

<https://doi.org/10.36719/2789-6919/42/28-34>

Ziyafət Əmirov

Dövlət Təhlükəsizlik Xidmətinin Heydər Əliyev adına Akademiyası
texnika elmləri namizədi

<https://orcid.org/0009-0005-6358-5768>

zamirov@inbox.ru

Müjkan Məmmədzadə

Hərbi Elmi Tədqiqat İnstitutu
pedaqogika üzrə fəlsəfə doktoru

<https://orcid.org/0000-0001-5693-3748>

mujkan@mail.ru

Müasir informasiya cəmiyyətinin formalaşması ilə cəmiyyətdə yaranan informasiya təhlükəsizliyi problemləri

Xülasə

Məqalədə müasir informasiya cəmiyyətinin formalaşması ilə cəmiyyətdə yaranan informasiya təhlükəsizliyi problemlərindən bəhs olunur. Belə ki, təcrübə göstərir ki, informasiya cəmiyyətinə qədəm qoymuş ölkələrdə formalaşmış informasiya mühiti, informasiya ehtiyatları və informasiya texnologiyaları sosial-iqtisadi, elmi-texniki və mədəni inkişafın həm səviyyəsini, həm də dinamikasını müəyyən edir.

Cəmiyyətin informasiyalaşdırılması texniki, texnoloji, sosial, iqtisadi, siyasi və mədəni komponentlərin üzvi qarşılıqlı əlaqədə olduğu, sosial orqanizmin bütün strukturunu keyfiyyətcə dəyişdirən çoxşaxəli prosesdir. İnformasiya cəmiyyətinin formalaşması sosial-iqtisadi, siyasi münasibətlərdə köklü dəyişikliklərlə yanaşı, mədəniyyətdə, mənəvi həyatda və məişətdə də dəyişiklikləri əks etdirir. Yuxarıdakıları ümumiləşdirərək deyə bilərik ki, informasiyalaşdırma, yaxud informasiya cəmiyyətinin formalaşması təkcə texniki və texnoloji deyil, bütün ictimai münasibətlər sisteminin sosial-texnoloji və intellektual-humanitar transformasiyasıdır.

Məqalədə sosial şəbəkələrdə istifadəçilərin qurbana çevrilməsinin qarşısının alınması və risklərin minimuma endirilməsi üçün ölkənin təhsil sistemində informasiya texnologiyaları və informasiya təhlükəsizliyi üzrə ixtisasların effektiv tədrisinin təşkil edilməsinə, müasir tələblərə cavab verən ixtisaslı kadrların hazırlanmasına dövlət dəstəyinin gücləndirilməsi, informasiya təhlükəsizliyi və kibertəhlükəsizlik istiqamətləri üzrə ali təhsil müəssisələrində ixtisaslaşmış fiziki laboratoriyaların, maliyyə imkanlarının məhdud olduğu ali təhsil müəssisələrində və təşkilatlarda isə analoji virtual laboratoriyaların yaradılması və bu laboratoriyalarda elmi-tədqiqat xarakterli praktiki işlərin icrasının geniş şəkildə aparılması, yetkinlik yaşına çatmayan istifadəçilərin sosial şəbəkələrdən istifadəsinin mümkün qədər məhdudlaşdırılması, bu mümkün olmadıqda isə təhlükəsiz şəkildə istifadə qaydalarının onlara öyrədilməsi və s. hərəkətlərin icrasını məqsədəuyğun hesab edilmişdir.

Açar sözlər: informasiya, dezinformasiya, fərd, cəmiyyət, informasiya cəmiyyəti, sosial şəbəkə savadlılığı, fırıldaqçılıq

Ziyafət Amirov

Heydar Aliyev Academy of the State Security Service
PhD in Technical Sciences

<https://orcid.org/0009-0005-6358-5768>

zamirov@inbox.ru

Mujkan Mammadzadeh

Military Scientific Research Institute

PhD in pedagogy

<https://orcid.org/0000-0001-5693-3748>

mujkan@mail.ru

Information Security Problems Arising in Society With the Formation of the Modern Information Society

Abstract

The article discusses the problems of information security arising in society with the formation of a modern information society. Thus, experience shows that the information environment, information resources and information technologies formed in countries that have entered the information society determine both the level and dynamics of socio-economic, scientific-technical and cultural development. If we look at history, we will see that the geopolitical processes taking place in the world over the past 30-40 years, their management, regulation of international relations, as well as the solution of military-geostrategic, geographical-territorial and socio-economic problems are closely related to the activities of each state in the information field.

