İnternet İstifadəçiləri üçün Kibertəhlükəsizlik Riskləri

Məhəmmədəli Babayev
Azərbaycan Dövlət Neft və Sənaye Universiteti, Bakı, Azərbaycan
mhmmdlibabayev42@gmail.com

***Xülasə*— İnternet müasir dövrdə insanların gündəlik həyatının ayrılmaz hissəsinə çevrilmişdir. Sosial şəbəkələr, elektron poçt, bulud xidmətləri və onlayn platformalardan geniş istifadə olunur. Lakin bu imkanlarla yanaşı, kibertəhlükəsizlik riskləri də artır. Parol idarəetməsində zəiflik, ictimai Wi-Fi şəbəkələrindən istifadə, sosial mühəndislik hücumları və məlumatların qorunmaması istifadəçilər üçün ciddi təhlükələr yaradır. Bu məqalədə gündəlik internet istifadəsində rast gəlinən əsas kibertəhlükəsizlik riskləri araşdırılır, beynəlxalq təcrübə ilə müqayisə aparılır və Azərbaycan istifadəçiləri üçün praktik təkliflər irəli sürülür.**

Açar sözlər— ***kibertəhlükəsizlik; internet istifadəsi; parol idarəetməsi; sosial şəbəkələr; bulud xidmətləri.***

I. GİRİŞ

İnformasiya və kommunikasiya texnologiyalarının sürətli inkişafı interneti müasir cəmiyyətin əsas ünsiyyət və məlumat mübadiləsi vasitələrindən birinə çevirmişdir. Sosial şəbəkələr, elektron poçt, bulud xidmətləri və onlayn platformalar insanların informasiya mühitini formalaşdırır. Elektron bankçılıq, dövlət xidmətlərinin rəqəmsallaşdırılması, elektron ticarət və bulud texnologiyalarının geniş tətbiqi yeni imkanlar yaratmaqla yanaşı, yeni risklərin də meydana çıxmasına səbəb olur.

Beynəlxalq Telekommunikasiya İttifaqının (ITU) Global Cybersecurity Index 2024 hesabatında rəqəmsal texnologiyaların və bağlantının genişlənməsi fonunda kibertəhlükəsizliyin əhəmiyyətinin artdığı, ölkələrin kibertəhlükəsizlik üzrə hüquqi, texniki, təşkilati, potensialın inkişafı və əməkdaşlıq istiqamətlərində tədbirlər gördüyü vurğulanır [1].

Avropa İttifaqının Kibertəhlükəsizlik Agentliyi (ENISA) istifadəçilərə eyni paroldan bir neçə hesabda istifadə etməməyi tövsiyə edir. Çünki bir hesab üçün istifadə olunan parolun ələ keçirilməsi digər hesabların da təhlükə altına düşməsinə səbəb ola bilər [2].

Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyasında ölkənin informasiya məkanının müasir təhdidlərdən qorunması, informasiya təhlükəsizliyi sahəsində normativ hüquqi bazanın təkmilləşdirilməsi və kibertəhlükəsizliyin gücləndirilməsi ilə bağlı istiqamətlər müəyyən edilmişdir [3].

II. TƏHLİL VƏ MÜŞAHİDƏLƏR

2.1. Kibertəhlükəsizlik anlayışları və müasir təhdidlər

Kibertəhlükəsizliyin təmin olunması, xüsusilə korporativ və dövlət sektoru üçün böyük əhəmiyyət daşıyır. Çünki kiber təhdidlər mühüm məlumatların oğurlanması, sistemlərin kilidlənməsi və ya sıradan çıxarılması, müştəri məlumatlarının ələ keçirilməsi kimi ciddi nəticələrə səbəb ola bilər. Buna görə də kibertəhlükəsizliyin təmin edilməsi və kiber təhdidlərlə mübarizə getdikcə daha vacib xarakter almışdır.

Texnologiyanın inkişafı ilə müharibələr quru, hava, dəniz və kosmos sahələrindən sonra internetin yaranması nəticəsində yeni bir mübarizə sahəsi olan kiber məkanın formalaşmasına gətirib çıxarmışdır. Bu məkanın təhlükəsizliyi informasiya üzərində qurulduğundan, əslində kibertəhlükəsizlik bir növ informasiya təhlükəsizliyi kimi izah edilir. Məlumatın qorunması əsas şərt olaraq qalır: əgər ona sahib olmayan şəxslər tərəfindən çıxış əldə edilirsə, bu zaman təhlükəsizlik boşluğu yaranır. Kiber təhdidlər artdıqca kibertəhlükəsizlik boşluqları da müxtəlifləşir.

