respublika konfransı, Bakı, 29 noyabr 2019-cu il, pp. 74-80.
28. Radanliev P., De Roure D., & Van Kleek M. Digitalization of COVID-19 pandemic management and cyber risk from connected systems. arXiv preprint arXiv:2005.12409. IEEE Internet of Things News, 2020, 8 p.
29. Bhate C., Ho C.H., & Brodell R.T. Time to revisit HIPAA? Accelerated telehealth adoption during the COVID-19 pandemic // Journal of the American Academy of Dermatology, 2020, DOI: 10.1016/j.jaad.2020.06.989.
30. Portnoy J., Waller M., Elliot T. Telemedicine in the era of COVID-19 // The Journal of Allergy and Clinical Immunology: In Practice, 2020, Vol. 8, No. 5, pp. 1489-91.
31. Gradon K. Crime in the time of the plague: Fake news pandemic and the challenges to law-enforcement and intelligence community // Society Register, 2020, vol. 4, no. 2, pp. 133-148.
32. Ferrara E. # covid-19 on twitter: Bots, conspiracies, and social media activism. arXiv preprint arXiv:2004.09531. 2020, 25 p.
33. Sukhankin S. COVID-19 as a tool of information confrontation: Russia's approach // The School of Public Policy Publications, 2020, vol. 13, no. 3, 11 p.
34. Moore M. FBI to warn of Chinese hackers trying to steal coronavirus vaccine data. New York Post. 2020, May 11, https://www.nypost.com/2020/05/11/fbi-towarn-of-hackers-trying-to-steal-coronavirus-vaccine-data
35. Room S. COVID-19, adverse scrutiny and the journey to code: where next for biometric tech? Biometric Technology Today, 2020, No. 5, pp. 9-11.
36. Kindervag J. Build security into your network's DNA: The zero trust network architecture. Forrester Research Inc.: Cambridge, MA, USA, 2010. pp. 1–26.
37. Rose S., Borchert O., Mitchell S., & Connelly S. Zero trust architecture. NIST Special Publication (SP) 800-207 (2nd Draft). National Institute of Standards and Technology. 2020, 58 p., DOI: 10.6028/NIST.SP.800-207-draft2.
38. Gilman E., & Barth D. Zero trust networks: Building trusted systems in untrusted networks. O'Reilly Media; 1 edition, 2017, 240 p.

39. Abukari A. M., & Bankas E. K. Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond // International Journal of Scientific & Engineering Research, 2020, vol. 11, Issue 4, pp.1401-1407.
40. Souppaya M., and Scarfone K. Guide to enterprise telework, remote access, and bring your own device (BYOD) security. NIST Special Publication (SP) 800-46 Rev. 2. National Institute of Standards and Technology, 2016, 53 p., DOI: 10.6028/NIST.SP.800-46r2
41. Chawla A. COVID-19 cyber insurance or cyber Liability: Do you have the coverage? 2020, DOI: 10.2139/ssrn.3610435.

УДК 004.056:351

Имамвердиев Ядигар Н.
Институт Информационных Технологий НАНА, Баку, Азербайджан
yadigar@iit.science.az

Анализ проблем кибербезопасности во время пандемии COVID-19

Мир в настоящее время переживает одну из самых страшных пандемий этого столетия. Поэтому значение кибербезопасности еще более возрастает, поскольку общество сталкивается с огромным увеличением кибератак во время этой пандемии. В данной статье анализируется общая картина угроз кибербезопасности во время пандемии COVID-19, рассматриваются законодательные и технологические аспекты безопасности персональных данных, освещаются и кратко описываются новые киберугрозы, возникающие в системах цифрового мониторинга пандемии. Исследуются меры по борьбе с инфодемией и роль социальных медиа в этом вопросе. Наконец, разрабатываются рекомендации для пользователей и организаций по обеспечению кибербезопасности и предложения по модернизации инфраструктуры кибербезопасности, связанные с реализацией концепции работы из дома. В статье использованы методы систематизации, обобщения, классификации и сравнительного критического анализа. Ожидается, что результаты будут очень полезны для улучшения систем кибербезопасности в организациях в контексте новых повышенных требований во время пандемии COVID-19 и постпандемии.

Ключевые слова: *COVID-19, пандемия, коронавирус, кибербезопасность, приватность, инфодемия.*

Yadigar N. Imamverdiyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
yadigar@iit.science.az

Analysis of cybersecurity problems during the COVID-19 pandemics

The world is currently experiencing one of the worst pandemics of this century. During this period, cybersecurity becomes even more important, because during a pandemic, the cyber environment is very favorable for malevolent attackers, and society is facing a huge increase in cyberattacks. This article analyzes the general picture of cybersecurity threats during the COVID-19 pandemic, discusses the legislative and technological aspects of personal data security, highlights and briefly describes the new cyber threats that arise in digital pandemic monitoring systems. Measures to combat infodemia and the role of social media in this matter are being investigated. Finally, recommendations for users and organizations to ensure cybersecurity and proposals for modernization of cybersecurity infrastructure are being developed related to implementation of the concept of work from home. The article uses the methods of systematization, generalization, classification and comparative critical analysis. The obtained results are expected to be very useful for improving the cybersecurity systems in organizations in the context of the new increased requirements during the COVID-19 pandemic and post-pandemic period.

Keywords: *COVID-19, pandemic, coronavirus, cybersecurity, privacy, infodemics.*