The relevance of research on the information society is associated with the need for theoretical understanding of the processes arising under the influence of information and communication technologies and their effective political management. Against the background of the emergence of an information society, global changes are taking place that change the entire social structure and affect political, economic, cultural and social processes. The socio-economic structure of society is changing radically.

The informatization of society is a multifaceted process in which technical, technological, social, economic, political and cultural components are organically interconnected, qualitatively changing the entire structure of the social organism. The formation of an information society reflects, along with radical changes in socio-economic and political relations, changes in culture, spiritual life and everyday life. Summarizing the above, we can say that informatization, or the formation of an information society, is not only a technical and technological, but also a socio-technological and intellectual-humanitarian transformation of the entire system of social relations.

The article considers it appropriate to organize effective teaching of information technology and information security specialties in the country's education system in order to prevent users from becoming victims and minimize risks, strengthen state support for the preparation of qualified personnel who meet modern requirements, create specialized physical laboratories in higher education institutions in the areas of information security and cybersecurity, and similar virtual laboratories in higher education institutions and organizations with limited financial resources, and widely carry out practical work of a scientific and research nature in these laboratories, limit the use of social networks by minors as much as possible, and if this is not possible, teach them the rules for safe use, etc.

Keywords: *information, disinformation, individual, society, information society, social network literacy, fraud*

Giriş

Sivilizasiyanın müasir inkişaf tendensiyası inkişaf etmiş sənaye cəmiyyətindən informasiya cəmiyyətinə keçid ilə xarakterizə olunur. Bu gün dünyada baş verən ictimai-siyasi proseslər bir daha onu göstərir ki, dövlətin qarşısında duran ən vacib vəzifələr sırasında hüquqi dövlət quruculuğu və informasiya cəmiyyətinin bərqərar olmasıdır. Belə bir şəraitdə hər bir ölkədə insan və vətəndaş hüquqlarının təminatı bilavasitə informasiya cəmiyyətinin formalaşması səviyyəsindən asılıdır.

Təcrübə göstərir ki, informasiya cəmiyyətinə qədəm qoymuş ölkələrdə formalaşmış informasiya mühiti, informasiya ehtiyatları və informasiya texnologiyaları sosial-iqtisadi, elmi-texniki və mədəni inkişafın həm səviyyəsini, həm də dinamikasını müəyyən edir. Tarixə nəzər salsaq görərik ki, son 30-40 ildə dünyada cərəyan edən geosiyasi proseslər, onların idarə edilməsi, beynəlxalq münasibətlərin tənzimlənməsi, eləcə də hərbi-geostrateji, coğrafi-ərazi və sosial-iqtisadi problemlərin həlli hər bir dövlətin informasiya sahəsində fəaliyyəti ilə sıx bağlıdır. Son onilliklərdə baş verən informasiya texnologiyaları inqilabı bəşəriyyətin yeni cəmiyyət tipi olan informasiya cəmiyyətinə doğru hərəkətini müəyyən etmişdir. İnformasiya texnologiyaları maddi nemətlərin istehsalının yeni iqtisadiyyatında əsas məhsuldar qüvvəyə çevrilir. Onların sayəsində əməyin təbiətində, mülkiyyət

münasibətlərində dərin dəyişikliklər, ictimai quruluşda və sosial həyatın bütün digər alt sistemlərində baş verən dəyişikliklərlə əlaqəli yeni informasiya istehsal üsulu yaranır (https://vuzlit.com/964950/problema_informatsionnoy_bezopasnosti_obschestva).

Beləliklə, informasiya cəmiyyətinə aid tədqiqatların aktuallığı informasiya-kommunikasiya texnologiyalarının təsiri altında yaranan proseslərin nəzəri dərk edilməsi və səmərəli siyasi idarə olunması ehtiyacı ilə bağlıdır. İnformasiya cəmiyyətinin yaranması fonunda bütün ictimai quruluşu dəyişdirən, siyasi, iqtisadi, mədəni və sosial proseslərə təsir edən qlobal dəyişikliklər baş verir. Cəmiyyətin sosial-iqtisadi strukturu köklü şəkildə dəyişir.

