

Təhmasib FƏTƏLİYEV

Azərbaycan Milli Elmlər Akademiyasının
İnformasiya Texnologiyaları İnstitutu
e-mail: tfataliyev@gmail.com

Nərgiz VERDİYEVA

Azərbaycan Milli Elmlər Akademiyasının
İnformasiya Texnologiyaları İnstitutu
e-mail: nergiz_verdieva@mail.ru

VƏTƏNDAŞ ELMİNİN INDUSTRY 4.0 HƏLLƏRİ ƏSASINDA İNKİŞAFINDA İNFORMASIYA TƏHLÜKƏSİZLİYİ MƏSƏLƏLƏRİ

Xülasə: *Məqalə vətəndaş elminin Industry 4.0 həlləri əsasında inkişafında informasiya təhlükəsizliyi məsələlərinə həsr olunmuşdur. Vətəndaş elmi layihələrində təhlükəsizlik məsələləri təsnif edilərək kateqoriyalara bölünmüşdür. Onun könüllü iştirakçılarının demografik analizi məsələsi nəzərdən keçirilmiş və fərdi məlumatların təhlükəsizliyinin qorunmasını təmin edən normativ-hüquqi sənədlər təhlil olunmuşdur. Vətəndaş elmi 4.0 çərçivəsində təhlükəsizliyin təmin olunması və şəxsi məlumatların qorunması yolları təhlil edilmişdir. Aparılan tədqiqatlara əsasən bu istiqamətdə görülmüş işlər təhlil edilmiş və müvafiq təkliflər verilmişdir.*

Açar sözlər: *Industry 4.0, vətəndaş elmi, vətəndaş elmi 4.0, informasiya təhlükəsizliyi, fərdi məlumatlar.*

Müasir sivilizasiyanın mövcud elmi-texniki səviyyəsi təkamül nəticəsində baş vermiş sənaye inqilabları ilə sıx əlaqəlidir. Hazırda biz dördüncü sənaye inqilabı adlanan və Industry 5.0-a doğru inkişaf edən mərhələdə yaşayırıq. Industry 4.0 kimi tanınan dördüncü sənaye inqilabına keçid radiotezlik identifikasiyası (Radio Frequency Identification, RFID), simsiz sensor şəbəkələr, Əşyaların İnterneti (Internet of Things, IoT), Big Data, bulud hesablamaları (cloud

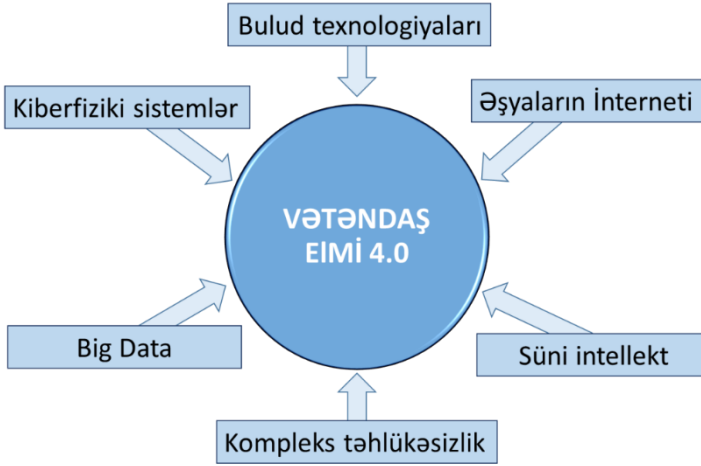
computing), süni intellekt (Artificial Intelligence, AI) kimi qabaqcıl texnologiyalar vasitəsilə mümkün olmuşdur [7].

Industry 4.0-da rəqəmsallaşma və texniki sistemlərin birləşdirilməsi fiziki və rəqəmsal dünyanın kiberfiziki sistemlər vasitəsilə (KFS) əlaqələndirilməsinə imkan yaratmışdır. Texniki sistemlər bir-biri ilə avtonom olaraq verilənlərin mübadiləsinə aparmaq və bununla da proseslərin gedişatını optimallaşdırmaq qabiliyyətinə malikdir. Bu zaman Industry 4.0-da əsas rolu sensorların yaradılması oynayır. Sensorlar ilkin ölçmə verilənlərinin mənbəyi olmaqla, həm də mərkəzləşdirilməmiş hesablama gücü və proqramlaşdırılma imkanı verir [4, 9]. Sensorlar həm də Əşyaların İnterneti texnologiyasının əsasını təşkil edir. Müasir “ağıllı” sensorlardan müxtəlif obyektlərin identifikasiyasında istifadə olunur.