"Kiber cinayət", "kiber təhdid", "kiber hücum", "kiber təhlükəsizlik" kimi anlayışlar bir-biri ilə sıx bağlıdır və biri digəri olmadan tam şəkildə izah edilə bilməz. Son dövrlərdə bir çox beynəlxalq aktorlar informasiya təhlükəsizliyini təmin etmək üçün mübarizə aparırlar. Lakin kibercinayətkarları/hakerləri müəyyənləşdirmək və cəzalandırmaq çətin olduğundan, təhlükəsizliyin təmin edilməsi daha da vacib xarakter alır.

Texnologiyanın inkişafı ilə kiber cinayətlər yalnız informasiya oğurluğu ilə məhdudlaşmır. Artıq sosial media fırıldaqları, kimlik oğurluğu, kiber zorbalıq və digər oxşar əməllər də bu kateqoriyaya daxil edilmişdir. Bu isə göstərir ki, kibertəhlükəsizlik yalnız texniki məsələ deyil, həm də sosial və hüquqi müstəvidə geniş miqyaslı problem olaraq qalır [4].

2.2. Parol idarəetməsi

Sadə və təkrar istifadə olunan parollar hesabların ələ keçirilməsi riskini artırır. ENISA-nın 2023-cü il hesabatında göstərilir ki, Avropa İttifaqında istifadəçilərin 60%-i eyni parolu bir neçə hesabda tətbiq edir [2]. Bu, hesab oğurluqlarının əsas səbəblərindən biridir. Mənbələrdə qeyd olunur ki, fişinq hücumları çox vaxt zəif parol idarəetməsindən faydalanır və istifadəçilərin hesablarına sızmaq üçün ən geniş yayılmış üsullardan biridir. Tədqiqatçı Arslan bu məsələni Türkiyə modeli üzərində tətbiq edərək, vurğulayır ki, "Türkiyədə güclü kimlik doğrulama sistemlərinin yayılması milli təhlükəsizlik baxımından zəruridir" [5]. Bu yanaşma Azərbaycanda da parol təhlükəsizliyinin gücləndirilməsi üçün aktualdır.

2.3. İctimai Wi-Fi şəbəkələri

İctimai Wi-Fi rahatlıq təmin etsə də, məlumatların oğurlanması üçün risk yaradır. ITU-nun (*International Telecommunication Union* (Beynəlxalq Telekommunikasiya

DOI: 10.25045/forensic.gov.2026.93

İttifaqı)) 2024-cü il hesabatında ictimai Wi-Fi istifadəçilərinin, xüsusilə mobil bank əməliyyatları zamanı ciddi təhlükələrə məruz qaldığı vurğulanır [1]. Ümumiyyətlə, çox qatlı qoruma, müdafiə üsulları tətbiq edilmədikdə, ictimai şəbəkələr kiber hücumlara açıq vəziyyətə gəlir [4]. Bu, Azərbaycanda da ictimai yerlərdə Wi-Fi istifadəsi zamanı VPN və şifrələmə texnologiyalarının tətbiqinin vacibliyini göstərir.

2.4. Sosial mühəndislik və sosial şəbəkələr

Gənclər arasında ünvan, telefon nömrəsi və gündəlik fəaliyyətlərin paylaşılması geniş yayılıb. Dünya Bankının 2024-cü il hesabatına görə, bu vərdişlər sosial mühəndislik hücumlarını daha effektiv edir [6]. F. Aslay sosial mühəndisliyi "insanların zəifliklərindən istifadə edərək sistemə sızma" kimi təsvir edir. Arslan isə sosial mühəndislik hücumlarının qarşısını almaq üçün maarifləndirmə kampaniyalarının vacibliyini vurğulayır və qeyd edir ki, "Türkiyədə fərdlərin məlumatlandırılması kiber təhlükəsizliyin ən mühüm addımlarından biridir" [4]. Bu, Azərbaycanda da gənclərin sosial şəbəkələrdə məlumat paylaşımını məhdudlaşdırmaq üçün maarifləndirmə tədbirlərinin gücləndirilməsini zəruri edir.

