

UOT 04:37

DOI: 10.25045/jpis.v10.i2.11

Ocaqverdiyeva S.S.

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
allahverdiyevsabira@gmail.com

UŞAQLARIN İNTERNET TƏHLÜKƏLƏRİNDƏN QORUNMASINDA QANUNVERİCİLİKDƏN İRƏLİ GƏLƏN TEXNOLOJİ VƏZİFƏLƏR HAQQINDA

Daxil olmuşdur: 17.05.2019. Düzəliş olunmuşdur: 10.06.2019. Qəbul olunmuşdur: 01.07.2019.

Uşaqların İnternet mühitində təhlükəsizliyinin təmin olunması bu gün dünyada informasiya təhlükəsizliyinin vacib məsələlərindəndir. Hər bir dövlət gələcək nəslin daha sağlam və yararlı vətəndaş olmasında maraqlıdır. Məqalədə uşaqların İnternet mühitində qarşılaşdığı təhlükələr analiz edilərək müəyyənləşdirilmiş, uşaqların informasiya təhlükəsizliyinin təmin olunması ilə əlaqədar beynəlxalq və ölkədaxili tədbirlər, normativ sənədlər və qanunlar araşdırılmışdır. Müvafiq qanunvericilik aktlarından irəli gələn texnoloji vəzifələr müəyyənləşdirilmişdir. Uşaqların zərərli informasiyadan qorunmasını daha səmərəli şəkildə təmin etmək üçün texnoloji tədbirlərin görülməsinə dair təkliflər işlənmişdir.

Açar sözlər: uşaqların təhlükəsizliyi, zərərli informasiya, kibercoraklıq, kiberdələduzluq, İnternet asılılıq, fişinq.

Giriş

İnternet insan fəaliyyətinin bütün sahələrinə tətbiq edilir və bunun təsiri ilə son onilliklər ərzində istifadəçilərin sayı bir neçə dəfə artmışdır. İnternetə daxil olan hər bir istifadəçi özünün mənfi və ya müsbət fikirlərini virtual mühitdə paylaşır.

Uşaq və yeniyetmələr İnternetin aktiv istifadəçiləridirlər. Rəqəmsal dünyaya daxil olmaq, ünsiyyət yaratmaq, yeni məlumat əldə etmək uşaqların həyat tərzini köklü surətdə dəyişir və onların potensialını artırır. İnternet uşaqların məlumatlanmasında, sosiallaşmasında, dünyagörüşünün formalaşmasında və informasiyanın sürətlə əldə edilməsində mühüm rol oynayır. Uşaqlar İnternetdən faydalanırlar, lakin istifadə zamanı müxtəlif təhlükələrlə üzləşir və kibercinayətkarların hədəfinə çevrilirlər. Araşdırmalara görə sosial şəbəkələrə daxil olan üç uşaqdan biri özü haqqında tam məlumat yerləşdirir [1].

UNICEF-in London İqtisad Universiteti ilə birgə təşkil etdiyi “Global kids online” layihəsi dünyanın müxtəlif ölkələrində uşaqların İnternet mühitində təhlükəsizliyi mövzusunda tədqiqat aparan mütəxəssisləri öz ətrafında birləşdirir. Bu layihə uşaqların İnternetdən istifadə bacarıqları, yaş kateqoriyasına görə rəqəmsal resurslardan istifadə, kibertəhlükələrlə qarşılaşma riski və onların nəticələri, ziyanlı informasiyanın vurduğu zərərlər və s. mövzularını əhatə edir. Həmin təşkilatın müxbir üzvləri tərəfindən 2016-cı ildə Argentinada aparılan tədqiqatların nəticələrinə görə hər 10 uşaqdan 9-u İnternetə mobil telefonla bağlanır, uşaq və yeniyetmələrin 95%-nin Facebook profili vardır və İnternet istifadəçisi kimi qızlar oğlanlardan daha fəaldırlar [2].

Serbiyada aparılan tədqiqatın nəticələrinə əsasən il ərzində onlayn mühitdə uşaq və yeniyetmələrin əksəriyyəti cinsi istismar xarakterli kontentlə qarşılaşmışdır. Eyni zamanda aqressiya xarakterli məlumatlarla üzləşən uşaqların 14 %-i bildirmişdir ki, il ərzində belə hallar bir neçə dəfə təkrarlanır [3].