Tədqiqat

İnformasiya cəmiyyətinin formalaşmasında mühüm rol oynayan sosial şəbəkələr çoxdan həyatımızın ayrılmaz hissəsinə çevrilmişdir. Xüsusilə də, pandemiya zamanı təcrid insanları daha çox onlayn ünsiyyətə və sosial şəbəkələrdən məlumat əldə etmək üçün əsas kanal kimi istifadə etməyə sövq etmişdir. Eyni zamanda getdikcə genişlənən auditoriya, bütün dünyada əhatə dairəsinin mövcudluğu və istifadəçilərin hər şeyə tez inanan olmaları sosial şəbəkələrdə kibercinayətkarların çoxalmasına səbəb olmuşdur. İstifadəçilər verilənləri açıq şəkildə paylaşır, tez-tez zəif parollardan istifadə edir və hər il milyonlarla insan hesabın sındırılmasının, şəxsi məlumatların oğurlanmasının qurbanı olur, nəticədə külli miqdarda pul itirir. Təəssüf ki, universal qorunma vasitəsi yoxdur, ona görə də yalnız bilik və əsas təhlükəsizlik qaydalarına riayət etmək sosial şəbəkələrdə istifadəçilərin aldadılmalarının qarşısını almağa kömək edəcəkdir.

Adi həyatda olduğu kimi, informasiya cəmiyyəti mühitində də fırıldaqçılardan həyata keçirirdikləri bütün hərəkətlərinin bir əsas məqsədi olur - pul qazanmaq! Sosial şəbəkələrdə istifadəçiləri aldatmağın ən sadə və az əmək tələb edən üsullarından biri *saxta hesab* yaratmaq və ondan istifadədir. Fırıldaqçılar özlərini aşağıdakı formaların birində təqdim etməklə məqsədlərinə nail ola bilərlər (<http://www.sberbank.ru/promo/scs-school/courseid-3.html>):

- 1) *“can yoldaşı axtaran” tək adam* – bu tək adamın əsl məqsədi istifadəçilərdən maliyyə və ya şəxsi məlumat əldə etməkdir;
- 2) *ehtiyacı olan* və maddi yardım istəyən bir şəxs;
- 3) *məşhur bir şəxs* – fırıldaqçı onun adından “qazan-qazan” lotereyaları və müsabiqələr keçirir;
- 4) *dəstək xidməti* - dövlət qurumları, digər təşkilatlar. Onların adından qurbanları tora salmaq üçün fişinq mesajları göndərir;
- 5) *onlayn mağaza* - məhsullarını sosial şəbəkə vasitəsilə “satmaq” istəyən fırıldaqçı;
- 6) *bədxah* - qəzəbli mesajlar və şərhlər yazan şəxs;
- 7) özünü *istifadəçinin dostu kimi* təqdim edib onun adından maddi yardım istəyən şəxs.

Hansı formada maskalanmalarından asılı olmayaraq, fırıldaqçılar qurbanlarını aldatmağa çalışacaqlar ki, aldadılmış qurbanı fişinq linkini izləməyə, zərərli proqram yükləməyə və ya pul köçürməyə məcbur etsinlər.

Sosial şəbəkələrdə dezinformasiyanın tanınması və onunla mübarizə. Bəlli olduğu kimi, **dezinformasiya** insanları aldatmaq üçün qəsdən yayılan yalan məlumatdır. Müasir informasiya məkanında, xüsusən də sosial şəbəkələrdə dezinformasiya cəmiyyət və ayrı-ayrı fərdlər üçün əsl bəlaldan birinə çevrilmişdir. Bu səbəbdən geniş həcmli, müxtəlif çeşidli informasiya axınında dezinformasiyanın tanınması və onunla mübarizə xüsusi əhəmiyyət kəsb edir. Sosial şəbəkələrdə dezinformasiyanın tanınmasının geniş yayılmış üsullarına aşağıdakı nümunələri göstərmək olar (<https://www.securitylab.ru/blog/personal/SimpleHacker/352876.php>):

1. Məlumatın mənbəyinin yoxlanılması - mənbə nüfuzlu və yoxlanılmış deyildirsə, bu məlumatı təsdiqləyən digər mənbələri axtarmaq lazımdır. Əgər onlar yoxdursa, çox güman ki, istifadəçinin qarşılaşdığı məlumat dezinformasiyadır.