Qabaqcıl Industry 4.0 həlləri vətəndaş elminin (VE) son illərdə daha sürətli inkişafını təmin etmişdir. Bu, müasir informasiya texnologiyaları (İT) sahəsində əldə olunan son nailiyyətlərlə bağlıdır. Vətəndaş elmi – əksəriyyətinin ixtisas üzrə ilkin hazırlığı olmayan çoxlu sayda həvəskar vətəndaşın elmi tədqiqatlarda iştirakı konsepsiyasıdır.

Bugünkü gündə dördüncü sənaye inqilabı akademik sahədə ən aktual trendlərdən biri hesab olunur. Industry 4.0 əvvəlki sənaye inqilablarından daha çox avtomatlaşdırılma, fiziki və rəqəmsal dünyanın KFS vasitəsilə əlaqələndirilməsi, eləcə də istehsal mərhələlərinin intellektual məhsulların köməyi ilə müəyyən olunduğu yeni sistemə keçidlə xarakterizə olunur.

İT-nin sürətli inkişafı ilə sənayedə baş verən dəyişikliklər məhsul və xidmətlərin keyfiyyətini xeyli yaxşılaşdırmağa imkan verir. Industry 4.0 texnologiyalarının bu cür üstünlüklərinin VE-də tətbiqi yeni Citizen science 4.0 (Vətəndaş elmi 4.0, VE 4.0) konsepsiyasının reallaşdırılmasını aktual edir (şəkil 1). Citizen science 4.0 konsepsiyası Industry 4.0-ın ənənəvi VE-nə proyeksiyası kimi başa düşülür.



Şəkil 1. Vətəndaş elmi 4.0-in tərkib hissələri

Industry 4.0-da fiziki obyektlər və proseslərə KFS vasitəsilə nəzarət olunur və idarə edilir. Burada birləşdirilmiş və ya fərdi idarəetmə sistemləri istifadə oluna bilər. Sensorlardan alınan verilənlər, məsələn, temperatur, təzyiq, maddənin sıxlığı və s. sistemdə nəzarət və idarəetmə məqsədilə istifadə olunur. Böyük həcmli verilənlərin toplanması və emalının artması, eləcə də idarəetmə sistemlərinin avtonomluğunun yüksək səviyyəsi və mərkəzləşdirilməmiş olması Industry 4.0-da kibertəhlükəsizliyə də təsir edən amillərdəndir. Ənənəvi olaraq kibertəhlükəsizlik insanların və təşkilatların zərərli proqram təminatı, kibercinayətkarların hücumları, veb-saytlara ziyan vurulması və s. kimi təhdidlərdən mühafizə olunmasına yönəlmişdir [6]. Son zamanlar maliyyə cinayətlərinə, bəzi hallarda hətta hökumətə və mühüm infrastrukturlara yönələn kibercinayətkarların müəkkəbləşməsi və intensivləşməsi müşahidə olunur. Industry 4.0 dövründə təşkilatlar özlərinin intellektual avadanlıqları və şəbəkələrindən daha çox asılıdır. Bu işə şəbəkələrə və avadanlıqlara daha asan giriş nöqtələri tapan kibercinayətkarlar üçün əlverişli şərait yaradır. Mühüm infrastrukturlara və strateji sənaye sektorlarına yönələn kibercinayətkarlıq xeyli artmış və müəkkəbləşmişdir. Onlar

cəmiyyətin normal yaşayışının pozulmasına gətirməklə yanaşı, həm də zərərçəkmiş ölkələrin mənəvi ruhuna ziyan vurur [12].

VE 4.0-da təhlükəsizlik problemlərini üç cür növləndirmək olar [1]:

- Texniki vasitələrin təhlükəsizliyi;
- Proqram təminatının təhlükəsizliyi;
- İnformasiya təhlükəsizliyi.