Qeyd etmək lazımdır ki, real həyatda olduğu kimi, virtual məkanda da uşaqların fəaliyyəti yaş qruplarına və cinsinə görə fərqlidir. İnternetdə erkən yeniyetməlik yaşlarında oğlanlar qızlardan daha aktivdirlər. 15-17 yaşlarda isə qızlar daha çox İnternetdən istifadə edir [3]. Məlumdur ki, uşaqların yaşları artdıqca onların İnternetdən istifadə bacarıqları dəyişir və maraqları müxtəlifləşir. Şagirdlərin çoxu İnternetdən yalnız təhsil məqsədləri üçün istifadə etmirlər. Onlar təhsil saytları ilə yanaşı digər veb-səhifələrə daxil olur və bu zaman ziyanlı məlumatlarla qarşılaşır, İnternetdə tanımadıqları insanlarla əlaqə yaradır və əksər hallarda bu insanlarla real həyatda da görüşürlər.

“Kaspersky Laboratoriyası”nın apardığı araşdırmaların nəticələrinə görə İnternet təhdidlərinə ən çox məruz qalan 13-15 yaş arası uşaqlardır [4].

İnternet səhifələrdə arzuolunmaz mənəvi və əxlaqi keyfiyyətləri aşılayan kontentlər çoxdur. Belə kontentlər uşaqların yaşına uyğun olmayan şəkillərlə cinsi istismarını və spirtli içkilərin istehlakını təbliğ edir. Həmçinin psixotrop maddələrin qəbulunu, qəddarlığı, təcavüz və intiharı, ailəyə qarşı hörmətsizliyi, aldatma, yalan və jarqon ifadələrlə danışmağı təbliğ edir [5]. Uşaqlar və yeniyetmələri belə kontentlərdən qorunmaq üçün İnternetdən istifadəni tamamilə qadağan etməklə onları onlayn təhlükələrdən uzaqlaşdırmaq mümkün deyil. Bu yanaşma çox vaxt əksinə azyaşlı istifadəçinin İnternetə marağını bir qədər də artırmağa bilər. Müasir dövrdə artıq istənilən məkandan müxtəlif qurğular vasitəsilə İnternetə daxil olmaq mümkündür. Belə nəticəyə gəlmək olar ki, uşaqların onlayn fəaliyyətlərinə nəzarət etmək daha məqsədəuyğundur. İnternetdə uşaq və yeniyetmələrin təhlükəsizliyi problemini həll etmək üçün müxtəlif tədbirlər həyata keçirilir. Bunlara aşağıdakılar aid edilir:

1. İnternetdə olan mövcud təhlükələr barədə uşaq, valideyn və müəllimlərin məlumatlandırılması;
2. proqram-texniki tədbirlərin həyata keçirilməsi;
3. hüquqi səviyyədə tənzimləmə.

Bu məqalədə uşaqların İnternetdə qarşılaşdığı risklər təhlil edilir. İnternet mühitində uşaq və yeniyetmələrin qarşılaşdığı təhlükələrin hüquqi səviyyədə tənzimlənməsinin onların davranışlarına və fəaliyyətlərinə təsir perspektivləri əks olunur. Bir sıra dünya ölkələrində və beynəlxalq təşkilatlarda uşaq və yeniyetmələrin təhlükəsiz İnternet probleminin həlli ilə bağlı qəbul edilmiş qanunlar araşdırılır. Ölkəmizdə bu problemlə əlaqədar qəbul edilən rəsmi sənədlər diqqətə çatdırılır.

Uşaqların İnternet mühitində qarşılaşdığı risklər

Uşaq və yeniyetmələr daha çox sosial şəbəkələr, çatlar, oyun otaqları, onlayn alış-veriş saytları, forum və s. kimi virtual məkanlarda ziyanlı kontentlə üzləşirlər. Bu ziyanlı kontentlər onlar üçün müəyyən təhlükələr yaradır. Bu təhlükələr bir neçə risk qrupuna bölünür. Risk dedikdə təhdidlərin sistemə (obyekt, resurs və ya proses) təsirinin nə dərəcədə təhlükəli olduğu başa düşülür [6]. Ümumi halda təhdid birinin maraqlarına zərər verə biləcək əməliyyat, proses və ya hadisə olmaqla informasiya təhlükəsizliyi sahəsində əsas anlayışlardan biridir.

İnternet təhlükələri ilə bağlı risklər aşağıdakı kimidir:

- məzmunla bağlı risklər;
- elektron (kiber) risklər;
- ünsiyyət və davranışla bağlı risklər;
- istehlakçı riskləri.

Məzmunla bağlı risklər. Bu risklər İnternetdə paylaşılan və uşaqlar üçün qeyri-qanuni, qeyri-münasib hesab edilən məlumatların (mətn, video və audio fayllar) istifadəsi ilə əlaqədardır. Bu məlumatlar təkcə uşaqlar üçün deyil, böyüklər üçün də təhlükəli hesab edilir [6].

