AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ
SUMQAYIT DÖVLƏT UNİVERSİTETİ

МИНИСТЕРСТВО ОБРАЗОВАНИЯ АЗЕРБАЙДЖАНСКОЙ РЕСПУБЛИКИ
СУМГАИТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

MINISTRY OF EDUCATION OF AZERBAIJAN REPUBLIC
SUMGAYIT STATE UNIVERSITY

KONFRANS
MATERİALLARI

МАТЕРИАЛЫ КОНФЕРЕНЦИЙ
CONFERENCE PROCEEDINGS

SUMQAYIT – 2020

COVID-19 PANDEMİYASI VƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ MƏSƏLƏLƏRİ

İmamverdiyev Y.N., Şıxəliyev R.H.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı şəh., Azərbaycan
yadigar@iit.science.az, ramiz@science.az

Giriş. 2019-cu ilin dekabrında Çinin Hubei əyalətinin Wuhan şəhərində aşkarlanmış naməlum təbiətli sətəlcəm tezliklə bütün dünyada indiyədək görünməmiş müqyasda yayıldı. (Wuhan 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 yayıldı, qlobal böhrana çevrildi və ÜST 11 mart 2020-ci ildə bu xəstəliyi pandemiya elan etdi [1].

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. 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.

Məqalədə COVID-19 pandemiyası dövründə informasiya təhlükəsizliyi 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 [2]. Onları nüvəsi və səthdəki çıxıntıları ilə sferik virionlar şəklindəki formasına görə günəş tacına oxşadıqları üçün koronavirus adlandırmışdılar (latınca Corona – tac deməkdir). Koronaviruslar ailəsi xeyli genişdir, 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 [3].

COVID-19 ilə Şiddətli Kəskin Tənəffüs Sindromu (Severe Acute Respiratory Syndrome, SARS) və Yaxın Şərq Tənəffüs Sindromu (Middle East Respiratory Syndrome, 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 [3].

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) [3]. 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 kibertəhdidlər. Bədniyyətlilərin kiberhücum motivləri, hədəfləri senariləri və alətləri olduqca rəngarəngdir. COVID-19 ilə əlaqəli sosial mühəndislik və ransomware hücumlarına daha çox cəhd edilir [4]. Sosial mühəndislik metodlarından daha çox phishing istifadə edilir, onu təkcə veb üzərindən təşkil etmirlər, 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 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.

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 [4].

Son aylarda COVID-19 ilə əlaqəli saxta URL-ünvanların alınmasında böyük artım müşahidə edilir [4]. 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.

COVID-19 və fərdi məlumatların təhlükəsizliyi. Məlumdur ki, COVID-19 pandemiyası ölkələrin e-dövlət infrastrukturunun yükünü artırmışdır, yəni yeni onlayn e-dövlət xidmətlərinin yaranmasına səbəb olmuş və mövcud e-xidmətlərə tələbləri artırmışdır. Pandemiya dövründə bu xidmətlərə müraciətlərin sayı həddindən çoxdur və qeydiyyat zamanı vətəndaşlar rəqəmsal imza, asan imza və ya şəxsiyyət vəsiqəsinin

FİN kodundan istifadə edirlər. Bu şəraitdə şəxsi həyatın toxunulmazlığı (Privacy), fərdi məlumatların təhlükəsizliyi məsələlərinin həlli daha da aktuallaşır və fişinq, dələduzluq və digər kiberhücumların başvermə ehtimalı artır.

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) [5]. Qeyd edək ki, Avropa Verilənlərin Mühafizəsi Şurası COVID-19 epidemiyası kontekstində fərdi məlumatların emalı üzrə bəyanat yaymışdır [6].

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

ÜST-ə görə, infodemiya – səhiyyə sahəsində fövqəladə vəziyyət zamanı problem haqqında böyük həcmdə yalan, saxta informasiya, dezinformasiya və şaiyələrin 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 şaiyələrin qarşısını almağa çalışır. Məlumatlara görə, bu şirkətlər əsaslandırılmamış tibbi məsləhətlərin, yalan məlumatların və əhalinin sağlamlığına risk təşkil edən digər yalan informasiyanın qarşısını fəal şəkildə alırlar [7].