2.5. Bulud xidmətləri

Bulud xidmətləri rahatlıq təmin etsə də, şifrələnmə və təhlükəsizlik tədbirləri yetərli olmadıqda risk yaradır. Arslan öz tədqiqat işində bu məsələyə toxunaraq, dövlət qurumlarının bulud xidmətlərindən istifadəsində milli serverlərin üstün tutulmasını tövsiyə edir. O, qeyd edir ki, "Kritik məlumatların ölkə daxilindəki serverlərdə saxlanması milli təhlükəsizlik baxımından zəruridir" [5]. Bu yanaşma Azərbaycanın da bulud xidmətlərində milli təhlükəsizlik standartlarını gücləndirməsi üçün aktualdır.

2.6. Süni intellekt (Sİ) əsaslı xidmətlərin mənfi və müsbət xüsusiyyətləri

Son illərdə Sİ texnologiyalarının geniş yayılması gündəlik internet istifadəsinə yeni imkanlar gətirmişdir. ChatGPT, Copilot, Gmail-in avtomatik cavab sistemləri və digər SI əsaslı platformalar insanların gündəlik ünsiyyətini, işini və təhsilini asanlaşdırır. Bu texnologiyalar istifadəçilərə məlumatı daha tez əldə etmək, yazışmaları sürətləndirmək və məhsuldarlığı artırmaq imkanı verir.

Lakin bu xidmətlərin kütləvi yayılması ilə yanaşı, yeni kibertəhlükəsizlik riskləri də ortaya çıxır. Furkan Arslanın araşdırmasında qeyd olunur ki, "Yeni texnologiyaların sürətli yayılması fərdlərin şəxsi məlumatlarını qoruma baxımından daha diqqətli olmasını zəruri edir" [5]. Sİ əsaslı platformalarda istifadəçilər çox vaxt dostla danışırmış kimi yazışır, şəxsi məlumatlarını paylaşır və bunun nəticəsində məlumatların üçüncü şəxsə ötürülmə riskini də artırmış olur.

F.Aslay isə vurğulayır ki, sosial mühəndislik hücumları yalnız texniki boşluqlardan deyil, insanların psixoloji davranışlarından da qaynaqlanır [4]. Sİ ilə ünsiyyət zamanı istifadəçilərin şəxsi məlumatlarını rahatlıqla paylaşması bu hücumların effektivliyini artırır [4, 6].

Müsbət tərəfdən, Sİ əsaslı sistemlər kibertəhlükəsizlikdə də istifadə olunur. Məsələn, Google və Facebook Sİ-dən istifadə edərək fişinq hücumlarını daha tez aşkar edir, şübhəli davranışları avtomatik izləyir və istifadəçilərə xəbərdarlıq göndərir. Bu, Sİ-nin həm risk, həm də yeni imkanlar yaratdığını göstərir.

Deməli, nəticə olaraq Sİ əsaslı xidmətlərin mənfi və müsbət cəhətlərini belə qruplaşdırmaq mümkündür.

Müsbət tərəfləri:

- İnsanlar məlumatı daha tez əldə edir, yazışmaları sürətləndirir və işdə məhsuldarlıq artır. Təhsil və araşdırma sahəsində tələbələr və alimlər üçün böyük dəstəkdir. Böyük şirkətlər Sİ-ni kibertəhlükəsizlikdə də istifadə edərək fişinq hücumlarını daha tez aşkar edir və istifadəçiləri xəbərdar edir.
- Müsbət cəhətlərindən biri də, əlçatanlıq və inklüzivliyin olmasıdır. Belə ki, Sİ xidmətləri görmə, eşitmə və digər məhdudiyyətləri olan insanlar üçün xüsusi dəstək yaradır (məsələn, avtomatik oxuma, səsli cavablar).
- Dil baryerlərinin aradan qaldırılması: ChatGPT və oxşar sistemlər çoxdilli dəstək göstərərək fərqli dillərdə ünsiyyəti asanlaşdırır. Bu, beynəlxalq əməkdaşlıq və təhsil üçün böyük üstünlükdür.
- Sürətli qərarvermə də onun ən müsbət keyfiyyətlərindəndir. Sİ böyük məlumat bazalarını analiz edərək daha tez nəticə çıxarır. Bu, biznes və dövlət idarəçiliyində qərarların sürətləndirilməsinə kömək edir.
- Müsbət cəhətlərindən biri də innovasiya və yaradıcılıq məsələsidir. Sİ yeni ideyaların formalaşmasına, mətnlərin, dizaynların və layihələrin hazırlanmasına yeni ideyalar verə bilir.
- Kibertəhlükəsizlikdə proaktiv müdafiə: Böyük şirkətlər Sİ-ni istifadə edərək hücumları əvvəlcədən aşkar edir, riskləri proqnozlaşdırır və müdafiə mexanizmlərini gücləndirir.
- İqtisadi səmərəlilik: Müəssisələr Sİ-lə iş proseslərini avtomatlaşdıraraq xərcləri azaldır və məhsuldarlığı artırır.
- Ən başlıcası, sürətli məlumat əldə etmə, qərarvermə və s. baxımından vaxta qənaət edir. Bu platformalar saniyələr içində geniş məlumat bazasına çıxış verərək, uzun axtarış prosesini qısaldır.