Belə kontentləri uyğunsuz və qanunsuz məzmun olaraq iki hissəyə bölmək olar. Uyğunsuz məzmunla ölkənin mədəniyyətinə, mentalitetinə zidd olan və qanunvericiliyə əsasən təsdiq olunmuş qaydada uyğun olmayan materiallar aid edilir. Buraya şiddət, qərəzli məzmun, erotizm və pornoqrafiya, normadan kənar leksika (söyüş, jarqon) ilə danışmaq və irqi ayrı seçkiliyi təbliğ edən materiallar aid edilir. Suisid (intihara cəlb) istiqamətli materiallar, sektant materiallar, partlayıcı maddələrin, narkotik vasitələrin hazırlanması və istifadəsi ilə bağlı informasiyalar məzmunla bağlı risklərə aid olunur [6].

Ölkələrin qanunvericiliklərinə əsasən, müxtəlif materiallar qanunsuz hesab oluna bilər. Bir çox ölkələrdə uşaq və yeniyetmələrlə cinsi əlaqəli materiallar, pornoqrafik məzmun, cinsi zorakılığı təbliğ edən məzmun, ekstremizm və irqçilik, nifrət də daxil olmaqla zorakılıq təsvirlərini

ehtiva edən bu cür məlumatların yayımlanması qadağan edilir və belə məlumatlar qanunsuz hesab olunur.

Elektron risklər. Veb-səhifələri açarkən reklam və pulsuz proqram təminatları avtomatik olaraq kompüterin yaddaşına yüklənir. Fərdi məlumatların açıqlanması, virusların hücumuna məruz qalma, onlayn fırıldaqçılıq və spam elektron risklərə aid edilir [6,7].

Zərərli Proqramlara kompüterdə işləyərkən həm istifadəçinin özünə, həm də istifadə etdiyi kompüterə mənfi təsir göstərən proqramlar (viruslar, casus proqramları, istənilməyən reklam proqramları, zərərli kodun müxtəlif formaları) daxildir [6,7].

Spam reklam materialları yerləşdirilmiş, arzuolunmayan və istənilməyən elektron məktublardır. Belə məktublar istifadəçinin vaxtını və ona sərf edilən İnternet trafikini istismar edir [2,7].

Ünsiyyət və davranışla bağlı risklər. Bu risk qrupuna İnternet istifadəçilərinin qarşılıqlı əlaqələri aid edilir [6,7]. Buraya "qeyri-qanuni əlaqə" və "kibertəhlükəsizlik" (və ya kibertəhqir) daxildir. İnternetdə uşaqlar çox vaxt kibercinayətkarların (pedofillər və s.) qurbanına çevrilirlər. Kiberöküzlük də həmçinin ünsiyyətlə bağlı risklərə aid edilir.

Kiberzorakılıq (kiberöküzlük) - virtual terrorudur (ing.cyberbullying–kiberzorakılıq, bull ingiliscə öküz mənasını verir), tərcümədə bu söz: təcavüzkar hücum, təcavüz, təhqir, təhrik etmək və qəzəbləndirmək mənasını ifadə edir. Bu hücum elektron poçt, ani mesajlaşma, çat otaqları, sosial şəbəkələr, veb-saytlar, eləcə də mobil telefonlar vasitəsilə həyata keçirilir. İnsanlara psixoloji zərər vurur və dörd əsas komponentdən ibarətdir [8]:

- təcavüzkar və mənfi davranışdır;
- müntəzəm olaraq həyata keçirilir;
- iştirakçılar arasında müxtəlif gücə (qeyri-bərabər güc) malik münasibətlər baş verir;
- qəsdən edilən bir davranışdır.

Təzahür formasından asılı olmayaraq kibercinayətkarlıq qurbanına ciddi zərər verər və ən kəskin hallarda faciəli nəticələrə belə gətirib çıxara bilər. Bu davranışlara ciddiyyə alınmayan zarafatlar, psixoloji virtual terror, insanın ölümünə səbəb olan davranışlar (bulisid - zorakılığa görə qurbanın ölümü) aiddir. Belə insanlar həm mesajla öz qurbanını təhqir edir, qurbanın veb-səhifəsini ləğv edir, həm də alçaldıcı məzmunun yerləşdiyi yerlərdə saxta səhifələr yaradır və həmin insanın ünvanına təhqiramiz və əxlaqsız mesajlar yayırlar.

İnternet vasitəsilə fotoşəkillər göndərməklə insanları təqib, təhqir, təcavüz, cinsi təcavüz etmək kimi davranışlar bu fikirlərə aid edilir. İnsanlarda qüsurlu tapmaq, yersiz irad tutmaq, təhrik etmək, əsəbləşdirmək, bəhanə axtarmaq, təngə gətirmək, narahat etmək, şaiyələr yaymaq, ələ salmaq, sataşmaq və aqressiv vəziyyətə gətirmək kimi xüsusiyyətləri də bura əlavə etmək olar.