2. Məlumatın üslubunun təhlili - çox vaxt saxta xəbərlər oxucuların diqqətini cəlb etmək üçün ifadəli, sensasiyalı üslubda yazılır. Əksər hallarda onlar çoxlu qrammatik və orfoqrafik səhvləri ehtiva edirlər. Məlumatın üslubunun şübhəli olması dezinformasiya əlaməti ola bilər.

3. Şəkil və video təhlili - dezinformasiya tez-tez saxtalaşdırılmış və ya fərqli kontekstdən götürülmüş şəkil və ya videolarla müşayiət olunur. Şəkillərin həqiqiliyini yoxlamağa imkan verən *Google Reverse Image Search* və ya *TinEye* kimi xüsusi alətlərdən istifadə oluna bilər.

4.Nəşr tarixinin yoxlanılması - bəzən köhnə xəbərlər və ya hadisələr insanları çaşdırmaq üçün yeniləri kimi təqdim olunur. Buna görə, həmişə materialın dərc tarixini yoxlamaq lazımdır. Sosial şəbəkələrdə dezinformasiyaya qarşı effektiv mübarizə məqsədilə aşağıdakı tədbirlərdən istifadə məqsədəuyğundur (<https://www.securitylab.ru/blog/personal/SimpleHacker/352876.php>)

Ω Sosial şəbəkə savadlılığının təkmilləşdirilməsi - dezinformasiya ilə effektiv mübarizə aparmaq üçün hər kəs sosial şəbəkələrlə işləmə savadını artırmalıdır. Burada savadlılıq dedikdə məlumatın necə və haradan gəldiyinin və onun necə təhrif və ya manipulyasiya edilə biləcəyinin başa düşülməsi kimi məsələlər başa düşülür;

Ω Tənqidi düşüncə - alınan məlumatlara tənqidi düşüncənin tətbiqi dezinformasiyanı tanımağa və onunla mübarizə aparmağa kömək edə bilər. Şübhəli görünən məlumatı soruşmaq və həmişə təsdiq üçün əlavə mənbələr axtarmaq gərəkdir;

Ω Təsdiqlənmiş məlumatı yaymaqdan imtina - dezinformasiya ilə mübarizə aparmağın bir yolu da onun yayılmasının dayandırılmasıdır. İstifadəçi məlumatın düzgünlüyünə əmin deyildirsə onu paylaşmamalıdır;

Ω Faktların yoxlanılması resurslarından istifadə - məlumatların yoxlanılması üzrə ixtisaslaşan müxtəlif fakt yoxlayan təşkilatlar və platformalar vardır (*FactCheck.org*, *OnTheMedia.org* və *PolitiFact.com*). Onların istifadəsi fakt ilə uydurma məlumatı bir-birindən ayırmağa kömək edə bilər (<https://ru.wikipedia.org/wiki/Фактчекинг>)

Yekun olaraq qeyd edək ki, sosial şəbəkələrdə və KİV-də dezinformasiya ilə mübarizə çətin, lakin vacib, ölkə əhəmiyyətli məsələlərdən biridir. Hər bir ölkə vətəndaşı sosial şəbəkə savadlılığını artırmaqla, tənqidi düşüncə tərzini tətbiq etməklə, saxta xəbərlərin yayılmasında iştirak etməməklə dezinformasiya ilə mübarizə öz töhfəsini verə bilər.

Qeyd edək ki, XXI əsrin ən məşhur on kiberhücumları sırasında sosial şəbəkələrlə bağlı iki hücum yer tutur (Zuikova, 2024)

Facebook sosial şəbəkəsinin sındırılması (hack edilməsi) – 2020-ci ilin martında şəbəkə istifadəçilərinin fərdi məlumatlarına hücum təşkil edilmişdir. Nəticədə sosial şəbəkədən ən yüksək məlumat sızması baş vermişdir. 2020-ci ilin mart ayında Britaniyanın Comparitech şirkəti 267 milyondan çox Facebook istifadəçisi haqqında məlumat sızdığını bildirdi (Writer Paul Bischoff, 2020). Onların əksəriyyəti amerikalılar idi (<https://www.vedomosti.ru/technology/news/2019/12/20/819272-ob-utechke-facebook>). Onlardan fişinq linklərini göndərmək üçün istifadə edilə bilərdi. 2020-ci ilin avqust ayında DarkNet Data Leakage & Breach Intelligence (DLBI) şirkətinin mütəxəssisləri Internetdə 150 milyon Facebook, Instagram və LinkedIn istifadəçisinin şəxsi məlumatlarını tapıblar (<https://t.me/dataleak/1847>). Bu dəfə məlumatlar Çinin Shenzhen Benniao Social Technology şirkətinə məxsus ABŞ serverindən oğurlanıb (<https://www.vedomosti.ru/media/news/2020/08/28/838094-eksperti-soobschili-ob-utechke-dannih-klientov-facebook-instagram-linkedin>).