Elektron texnologiyaların zamanla təkmilləşməsi müasir cəmiyyətdə fərdi informasiyadan istifadənin riskləri haqqında həm hökumət səviyyəsində, həm də vətəndaş cəmiyyətində maariflənmənin artmasına gətirib çıxarır. Elm və texnikanın inkişafı insanların həyat səviyyəsini yaxşılaşdırmış və imkanlarını genişləndirmişdir. Bulud hesablamaları fərdi məlumatları telefon, planşet və digər texniki vasitələrdən uzaqda saxlamağa imkan verir ki, bu da istifadəçiyə istənilən məkandan və istənilən cihazdan həmin informasiyaya giriş hüququnu təmin edir. İstifadəçilərin bu informasiyaya nəzarət etmək imkanı əhəmiyyətli dərəcədə azalmışdır. Bundan əlavə, mobil internet hər yerdə informasiya toplayır, bu, xüsusilə kontaktlar, şəkillər və elektron məktublar kimi fərdiləşdirilmiş informasiyaya aiddir. Lakin bulud hesablamalarının və mobil internetin populyarlaşması informasiyanın mühafizə olunmasını cəmiyyət cəhətdən mürəkkəbləşdirirsə, böyük həcmli verilənlərin yaranması hazırda fərdi informasiyanın mühafizəsi sisteminin bünövrəsini keyfiyyət baxımından zəiflədir ki, bu məqama da xüsusi diqqət yetirmək lazımdır. Məsələn, müasir dövrdə gizli qanunauyğunluqları və cəmiyyət arasındakı əlaqələri axtarmaq üçün hər yerdə profayliq texnologiyalarından istifadə olunur. Bundan başqa, bu texnologiyalar fərdi verilənləri təkrar identifikasiya etməyə imkan verir ki, bu da anonimləşmə strategiyasının effektivliyini azaldır.

Qeyd etmək lazımdır ki, VE-nin əsas məqsədi elmin demokratikləşməsi və global problemlərin səmərəli həllidir. Onun inkişafında əsas aktorları olan könüllü iştirakçı-alimlərin demoqrafiyası mühüm rol oynayır. Onları xarakterizə edən göstəricilərə demoqrafik xüsusiyyətlər (cins, doğum tarixi və yeri, ailə vəziyyəti və s.), iqtisadi (peşəsi, iqtisadiyyatın sahəsi və iqtisadi fəaliyyət növü,

dolanışiq mənbəyi və s.), ümumi və ya peşə təhsilinin xüsusiyyətləri (təhsil səviyyəsi, təhsil müəssisəsinə davamiyyət və s.), həmçinin etnik xüsusiyyətlər (milliyyət, ana dili, danışiq dili və s.) aid oluna bilər. VE layihələrinin iştirakçılarının demoqrafiyasına nəzər salsaq, burada yaş kateqoriyası, təhsil səviyyəsi, fiziki vəziyyəti, sosiallaşma səviyyəsi və s. göstəriciləri müxtəlif olan bir çox sayda vətəndaşların iştirakını görmək olar. VE layihələri əsasında aparılan demoqrafik tədqiqatlar layihələrin müvəffəqiyyətinin iştirakçıların demoqrafik xarakteristikalarından asılılığını təsdiq edir [3]. Ona görə də bunlarla yanaşı, iştirakçıların həssas qrupunun da olmasını nəzərə alaraq, fərdi məlumatların gizliliyinin qorunması ön plana çıxarılmalıdır.

Layihələndirmə prosesində VE layihələrində iştirak edən vətəndaşların şəxsi məlumatlarının qorunması məqsədi ilə proqnozlaşdırıcı, qabaqlayıcı və aradan qaldırıcı tədbirlər nəzərə alınmalıdır [1].

Avropa Vətəndaş Elmi Assosiasiyasının (European Citizen Science Association – ECSA) təşəbbüsü ilə bəyan edilmiş “Vətəndaş elminin 10 prinsipi” içərisində vətəndaş elmi layihələrinin rəhbərlərinin müəllif hüququ, intellektual mülkiyyət, informasiya mübadiləsi haqqında razılıq, konfidensiallıq, məsuliyyət, ətraf mühitə təsirlə bağlı hüquqi və etik aspektləri nəzərə alması barədə prinsip vardır [10]. Bundan başqa, Avropada Verilənlərin Mühafizəsi üzrə Ümumi Rəqlament qanunvericiliyinin fərdi məlumatların emalı ilə əlaqədar prinsiplərə görə, fərdi məlumatlar onların subyektinə qarşı ədalətli, qanuni və şəffaf şəkildə emal edilməlidir [5].