Kiberzorakılıq həm tamamilə tanımadığımız insanlar, həm də tanışlarımız tərəfindən həyata keçirilə bilər. Hətta bu, qrup şəklində olan insanlar ola bilər ki, onlar bir-birilərini tanıyırlar. Bəzən yeni yaradılmış bir qrup köhnə qrupun təzyiqlərinə də məruz qala bilər.

Təcavüz - təcavüz məqsədilə azyaşlılarla dostluq münasibəti yaradan böyük yaşlı insanların hərəkətidir. Təcavüzkarlar tez-tez uşaqlarla İnternetdə ünsiyyət yaradaraq müəyyən virtual məkanlarda onlarla dostluq münasibətləri qurmağa cəhdlər edirlər. Uşaqlarla şəxsi yazışmalar aparır, onların fərdi məlumatlarını öyrənir və onlarla real həyatda görüşməyə çalışırlar [9].

İnternet-asılılıq problemi İnternetin inkişafından sonra yaranmışdır. Elmi leksikona İ.Qoldberq tərəfindən daxil edilmişdir. Bəzi insanlar virtual aləmə o qədər aludə olurlar ki, onlar günün çox hissəsini - təxminən 18 saatını kompüter qarşısında keçirirlər. Bunun təsiri ilə onların sağlamlığında (gözləri zəifləyir, fiziki görkəmi dəyişir, pinqvinləşir və s.) və psixologiyasında (sosiallaşa bilmir, insanlardan qaçır, daha çox virtual mühitə can atır) ciddi problemlər yaranır. İnternetdən asılılığın ən təhlükəli cəhətlərindən biri belə uşaqların cinayətkarların hədəfinə çevrilməsidir [10].

Uşaq və yeniyetmələrin şəbəkədə daha çox vaxt keçirməsinə səbəb olan və onları asılı vəziyyətə gətirən səbəblərdən biri oyunlarla bağlıdır.

Azartlı oyunlar. İlk kompüter oyunları 1970-ci ildə yaradılmış, həmin vaxtdan başlayaraq əyləncə aləminə daxil olmuşdur. İnternetdə öyrədici xarakterli, intellektual, məntiqi, şəkili, əyləncəli, uşaqların beynini inkişaf etdirən oyunlarla yanaşı, həm də onlara zərər verə biləcək oyunlar vardır. Uşaqların maraqlarını cəlb edən bu oyunlar sonradan ailələrdə bir çox narahatlıqların və maddi problemlərin yaranmasını səbəb olur. Oyunlarda müxtəlif ideyalar təbliğ olunur. Şəbəkədə ideologiya xarakterli oyunlar şiddəti, zorakılığı, dini ayrı-seçkiliyi, İnternetin “diktə” etdiyi mədəniyyətləri təbliğ edir [5,10].

İstehlakçı riskləri. İnternetdə istehlakçı hüquqlarından sui-istifadə istehlakçı risklərinə aid edilir. Keyfiyyətsiz malların alınması riski, müxtəlif saxta məhsullar, bir məhsul və xidmətdən istifadə etmədən pul itkisi, kiberdələduzluq məqsədilə şəxsi məlumatların oğurlanması və s. buraya aid edilir [6].

Kiberdələduzluq istifadəçilərin aldadılması məqsədini daşıyan (gizli məlumatların oğurlanması, köhnə məlumatlardan istifadə, Nigeriya məktubları, fişinq və farming və s.) kibercinayətkarlığın bir növüdür.

Fişinq (ing. “Phishing”) texnologiyası kiberdələduzluğun ən çox yayılmış formasıdır. Hakerlər qanunsuz maddi mənfəət əldə etmək üçün bu texnologiyadan istifadə edirlər. Hər hansı bir fayda əldə etmək üçün insanları aldatmaqla və ya onların inamından sui-istifadə etməklə həyata keçirilən cinayətdir. Mahiyyəti ondan ibarətdir ki, saxta elektron poçta hansısa populyar İnternet qovşağa apararıq hiperkeçid daxil edilir, əslində isə bu istifadəçini görünüşcə rəsmi sayta bənzəyən başqa bir qovşağa aparır. İstifadəçini rəsmi saytda olduğuna inandıraraq onun etimadını qazandıqdan sonra istifadəçi parolunu, kredit kartının nömrəsini və digər məxfi məlumatlarını daxil etməyə yönləndirir. Bu məlumatlar gələcəkdə istifadəçiyə zərər vurmaq üçün istifadə edilir [11].

İnternetdə uşaqlara ziyan verə biləcək risklərin qarşısını almaq üçün yalnız profilaktik tədbirlərin həyata keçirilməsi ilə kifayətlənmək olmaz. İlk növbədə problemin həlli üçün beynəlxalq və ölkədaxili qanunların olması və bu qanunlar əsasında tədbirlərin görülməsi vacibdir.