Dəyən ziyan: İlk sızıntılardan sonra ABŞ Federal Ticarət Komissiyası Facebook şəbəkəsinə rekord məbləğdə 5 milyard dollar cərimə ödəməyi əmr etdi. Bu, məlumat sızmasına görə tətbiq edilən ən böyük sanksiyalardan 20 dəfə yüksəkdir.

Məşhurların Twitter (X) hesablarının sensasiyalı sındırılması – 2020-ci ilin iyulunda Bill Geyts, Elon Mask, Jeff Bezos, Kanye West və digər məşhur şəxslərin Twitter (X) hesabları hücumu məruz qalmışdır.

Onların sındırılmış (hack edilmiş) profillərində cinayətkarlar Amerika ulduzları, siyasətçiləri və iş adamları adından göstərilən kripto pul kisəsinə bitkoinlər göndərməyə çağırıblar. Onlar hər transferi ikiqat məbləğdə qaytaracaqlarına söz veriblər (şəkil 1, şəkil 2). Apple və Uber korporativ hesabları da zərər çəkmişdir. Ümumilikdə 50-dən çox məşhur şəxsin hesabları sındırılmış və dələduzlar 110000\$-dan çox pul əldə etmişlər.

Şəkil 1. Apple şirkətinin hesabı adından bitkoinlərin istənilməsi



Şəkil 2. Elon Maskın adından bitkoinlərin istənilməsi



Qeyd edək ki, 2009-2019-cu illərdə Barak Obama, Donald Tramp və Cek Dorsi (Twitter-in baş direktoru) kimi məşhurların Twitter hesabları sındırılmışdı (Litvinenko, 2020). Lakin 2020-ci ilin hücumu ən kütləvi hücum olmuşdur.

Nümunə. 2020-ci ildə 44 günlük Vətən Müharibəsi zamanı döyüş meydanında Azərbaycan Ordusu qarşısında məğlub olan əbədi düşmənlərimiz - ermənilər sosial şəbəkə və digər rəqəmsal platformalarda müxtəlif saxta saytlar yaradıb cəbhəboyu zonadakı vəziyyət, xüsusilə də hərbi-siyasi və əməliyyat şəraiti, hərbi texnika və onun hərəkəti haqqında, eləcə də silah-sursat barədə saxta xəbərlər ictimailəşdirməklə vətəndaşlarımızda çaşqınlıq yaratmağa, onlara psixoloji təsir göstərməyə cəhdlər edirdilər. Belə saytlara “hamimiz.com” saytını misal göstərmək olar. Bu saxta saytın Azərbaycanın şəhidlər siyahısında Aprel döyüşlərində şəhid olan qardaşlarımız, bəzən Sərdar Ortaç, CZN Burak kimi adamlar da yer alır. Bu o deməkdir ki, bu siyahılar heç bir kəşfiyyət məlumatı olmadan kortəbii, elə bizim verdiyimiz məlumatlar əsasında yaradılır. Buna görə vətəndaşlarımızdan şəhidlərimizin şəkillərini paylaşan zaman aşağıdakı məqamları nəzərə almaları xahiş olunur:

- ✓ Ümumiyyətlə paylaşmamaq məsləhətdir;
- ✓ Paylaşarkən ad və soyaddan başqa, hərbi vəzifə, hərbi hissə kimi məlumatları yazmaq doğru deyil;
- ✓ Belə paylaşmaları public yox, sadəcə dostlar üçün paylaşmağınız məsləhətdir və s.

Bu saxtakarlıq barədə Baş Prokurorluğun yaydığı məlumatda deyilir: “Azərbaycan Ordusunun uğurlarının Ermənistan əhalisindən gizlədilməsinə, vətəndaşlarımızda təşviş yaratmağa yönələn bu cəhdlər ifşa olunmuşdur. Ermənistan tərəfindən həyata keçirilmiş növbəti təxribatlardan biri də “hamimiz.com” adlı saxta saytın yaradılmasıdır. Həmin “fake” saytda guya şəhid olmuş və itkin düşmüş hərbi qulluqçuların siyahısına mülki şəxslərin, o cümlədən qadınların da adları daxil edilib.