Mənfi tərəfləri:

- Şəxsi məlumatların paylaşılması riski: İnsanlar ChatGPT, Copilot və oxşar platformalarla dostla danışırmış kimi rahat ünsiyyət qurur, şəxsi məlumatlarını açıqlayır. Bu isə sosial mühəndislik hücumlarının effektivliyini artırır. Məlumatların üçüncü şəxslərə ötürülməsi ehtimalı: Sİ xidmətləri çox vaxt bulud əsaslıdır. İstifadəçilərin yazışmaları və məlumatları serverlərdə saxlanılır, bu da məlumatların sızması riskini yaradır [6].
- Asılılıq və həddindən artıq istifadə: İstifadəçilər gündəlik işlərini Sİ-yə həvalə etdikcə öz analitik və yaradıcılıq bacarıqlarını daha az istifadə etməyə başlayır. Bu, uzunmüddətli perspektivdə düşünmə vərdişlərini zəiflədə bilər.

- Dezinformasiya riski: Sİ sistemləri bəzən yanlış və ya qeyri-dəqiq məlumat təqdim edə bilər. İstifadəçi bu məlumatı yoxlamadan qəbul etdikdə yanlış qərarlar verə bilər.
- Etik və hüquqi problemlər: Tədqiqat işində də vurğulandığı kimi, "yeni texnologiyaların sürətli yayılması hüquqi tənzimləmələrin də sürətlə yenilənməsini tələb edir" [4]. Əks halda, şəxsi məlumatların qorunması və istifadə qaydaları ilə bağlı boşluqlar yaranır.
- Psixoloji manipulyasiya riski və məxfilik: İnsan Sİ ilə yazışanda özünü dostla söhbət edirmiş kimi hiss edir. Bu rahatlıq ona şəxsi məlumatlarını paylaşmağı daha asan edir. Çünki qarşısındakı "sistem" ona neytral, təhlükəsiz və anlayışlı görünür. Bu etibar hissi insanı daha açıq danışmağa, bəzən də ehtiyat etmədən özəl məlumatlarını, planlarını və s. bölüşməyə sövq edir. Məsələ bundadır ki, Sİ-nin cavabları emosional və empatiya dolu görünə bilər. İstifadəçi bu üsluba inanaraq özünü daha rahat ifadə edir. Amma əslində bu yazışmalar arxada alqoritmlər və serverlər tərəfindən işlənir. Yəni, insanın psixoloji olaraq "təhlükəsiz mühit" kimi qəbul etdiyi bu ünsiyyət, əslində, məlumatların toplanması və yönləndirilməsi üçün fürsət yarada bilər [4, 6].

Gördüyümüz kimi, Sİ əsaslı xidmətlər gündəlik internet istifadəsində həm böyük üstünlüklər (məlumatın tez əldə olunması, vaxta qənaət, məhsuldarlığın artması və s.), həm də ciddi risklər (şəxsi məlumatların açıqlanması, psixoloji manipulyasiya, hüquqi boşluqlar) yaradır. Ona görə də bu texnologiyalardan istifadə edərkən həm imkanları dəyərləndirmək, həm də təhlükələri nəzərə almaq vacibdir.

III. TƏHLİL NƏTİCƏLƏRİ VƏ MÜZAKİRƏLƏR

Gündəlik internet istifadəsi ilə bağlı aparılan təhlillər göstərir ki, həm ənənəvi risklər (parol idarəetməsi, ictimai Wi-Fi, sosial mühəndislik, bulud xidmətləri), həm də müasir texnologiyalar (süni intellekt əsaslı platformalar) insanların məlumat təhlükəsizliyinə birbaşa təsir göstərir.