İnternetdə uşaqların təhlükəsizliyinin təmin edilməsi sahəsində xarici ölkələrin qanunvericilik təcrübəsi

İnternet təhlükələrinin yaratdığı problemlər artmaqda davam edir. Bu vəziyyət yalnız dövlət təşkilatları, səlahiyyətli şəxslərin deyil, cəmiyyətin də diqqətini özünə cəlb edir. Nəticədə, uşaq psixologiyasına, sağlamlığına təsir edən ziyanlı kontentin qarşısının alınması məqsədi daşıyan qanunların qəbul edilməsi zərurəti yaranır.

İnternetdə uşaq təhlükəsizliyi sahəsində beynəlxalq təcrübə son illərdə əhəmiyyətli dərəcədə irəliləmişdir və dünyanın müxtəlif ölkələrində uşaqların kiberməkanda təhlükəsizliyi problemi ilə bağlı yeni qanunlar qüvvəyə minmişdir. Uşaqları mövcud təhlükələrdən qoruma probleminin hüquqi səviyyədə tənzimlənməsi məqsədilə bir çox dünya ölkələrində müəyyən normativ sənədlər tətbiq edilir. Uşaqlara qarşı olan zorakılıqların, aqressiyanın, kibercinayətlərin və s. qarşısının alınması və uşaq təhlükəsizliyinin təmin olunmasına dair ölkələrin milli qanunvericiliyində müxtəlif yanaşmalar tətbiq edilir. Bu qanunların tətbiqi müəyyən dərəcədə cinayət məəcəlləsini, həm də digər məəcəllələri bir neçə prizmadan əhatə edir. Aşağıda uşaqların İnternet təhlükəsizliyi ilə bağlı müxtəlif ölkələrdə qəbul edilmiş normativ sənədlər nəzərdən keçirilir.

Avropa Şurası tərəfindən qəbul edilmiş 2003-cü il tarixli qərarı uşaqların cinsi istismarı və uşaq pornoqrafiyasına qarşı İnternetdə mübarizə aparmaq məqsədi daşıyır. Bu qərar Avropa Birliyinə daxil olan dövlətlər arasında əməkdaşlığın inkişaf etdirilməsinə yönəldilmişdir [12].

Avropa Birliyinə daxil olan ölkələrdə uşaqlara qarşı onlayn cinayətlərin qarşısının alınmasında polislərin ümumi konsensusa gətirilməsinə kömək edən Lanzarote Konvensiyası qəbul edilmişdir. 2013-cü ilin Avropa İttifaqı Direktivində uşaq və yeniyetmələrin virtual mühitdə qorunması üçün müxtəlif ölkələrdəki hüquq-mühafizə orqanlarının bir cəhətdə işləməsinin vacib olduğu qeyd edilir [13].

Uşaqların İnternetdən əldə olunan zərərli informasiyadan mühafizəsi problemi Birləşmiş Millətlər Təşkilatı tərəfindən hər zaman dəstəklənir və bu təşkilata daxil olan qurumların qarşısında qoyulan mühüm məsələlərdən biridir. Uşaqların İnternetin zərərli təsirlərindən qorunması məqsədilə 13 noyabr 2008-ci ildə Beynəlxalq Telekomunikasiya İttifaqı tərəfindən “Kiberməkanda uşaqların müdafiəsi” təşəbbüsü irəli sürülmüşdür [14].

Avropa Birliyi ölkələrində uşaqların onlayn təhlükəsizliyinin təmin edilməsi məqsədilə 1999-cu ildə “Təhlükəsiz İnternet Proqramı” qəbul edilmiş və mərhələli şəkildə həyata keçirilmişdir [15]. Bu proqram uşaq və yeniyetmələr üçün təhlükəsiz onlayn mühitin yaradılmasına yönəlmiş layihələrin maliyyələşdirilməsi, Avropada əhalinin İnternet təhlükələri barədə məlumatlandırılmasına yönəlmişdir. 2013-cü ildən bu proqram “Uşaqlar üçün daha yaxşı İnternet” adı altında öz fəaliyyətini davam etdirir. Əsas məqsədi təhlükəsiz İnterneti təbliğ etmək, xüsusən də gələcək nəsilləri global şəbəkədəki mövcud təhdidlərlə bağlı məlumatlandırmaq, maarifləndirmə işləri aparmaq, uşaq və yeniyetmələr arasında onlayn texnologiyalardan daha təhlükəsiz və məsuliyyətli istifadəni təbliğ etməkdir [16].