Bununla da, qeyd olunan saytın düşmənin maraqlarına xidmət etməsi, əhalimiz arasında təşviş yaratmaq məqsədi daşması müəyyən edilmişdir. Hər kəsi vətəndaş məsuliyyətini dərinlən dərk etməyə, ayıq-sayıq olmağa, bu kimi saxta saytlarda və digər informasiya daşıyıcılarında olan təxribat xarakterli məlumatlara inanmamağa çağırır, şübhəli hər hansı saxta platforma ilə qarşılaşan zaman hüquq-mühafizə orqanlarına dərhal məlumat verilməsi xahiş olunur” (<https://www.yeniavaz.com/az/news/152787/bas-prokurorluq-hamimizcom-adli-saxta-saytla-bagli-arasdirmalara-baslanilib>).

Nümunə. Medianın İnkişafı Agentliyinin (MİA) və Dövlət Təhlükəsizliyi Xidmətinin (DTX) birgə məlumatında bildirilmişdir: 2024-cü ilin aprel ayının ilk ongünlüyündə bəzi sosial şəbəkələrdə Azərbaycan-Ermənistan sərhədində gərginliyin artması, Azərbaycan Ordusunda şəhidlərin və yaralıların olması, qoşun birləşmələrinin və ağır artilleriya silahlarının hazırlıq vəziyyətinə gətirilməsi, Laçın rayonu ərazisində komendant saatının tətbiq edilməsi ilə bağlı bir sıra şəxslər tərəfindən əsassız məlumatlar, reallığı əks etdirməyən saxta xəbərlər yayımlanır (https://musavat.com/news/dtx-herekete-kecdi-ordu-ile-bagli-yalan-xeberyayanlar_1059407.html).

Bildirilib ki, DTX tərəfindən aparılan araşdırmalar nəticəsində cəmiyyətdə narahatlığın yaranmasına səbəb olan bu kimi məlumatları yayan şəxslərin Azərbaycan Respublikasının vətəndaşları – 1977-ci il təvəllüdü Əliyev Rəşad Balağa oğlu və 1973-cü il təvəllüdü Məlikov Pərviz Ramiz oğlu olduğu müəyyən edilib, onların belə məlumatları yaymalarının qarşısı alınaraq zəruri hüquqi prosedur tədbirlər həyata keçirilib.

MİA və DTX sözügedən əməllərin törədilməsinin ciddi hüquqi məsuliyyətə səbəb olduğuna dair xəbərdarlıq edərək, media subyektlərini və jurnalistləri sosial şəbəkələrdə yayımlanan qeyri-dəqiq, mənbəyi bilinməyən məlumatlardan istifadə etməməyə, vətəndaşları bu kimi hallara qarşı hər zaman prinsipiallıq nümayiş etdirməyə, sosial şəbəkələrdə yayılan, rəsmi mənbələrə söykənməyən əsassız informasiyalara inanmamağa çağırır.

Nəticə

Sosial şəbəkələrdə istifadəçilərin qurbana çevrilməsinin qarşısının alınması və risklərin minimuma endirilməsi üçün aşağıdakı hərəkətlərin icrasını məqsədəuyğun hesab edirik:

- ölkənin təhsil sistemində informasiya texnologiyaları və informasiya təhlükəsizliyi üzrə ixtisasların effektiv tədrisinin təşkil edilməsinə, müasir tələblərə cavab verən ixtisaslı kadrların hazırlanmasına dövlət dəstəyinin gücləndirilməsi;

- mütəmadi olaraq istifadəçilərin diqqətinə paylaşılması riskli olan məlumatların çatdırılması, belə məlumatlara şəxsiyyət vəsiqəsi, sürücülük vəsiqəsi, ümumvətəndaş pasportu, sağlamlıq göstəriciləri, kredit kartları, bank hesabları, eləcə də, iş yeri və olduğu məkan haqqında, əməkhaqqı barədə, bütün elektron resurslarda istifadə ilə əlaqəli ad və parollara aid məlumatlar aid edilə bilər;