Müzakirə nəticələri:

- İnkişaf edən texnologiyalar istifadəçilərə sürət, rahatlıq və məhsuldarlıq qazandırır, lakin eyni zamanda yeni təhlükələr yaradır.
- Parol idarəetməsində zəifliklər, ictimai şəbəkələrin açıq olması və sosial mühəndislik hücumları hələ də əsas risklər olaraq qalır [2, 4, 6].
- Süni intellekt xidmətləri isə həm kibertəhlükəsizlikdə müsbət rol oynayır (hücumların aşkarlanması, məlumatların sürətli analizi), həm də psixoloji manipulyasiya və şəxsi məlumatların açıqlanması baxımından yeni risklər doğurur [6].
- Bu balans göstərir ki, texnologiyanın müsbət tərəflərindən faydalanmaq üçün paralel şəkildə maarifləndirmə, hüquqi tənzimləmə və texniki qoruma tədbirləri gücləndirilməlidir [1, 3].

NƏTİCƏ

Gündəlik internet istifadəsi müasir həyatın ayrılmaz hissəsinə çevrilmişdir və bu proses həm üstünlüklər, həm də risklər doğurur. İnkişaf edən texnologiyalar insanlara məlumatı daha tez əldə etmək, vaxta qənaət etmək, iş və təhsil proseslərini sürətləndirmək imkanı verir. Lakin eyni zamanda şəxsi məlumatların açıqlanması, psixoloji manipulyasiya və hüquqi boşluqlar kimi təhlükələr də mövcuddur.

Bu səbəbdən, istifadəçilərin şüurlu davranışı və təhlükəsizlik mədəniyyətinin formalaşdırılması əsas şərt olaraq qalır. İnternetdən və süni intellekt əsaslı xidmətlərdən faydalanarkən parol idarəetməsində çoxfaktorlu autentifikasiyanın tətbiqi, ictimai Wi-Fi şəbəkələrində VPN texnologiyalarının istifadəsi, sosial şəbəkələrdə şəxsi məlumatların paylaşılmasının məhdudlaşdırılması, bulud xidmətlərində məlumatların şifrələnməsi və milli təhlükəsizlik standartlarının qorunması vacibdir. Aparılan təhlillər göstərir ki, gündəlik internet istifadəsinin doğurduğu riskləri lehimizə çevirmək üçün ən vacib addımlardan biri maarifləndirici seminarların təşkili və insanların kibertəhlükəsizlik barədə biliklərinin artırılmasıdır.

ƏDƏBİYYAT

[1] International Telecommunication Union (ITU), Global Cybersecurity Index 2024, 5th ed. Geneva, Switzerland: ITU, 2024.

[2] European Union Agency for Cybersecurity (ENISA), Basic Security Practices Regarding Passwords and Online Identities: End Users. Heraklion, Greece: ENISA.

[3] Azərbaycan Respublikası Prezidentinin Sərəncamı, "Azərbaycan Respublikasının informasiya təhlükəsizliyi və kibertəhlükəsizliyə dair 2023–2027-ci illər üçün Strategiyası," Bakı, Azərbaycan, 28 avqust 2023.

[4] F. Aslay, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi," International Journal of Multidisciplinary Studies and Innovative Technologies, vol. 1, no. 1, pp. 24–28, 2017.

[5] S. F. Arslan, 21. Yüzyılda Ulusal ve Uluslararası Siber Güvenlik: Türkiye'nin Siber Güvenlik Strateji ve Politikaları, Yüksek Lisans Tezi, İstanbul Yeni Yüzyıl Üniversitesi, Sosyal Bilimler Enstitüsü, İstanbul, Türkiye, 2023.

[6] National Institute of Standards and Technology (NIST), "Social engineering," Computer Security Resource Center Glossary, Gaithersburg, MD, USA.

Cybersecurity Risks for Internet Users

Mahammadali Babayev

Azerbaijan State Oil and Industry University, Baku, Azerbaijan

Mhmmdlibabayev42@gmail.com

Abstract– he Internet has become an integral part of people's daily lives in the modern era. Social media, email, cloud services, and online platforms are widely used. However, alongside these opportunities, cybersecurity risks are also increasing. Weak password management, the use of public Wi-Fi networks, social engineering attacks, and inadequate data protection pose serious threats to users. This article examines the main cybersecurity risks encountered in everyday Internet use, compares them with international practices, and proposes practical recommendations for Internet users in Azerbaijan.

Keywords– cybersecurity; internet use; password management; social networks; cloud services.