Evdən iş zamanı bəzi kibertəhlükəsizlik məsləhətləri. COVID-19 pandemiyası qlobal miqyasda çox sayda işçinin uzaqdan işləmək məcburiyyətində qalmasına səbəb olmuşdur. Evdən işləyən işçilər normal şəraitdə malik olduqları ilə müqayisədə minimal kiber təhlükəsizlik resurslarına malikdirlər [8]. Təşkilatlar və evdən işləyən insanlar aşağıdakı kibertəhlükəsizlik məsləhətlərinə əməl etməlidirlər:

- Təşkilatlar öz informasiya təhlükəsizliyi siyasətlərini yeniləməli və evdən, məsafədən işi nəzərə almalıdırlar.
- Təşkilatlar əməkdaşlarının istifadə etdikləri istənilən qoşulma nöqtəsinin tam təhlükəsiz olduğunu təmin etməlidirlər.
  - Əgər informasiya sızması fərdi qurğulardan baş verərsə belə, təşkilatlar məsuliyyət daşıyacaq.
  - Zəruri təhlükəsizlik olmadan təşkilat şəbəkəsinə giriş üçün istifadə edilən fərdi qurğular təşkilatı hakinq üçün həssas vəziyyətə gətirə bilər.
- Əməkdaş rəsmi məsələlərlə bağlı öz həmkarları ilə təşkilatın təqdim etdiyi IT-avadanlıqla ünsiyyətdə olmalıdır.
- Evdən işləyən istifadəçilər gizlilik və kibertəhlükəsizlik təhdidləri barədə maarifləndirilməli və təlimatlandırılmalıdırlar.
- Evdən işləyən insanlar koronavirus qorxusundan istifadə edən fişinq hücumlarından məlumatlı və bilikli olmalıdırlar.
- Evdən işləyən insanlar fişinq dələduzluqlarını və kiberhücumların digər növlərini necə aşkarlamağı və onlara necə reaksiya verməyi bilməlidirlər.
- Harada mümkündürsə, çoxfaktorlu autentifikasiyadan istifadə edilməlidir.
- İşçinin təşkilat daxilində informasiya resurslarına təhlükəsiz giriş əldə etməsinə imkan verən VPN-həllərin istifadəsinə cəhd edilməlidir.
- Videokonfrans və digər oxşar əməkdaşlıq alətlərinə yüksək tələbat səbəbindən bu alətlərdə hakerlərin istismarı üçün bir çox boşluqlar üzə çıxa bilər.

Pandemiya və e-dövlətin informasiya təhlükəsizliyi məsələləri. COVID-19 pandemiyası dünya ölkələri qarşısında yeni çağırışlar və problemlər yaratmışdır və bununla yanaşı, pandemiyaya qarşı mübarizədə dövlətin rolunun çox vacib olduğunu bir daha göstərmişdir. COVID-19 pandemiyası ölkələrin tibbi, iqtisadi və s. infrastrukturları ilə yanaşı, e-dövlət infrastrukturuna da problemlər yaradır. COVID-19 pandemiyası şəraitində e-dövlət infrastrukturunun əsas problemlərindən biri və ən vacibi informasiya təhlükəsizliyi məsələlərinin həllidir.

COVID-19 pandemiyası dövründə dövlət sektorunda kibertəhlükələrin baş verməsi ehtimalı daha da artır, çünki dövlət təşkilatlarının əməkdaşlarının fiziki olaraq öz iş yerlərindən kənarda (İnternet vasitəsilə, məsafədən) işləməsi insan faktorunu daha da qabardır və sosial mühəndislik hücumlarının artmasina gətirib çıxara bilər. Həmçinin, İnternet vasitəsi ilə ötürülən informasiyanın oğurlanmasının və ya itirilməsinin qarşısını almaq çətinləşir. Buna görə də, mövcud İT-infrastrukturun təhlükəsizliyi daim yüksək səviyyədə təmin edilməlidir. Lakin, e-dövlət xidmətlərinin təhlükəsizlik səviyyəsinin həddindən çox artırılması, vətəndaşlara bu və ya digər xidmətlərin əldə edilməsinə çətinliklər yarada bilər. Buna görə kompomis bir

variantın seçilməsi daha məqsədəuyğun olardı.