- informasiya təhlükəsizliyi və kibertəhlükəsizlik istiqamətləri üzrə ali təhsil müəssisələrində ixtisaslaşmış fiziki laboratoriyaların (nümunə olaraq kibernetika, kibermüdafiə, rəqəmsal kriminalistika, kriptografik və s. Qeyd etmək olar), maliyyə imkanlarının məhdud olduğu ali təhsil müəssisələrində və təşkilatlarda isə analogi virtual laboratoriyaların yaradılması və bu laboratoriyalarda elmi-tədqiqat xarakterli praktiki işlərin icrasının geniş şəkildə aparılması;

- tədris müəssisələrində və KİV-də, xüsusilə də televiziya kanallarında informasiya təhlükəsizliyi və kibertəhlükəsizlik sahələrində əhalinin bütün təbəqələrinin maarifləndirilməsi işinə ixtisaslı və peşəkar mütəxəssislərin daha çox cəlb edilməsi və maarifləndirmə işinin intensivləşdirilməsi;

- yetkinlik yaşına çatmayan istifadəçilərin sosial şəbəkələrdən istifadəsinin mümkün qədər məhdudlaşdırılması, bu mümkün olmadıqda isə təhlükəsiz şəkildə istifadə qaydalarının onlara öyrədilməsi;

- ölkədə tədris və maarifləndirmə işinin təkmilləşdirilməsi ilə bağlı tanınmış şəxslərin, alim və mütəxəssislərin iştirakı ilə elmi seminarların, dəyirmi masaların keçirilməsi və bu tədbirlərin KİV-də işıqlandırılması və s.

Ədəbiyyat

1. Baş Prokurorluq: “hamimiz.com” adlı saxta saytla bağlı araşdırmalara başlanılıb: [Elektron resurs] 09 noyabr, 2020. URL:<https://www.yeniavaz.com/az/news/152787/bas-prokurorluq-hamimiz-com-adli-saxta-saytla-bagli-arasdirmalara-baslanilib>
2. Британская компания сообщила об утечке данных 267 млн пользователей Facebook: 20 декабря 2019. URL: <https://www.vedomosti.ru/technology/news/2019/12/20/819272-ob-utechke-facebook>
3. DTX hərəkətə keçdi: ordu ilə bağlı yalan xəbər yayanlar...: [Elektron resursları] / - 08 aprel 2024. URL: https://musavat.com/news/dtx-herekete-kecdi-ordu-ile-bagli-yalan-xeberyayanlar_1059407.html

4. Эксперты сообщили об утечке данных клиентов Facebook, Instagram и LinkedIn: [Электронный ресурс] / - 28 августа 2020. URL: <https://www.vedomosti.ru/media/news/2020/08/28/838094-eksperti-soobschili-ob-utechke-dannih-klientov-facebook-instagram-linkedin>
5. Фактчекинг: [Электронный ресурс] / URL: <https://ru.wikipedia.org/wiki/Фактчекинг>
6. FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook: [Electronic resource] / - July 24, 2019. URL: <https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook>
7. Как распознать и бороться с дезинформацией в социальных сетях: [Электронный ресурс] / - 23 мая, 2023. URL: <https://www.securitylab.ru/blog/personal/SimlpeHacker/352876.php>
8. Литвиненко, Ю. Крупнейшая хакерская атака на Twitter: [Электронный ресурс] / - 16 июля 2020. URL: <https://www.vedomosti.ru/technology/articles/2020/07/16/834712-vzлом-milliardero-v-twitter>
9. Проблема информационной безопасности общества: [Электронный ресурс] / URL: https://vuzlit.com/964950/problema_informatsionnoy_bezopasnosti_obschestva
10. Утечки информации: [Электронный ресурс] / URL: <https://t.me/dataleak/1847>
11. ВНИМАНИЕ-СОЦИАЛЬНЫЕ СЕТИ!: [Электронный ресурс] URL: <http://www.sberbank.ru/promo/scs-school/courseid-3.html>
12. Зуйкова, А. 10 самых громких кибератак XXI века: [Электронный ресурс] / - 17 сентября 2024. URL: <https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e>.
13. Writer Paul Bischoff, Report: 267 million Facebook users IDs and phone numbers exposed online (UPDATE: now 309 million) [Electronic resource] March 9, 2020. URL: <https://www.comparitech.com/blog/information-security/267-million-phone-numbers-exposed-online/>

Daxil oldu: 11.11.2024

Qəbul edildi: 21.02.2025