Məlumdur ki, kibermüdafiə – sistemin infrastrukturunu və verilənlərinə edilən hücumları və təhdidləri aşkarlamaq, onların qarşısını almaq və zəiflətməyə yönəlmiş kompüter mühafizəsi mexanizmidir. VE 4.0-da istifadə olunan İndustry 4.0 alətləri kibermüdafiə məqsədilə geniş istifadə edilə bilər. Giriş verilənləri ardıcılığını emal edə bilən neyron şəbəkələr maşın təlimi ilə birlikdə istifadəçilərin şübhəli fəaliyyətini və kibertəhdidləri aşkar etmək məqsədilə təlim texnologiyalarının yaradılması üçün istifadə oluna bilər. Mürəkkəb alqoritmlərdən istifadə etməklə Sİ texnologiyaları vasitəsi ilə zərərli proqram təminatlarını aşkarlamaq,

obrazların tanınmasını işə salmaq və hətta zərərli proqram vasitələri sistemə daxil olmamışdan əvvəl onların ilkin əlamətlərini müəyyən etmək olar.

Bulud hesablamalarının çoxsaylı üstünlükləri sayəsində onlar VE layihələrində verilənlərin saxlanması və hostinqi üçün populyar texnologiyaya çevrilmişdir. Bununla belə, buludda şəffaflığın olmaması və birgə istifadə olunan verilənlərə tətbiq edilən əməliyyatlar üzərində nəzarətin itirilməsi nəticəsində bulud texnologiyalarının tətbiqi qeyri-müəyyənlik və risklər yaradır. Buludda verilənlərin saxlanması və birgə istifadəsi zamanı əsas tələb ümumi verilənlərin tamlığının qorunub saxlanmasıdır [2]. [11]-də müəlliflər bulud mühitində verilənlərin qrup şəklində dinamik mübadiləsi üçün yoxlama sxemi təklif etmişlər. Onlar istifadəçilərin üzvlüyü və şəxsiyyətinin izlənməsi üçün hüquqların paylaşılması mərkəzini (Rights Distribution Center, RDC) təqdim etmişlər. Bu yanaşma istifadəçinin şəxsiyyətinin konfidensiallığını qorumaqla yanaşı, verilənlərin tamlığının yoxlanılması üçün üçüncü tərəf yoxlamaları aparmağa imkan verir.

Dövrün ən qabaqcıl Industry 4.0 həllərindən biri hesab olunan Sİ vasitəsilə kibercinayətlərin qarşısını almaq mümkündür. Lakin Sİ-dən istifadə etməklə həm də kibercinayətkarlar boşluqları daha tez aşkarlaya bilər. Sİ insanın müəyyən edə bilmədiyi boşluqları aşkar etməyə imkan verir, çünki botlar çox kiçik dəyişiklikləri qeyd etmək üçün əvvəlki kiberhücumların verilənlərindən istifadə edə bilər.

İnformasiya texnologiyalarının inkişafı verilənlərin toplanması prosesini optimallaşdırmaqla, onların idarə edilməsi prosesini təkmilləşdirməklə, keyfiyyətə nəzarəti avtomatlaşdırmaqla və kommunikasiyanı sürətləndirməklə elmi tədqiqat prosesinə öz müsbət təsirini göstərir [8]. Bundan başqa, yeni texnologiyalar və bacarıqlar (məsələn, mobil tətbiqlər, sensor şəbəkələri, oyunlar) VE 4.0 iştirakçılarının əksəriyyəti üçün əlverişli olacaq, lakin onları qəbul etmək istəməyənləri bu sahədən kənarda qoymuş olacaq. Təşkilatlar şəbəkəsi (lokal, regional və global) və peşəkar assosiasiyalar, eləcə də açıq resenziyalı jurnallar və kiber-infrastruktura dəstək sistemləri genişlənməkdə olan VE cəmiyyətini

formalaşdırmağa və bu sahədə gələcək istiqamətləri müəyyən etməyə kömək edəcək.