2000-ci ilin oktyabrında ABŞ Konqresi tərəfindən “Uşaqların İnternetdə mühafizəsi haqqında” Qanun qəbul edilmişdir. Qanun uşaqları İnternetdə yerləşdirilən cinsi istismar və digər arzuolunmaz materiallardan qorunması məqsədini daşıyır [17]. Eyni zamanda ABŞ Konqresi tərəfindən “İnternetdə uşaqların məxfiliyinin qorunması haqqında” qanun da qəbul edilmişdir. Bu qanun Birləşmiş Ştatların qanunvericiliyinə əsasən 13 yaşına çatmamış şəxslərin və ya təşkilatlarda olan fərdi məlumatların toplanmasına aiddir [18].

27 iyul 2006-cı ildə ABŞ-da “Adam Uolş uşaq mühafizəsi və təhlükəsizliyi aktı” qəbul olunmuşdur. Qanunun qəbul edilməsində məqsəd uşaqları istismar olunmaqdan və zorakı cinayətlərdən qorumaq, uşaq pornoqrafiyasının qarşısının alınmasını bütün səviyyələrdə həyata keçirərək cinsi istismarçıların uşaqlara əlyətənliyinin qarşısını almaqdan ibarət idi [19].

Almaniyada İnternet provayderlər tərəfindən azyaşlı istifadəçiləri qorumaq və ya nifrət və ekstremizm təbliğatını məhdudlaşdırmaq üçün müxtəlif proqram təminatlarından (izləyici, süzgəc və s.) istifadə olunur. 2009-cu ildə ölkədə uşaq pornoqrafiyası yerləşdirilmiş saytların bloklanmasına dair qanun qəbul olunmuşdur, lakin bu qanun İnternetdən azad istifadəni məhdudlaşdırdığına görə 2011-ci ildə rədd edilmişdir [19].

İtaliyada 2006-cı ildə “Cinsi istismar və internetdə uşaq pornoqrafiyası ilə mübarizəyə dair akt” qəbul edilmişdir [20].

2016-cı ilin mayında Belarus Respublikasının “Uşaq hüquqları haqqında” Qanununda müvafiq dəyişikliklər edilmişdir və 1 iyul 2017-ci il tarixindən qüvvəyə minmişdir [21].

2 iyul 2018-ci il tarixdə “Uşaqların sağlamlığına və inkişafına zərər verən məlumatlardan qorunması haqqında” Qazaxıstan Respublikasının Qanunu qəbul edilmişdir [22].

2002-ci ildə Litva hökuməti tərəfindən “Yetkinlik yaşına çatmayanların zərərli ictimai məlumatlardan qorunması haqqında” qanun qəbul edilmişdir [23].

Rusiyanın “Uşaqların sağlamlığına və inkişafına zərər verən məlumatlardan qorunması haqqında” Federal Qanunu 01 sentyabr 2012-ci il tarixdə qüvvəyə minmişdir. 2013-cü ilin iyul ayında Rusiya Federasiyasının İnzibati Məcəlləsinə və “Uşaqların sağlamlığına və inkişafına zərər verən məlumatlardan qorunması haqqında” Federal Qanununa dəyişikliklər qəbul olunub, bu dəyişiklik yetkinlik yaşına çatmayanlar arasında qeyri-ənənəvi cinsi əlaqələrin “təbliğ edilməsi” üçün məsuliyyət yaradır. Rusiya qanunvericiliyinə görə, uşaqların informasiya təhlükəsizliyi - İnternetdə yayılmış məlumatların onların sağlamlığına, fiziki, zehni inkişafına təsir edən və mənəvi cəhətdən zərər verən informasiyalar ilə əlaqəli risklərdən onların qorunmasıdır [24]. Uşaqların bu şəkildə qorunması böyüklərin, xüsusilə də valideynlərin üzərinə informasiya savadlılığı, informasiya mədəniyyəti, mediasavadlılıq və uşaqların fərdi məlumatlarının toxunulmazlığı öhdəliyini qoyur.

Dünyanın bir çox ölkələrində uşaqların ziyanlı informasiyadan qorunmasına dair müxtəlif qanunlar qəbul edilmişdir. Azərbaycan Respublikasında da təhlükəsiz İnternet probleminin həlli ilə bağlı müəyyən tədbirlər həyata keçirilir və bütün bunlar qanunlarda öz əksini tapır.

Azərbaycanda uşaqların informasiya təhlükəsizliyinin təmin edilməsi məsələləri

Ölkəmizdə informasiya təhlükəsizliyinin təmin edilməsinin qanunvericilik bazasının formalaşdırılması və inkişaf etdirilməsi istiqamətində bir sıra mühüm konseptual sənədlər, qanunlar, normativ-hüquqi aktlar qəbul edilmişdir [25-27].

Qəbul olunmuş rəsmi sənədlər arasında uşaqların İnternet mühitində təhlükəsizliyinin təmin edilməsinə dair bir neçə sənəd vardır. Belə ki, “Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya”da “Uşaqların qanunazidd və təhlükəli kontentdən qorunması üçün “təhlükəsiz İnternet” mexanizminin işlənilməsi və tətbiqi” üçün müəyyən tədbirlərin görülməsi nəzərdə tutulur [28].