COVID-19 pandemiyası şəraitində e-dövlətin informasiya təhlükəsizliyinin təmin edilməsi üçün proaktiv strategiya – prioritetləri və boşluqları müəyyən etməyə imkan verən kompleks proqram işlənilməlidir. Dövlət təşkilatlarının əməkdaşları məsafədən işlədiyi üçün həmin mühitlərdə də monitorinq aparılması çox vacibdir. Dövlət təşkilatlarının informasiya sistemləri ilə qarşılıqlı əlaqədə olan hər bir informasiya sisteminin təhlükəsizliyinin monitorinqi və qiymətləndirilməsi çox vacibdir, çünki əmin olmaq lazımdır ki, onlar bir-birinə əlavə risklər (sertifikatsız sistemlərin istifadəsi, mühafizəsiz giriş nöqtələrinin və boşluqların olması və s.) yaratmırlar.

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 kampaniyaların da sayı artır.

Kompüter virusları da bioloji viruslar kimi çox asan və sürətli yayıla bilir. Virus ola biləcək əşyalara və səthlərə toxunmaqdan çəkindiyiniz kimi, tanımadığınız şəxslərdən gələn məktubları və etibar etmədiyiniz veb-saytları açmaqdan da çəkinməlisiniz. Əllərinizdən mikrobları təmizləmək üçün dezinfeksiyaedici vasitələrdən istifadə etdiyiniz kimi, öz kompüterinizi və şəbəkənizi də viruslardan təmizləmək üçün effektiv vasitələrdən istifadə etməlisiniz.

Ədəbiyyat

6. The World Health Organization (WHO). Coronavirus disease (COVID-2019) situation reports. URL: https://www.who.int/emergencies/diseases/novel-coronavirus-2019/situation-reports/
7. 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.
8. Velavan T. P., Meyer C. G. The COVID-19 epidemic // Tropical medicine & international health, 2020, vol. 25(3), pp. 278-280.
9. Fontanilla M. V. Cybercrime pandemic // Eubios Journal of Asian and International Bioethics, 2020, vol. 30(4), pp. 161-165.
10. Daubenschuetz T., Kulyk O., Neumann S., Hinterleitner I., et al. SARS-CoV-2, a Threat to Privacy? 2020. arxiv preprint arxiv:2004.10305.
11. EU: Statement on the processing of personal data in the context of the COVID-19 outbreak. 2020. URL: https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en
12. 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(2), pp. 133-148.
13. Ahmad T. Corona virus (COVID-19) pandemic and work from home: Challenges of cybercrimes and cybersecurity. 2020. DOI: 10.2139/ssrn.3568830.

ГРАФО-АНАЛИТИЧЕСКИЙ МЕТОД ОПРЕДЕЛЕНИЯ НЕОБХОДИМОГО ОБЬЕМА СПЕКТРАЛЬНЫХ ИЗМЕРЕНИЙ ДЛЯ ИССЛЕДОВАНИЯ СОСТОЯНИЯ ПОЧВЫ В ЗОНАХ ТРАНСПОРТИРОВКИ УГЛЕВОДОРОДОВ

Насиров Х.М.

Национальное аэрокосмическое агентство. г.Баку, Азербайджан

nasirovhabib@mail.ru

Резюме. Составлена и решена оптимизационная задача, определяющая условия достижения экстремального теплового воздействия сжигания газа на окружающую среду. Определено, что при выборе среди группы возможных функциональных зависимостей удовлетворяющих определенному условию, масштабированной и смещенной по горизонтальной оси корневой зависимости второй степени содержания углерода в саже от содержания углерода в попутном газе, может быть выделено минимальное тепло с факелов сжигания газа.

Для оценки площади разлившихся углеводородных продуктов, таких как дизель, бензин, реактивное топливо, и т.д. необходимо иметь точные оценки скорости разлива, скорость проникновения в почву и время достиженя углеводородами уровня грунтовых вод. Разработанный нами метод частично базируется на известной модели распространения углеводородов. Согласно