Nəticə

Aparılmış araşdırmalar göstərir ki, İKT-nin inkişafı Industry 4.0 həllərinin müxtəlif sahələrdə geniş tətbiqinə yol açır. Bu sahələrdən biri kimi məqalədə Industry 4.0 alətlərinin VE-də tətbiqi nəzərdən keçirilmişdir. Industry 4.0 həllərinin VE-də tətbiqi nəticəsində formalaşan VE 4.0 konsepsiyasının tərkib hissəsi olaraq təhlükəsizlik məsələlərinə baxılmışdır. Eyni zamanda Industry 4.0 həllərinin VE-də iştirak edən könüllülərin fərdi məlumatlarının qorunması üçün tətbiq imkanları nəzərdən keçirilmişdir. Qabaqcıl Industry 4.0 həllərinin köməyi ilə gələcəkdə VE-də təhlükəsizlik baxımından daha böyük nailiyyətlər əldə etmək mümkündür. Bu texnologiyalar inkişaf etdirilərək verilənlərin toplanmasının optimallaşdırılması, onların idarə olunmasının təkmilləşdirilməsi, eyni zamanda mövcud təhlükəsizlik tədbirlərindəki boşluqların aşkar edilməsi və aradan qaldırılması üçün mühüm rol oynayan alətə çevriləcək.

Ədəbiyyat

- [1] Verdiyeva N. "Vətəndaş elmi layihələrində fərdi məlumatların təhlükəsizliyinin təmini məsələləri", "İnformasiya təhlükəsizliyinin aktual multidissiplinar elmi-praktiki problemləri" V respublika konfransı, s. 142-145.
- [2] Angin P., Bhargava B., Ranchal R., Big Data Analytics for Cyber Security. Hindawi, Security and Communication Networks, v. 2019, 2 p.
- [3] Blake, C., et al., The Demographics of Citizen Science Participation and Its Implications for Data Quality and Environmental Justice. Citizen Science: Theory and Practice, 2020, 5(1): 21, pp. 1–10.
- [4] Fataliyev T. Kh., Mehdiyev Sh. A., "Analysis and new approaches to the solution of problems of operation of oil and gas complex as cyberphysical system", International Journal of Information Technology and Computer Science (IJITCS), 2018, Vol. 10, No. 11, pp. 67-76.
- [5] GDPR, <https://gdpr-info.eu/art-5-gdpr/>

- [6] Jang-Jaccard J., Nepal S., “A survey of emerging threats in cybersecurity”, *Journal of Computer and System Sciences*, Vol. 80, Issue 5, pp. 973-993, 2014.
- [7] Lu Y., “Industry 4.0: A survey on technologies, applications and open research issues”, *Journal of Industrial Information Integration*, 2017, No. 6, pp. 1–10.
- [8] Newman G. Et al., *The future of Citizen science: Emerging technologies and and shifting paradigms*, *Frontiers in Ecology and the Environment*, 2012.
- [9] Schütze A., Helwig N., Schneider T., “Sensors 4.0 – smart sensors and measurement technology enable Industry 4.0”, *Journal of Sensors and Sensors Systems*, 2018, No. 7, pp. 359-371.
- [10] Ten principles of citizen science, <https://ecsa.citizen-science.net/engageus/10-principles-citizen-science>
- [11] Yan Y.X., et al., *Integrity Audit of Shared Cloud Data with Identity Tracking*, *Hindawi, Security and Communication Networks*, v. 2019, 11 p.
- [12] Фаталиев Т., Мехтиев Ш., “Вопросы обеспечения энергетической безопасности инфраструктуры электронной науки”, 4-я Республиканская конференция по информационной безопасности, сс. 105-108, 2018.

Аннотация: *Статья посвящена проблемам информационной безопасности в развитии гражданской науки на основе решений Industry 4.0. Проблемы безопасности в проектах гражданской науки классифицируются по категориям. Рассмотрен вопрос демографического анализа его участников-волонтеров и проанализированы нормативно-правовые документы, обеспечивающие защиту безопасности персональных данных. Проанализированы способы обеспечения безопасности и защиты персональных данных в рамках гражданской науки 4.0. На основе результатов исследования проанализирована проделанная в этом направлении работа и выдвинуты соответствующие предложения.*

Ключевые слова: *Industry 4.0, гражданская наука, гражданская наука 4.0, информационная безопасность, персональные данные.*

Abstract: *The article is dedicated to the problems of information security in the development of citizen science on the basis of Industry 4.0*

solutions. The security issues in citizen science projects are classified by dividing into categories. The issue of demographic analysis of its volunteer participants is considered and normative-legal documents ensuring protection of personal data security are analyzed. Ways to ensure security and protection of personal data within the framework of citizen science 4.0 are analyzed. Based on the research carried out, the works done in this direction are analyzed and relevant suggestions are made.

Keywords: *Industry 4.0, citizen science, citizen science 4.0, information security, personal information.*