“Telekommunikasiya haqqında” Azərbaycan Respublikasının Qanununda dəyişikliklər edilməsi barədə 29 aprel 2016-cı il tarixli Azərbaycan Respublikasının Qanununda (34.1.2-1. Uşaqların sağlamlığına və inkişafına ziyan vuran informasiyadan qorunması üçün tədbirlər görülməsini tələb etmək) bu haqda qeyd olunmuşdur [29].

Ümumiyyətlə, ölkəmizdə uşaqların arzuolunmayan məlumatlardan qorunması və İnternet təhdidlərinin qarşısının alınması məqsədilə təklif olunan tənzimləyici çərçivənin olduqca əhəmiyyətli olduğunu qeyd etmək lazımdır. “Uşaqların zərərli informasiyadan qorunması haqqında” Azərbaycan Respublikasının 2018-ci il 30 oktyabr tarixli qanunun 3-cü maddəsində “Uşaqların zərərli informasiyadan qorunması sahəsində əsas prinsiplər” verilmişdir və orada göstərilir ki, “zorakılığın, qəddarlığın, narkotik vasitələrin və psixotrop maddələrin, alkoqollu içkilərin və tütün məmulatlarının, cəmiyyət əleyhinə davranışın, pornoqrafik xarakterli informasiyanın təbliğinin yolverilməzliyi” əsas faktordur. Qanun uşaqların fiziki, zehni və mənəvi inkişafına zərər verən məlumatlardan qorunması üçün qanuni mexanizmləri müəyyən edir [30].

Qanunda uşaqların yaş həddinə görə kateqoriyalara ayrılması onu göstərir ki, uşaqlar üçün nəzərdə tutulmuş informasiya məhsulları hər bir yaşa uyğun olaraq analiz olunmalı və təsnifatlandırılmalıdır. Yaş həddi (0+, 6+, 12+, 16+, 18+) nəzərə alınmaqla uşaqlar arasında dövriyyəsi qadağan edilən informasiyanın növlərinə aşağıda qeyd olunan problemlər aid edilir [29]:

- zorakılığı və qəddarlığı təbliğ edən informasiya;
- cinayətkarlığı təbliğ edən informasiya;
- uşaqların həyat və təhlükəsizliyinə potensial təhlükə yaradan əməlləri təbliğ edən informasiya;
- əxlaqdan kənar leksik (söyüş) məzmunlu informasiya;
- erotik və pornoqrafik xarakterli informasiya;
- qeyri-məişət leksik (jarqon) məzmunlu informasiya;
- qorxu məzmunlu informasiya.

Qanunda uşaqların sağlamlığı, düzgün inkişafı üçün zərərli məlumatlar və onlardan qorunma təqdim olunur. Görülən tədbirlərə baxmayaraq, müasir dövrdə uşaqlar üçün təhlükəli məlumatların yayılması ilə bağlı yeni risklərin artması davam etməkdədir. Uşaqların təhlükəsiz və məsuliyyətli İnternetdən istifadəsi üçün daha çox işlərin görülməsinə ehtiyac vardır və bu məqsədlə uşaqların İnternetdən düzgün istifadəsini təbliğ edən addımlar atılmalıdır.

Uşaqların İnternet təhlükələrindən qorunması sahəsində texnoloji çağırışlar

Rəqəmsal bacarıqlar informasiya cəmiyyəti üçün lazım olan xüsusiyyətlərdəndir. Lakin onun gətirdiyi bir sıra problemlər qaçılmazdır. Araşdırmalardan məlum olur ki, dünyanın hər yerində uşaqların İnternetdə təhlükəsizliyi problemi gündəmədədir. Texnologiyaların inkişaf tempi elektron dövlət mühitində təhlükəsizliyin təmin edilməsi ilə bağlı yeni tələblər yaradır.

İnformasiya təhlükəsizliyi məsələləri milli təhlükəsizliyin əsas tərkib hissələrindən biri olduğuna görə qeyd etmək olar ki, uşaqların İnternet mühitində qorunması məsələləri bu tərkibə daxildir.

Uşaqların informasiya təhlükəsizliyinin təmin edilməsi, uşaq və yeniyetmələrin fiziki, zehni, mənəvi inkişafının qorunması, habelə bütün audiovizual media xidmətləri və elektron mediada insan şəxsiyyətinin, ləyaqətinin qorunması beynəlxalq hüququn tələbidir. Bütün ölkələrdə uşaqların mühafizəsi aktual bir problem kimi diqqəti cəlb edir. Lakin hər ölkədə bu problemlə bağlı fərqli siyasətlər həyata keçirilir.

Baxmayaraq ki, dünyada uşaq və yeniyetmələrin İnternetdən təhlükəsiz istifadə problemlərinə yönəlmiş çoxlu sayda proqram təminatından istifadə olunur. Bu proqramlar vasitəsilə təhlükələrin uşaq psixologiyasına qoyduğu mənfi izlərin sağlması üçün müəyyən addımlar atılır. Həmçinin kibertəhlükələr haqqında istifadəçilərə məlumat verilir. Onlayn təhlükələrdən qorunma üsulları göstərilir və hətta kiberhücumların qurbanlarına psixoloji dəstək də göstərilir.

Tədqiqatlar onu göstərir ki, həm inkişaf etmiş, həm də inkişaf etməkdə olan dövlətlərin əsas problemlərindən biri gənc nəslin İnternet təhlükələrindən qorunmasıdır. Qəbul olunan qanun və sərəncamlar İnternet təhlükələrini tam olaraq aradan qaldırmasa da, müəyyən qədər sağlam sosial mühitin təmin olunmasında əhəmiyyətlidir. Lakin yalnız beynəlxalq və dövlət səviyyəsində qəbul olunmuş qanun və sərəncamlar uşaqların İnternet təhlükəsizliyi üçün kifayət deyildir. Bütün bunlarla yanaşı, uşaqların İnternet təhlükələrindən qorunması üçün intellektual sistemlərə ehtiyac vardır. Bu sistemlər vasitəsilə ziyanlı informasiyanın qarşısının alınması mümkün olacaqdır.

Virtual məkanda uşaqların daha etibarlı şəkildə qorunması məsələlərinə aşağıda göstərilən texnoloji şərtləri də əlavə etmək olar:

1. Qanunlara söykənən dövlət tərəfindən idarə olunan ümumi milli intellektual sistemlərin olması vacibdir;
2. Serverlərə daxil edilən və əsas vəzifəsi uşaqların İnternet təhlükələrindən qorunması olan qoruyucu sistemlər vasitəsilə qanunlarda verilən şərtlər əsasında uşaqların əhəmiyyətli informasiya ilə təmin olunması daha məqsədəuyğundur;
3. Qanunlarda verilən terminlər nəzərə alınmaqla veb-kontentin yoxlanmasında “Vulqar sözlərdən ibarət lüğətin” hazırlanması İnternetdən gələn məlumatların daha keyfiyyətli analizinə imkan verə bilər;
4. Ölkə üçün tətbiq olunan qoruyucu sistemlərdə ölkənin milli xüsusiyyətləri və adət-ənənələr nəzərə alınmalıdır;
5. Ümumi milli intellektual sistemlərin digər dövlətlərdə eyni funksiyaları daşıyan sistemlərlə əlaqəli işləməsi, həmçinin informasiya təhlükəsizliyi məsələləri ilə məşğul olan beynəlxalq təşkilatların imkanlarından səmərəli istifadəsi daha yaxşı nəticə əldə etməyə kömək edəcəkdir.

Uşaq və yeniyetmələrin, ümumiyyətlə cəmiyyətin İnternet təhlükələrindən qorunması məqsədini daşıyan qanun və sərəncamlar uşaqların sağlam böyüməsinə kömək edir. Onların psixoloji və fiziki səviyyədə problemsiz yaşamasını, düzgün tərbiyə olunmasını və sağlam mühitdə sosiallaşmasını təmin edir. Uşaq və yeniyetmələrdə yüksək səviyyədə vətəndaşlıq, vətənpərvərlik hisslərinin aşılmasında böyük rol oynayır və yeni sosial dövlət sisteminin formalaşmasına şərait yaradır.

Nəticə

Hər il yeni-yeni qanun və sərəncamların verilməsinə və cinayətkarlara qarşı müxtəlif cəza tədbirlərinin tətbiqinə baxmayaraq, zərərli məlumatlar İnternet qlobal şəbəkəsi vasitəsilə (elektron oyunlar, qorxu və terrorizmi təbliğ edən cizgi filmləri, videoçarxlar və s.) uşaqlara ötürülür. Bunun təsiri ilə yeni-yeni kiberqurbanların sayı artmaqda davam edir. İnternet təhdidlərinin çoxluğu, kibercinayətlərin sayının artması və eyni zamanda uşaqların təcrübəsizliyi göstərir ki, uşaqları virtual aləmdə arzu olunmayan məlumatlardan qorumaq problemi kompleks yanaşma tələb edir.

Digər tədbirlərlə yanaşı, qanunlar vasitəsilə həyata keçirilən tədbirlər də (kibecinayətkarların qanunla cəzalandırılması) uşaq və yeniyetmələri İnternet təhlükələrindən müəyyən qədər uzaqlaşdırır. Dünya ölkələrində və eləcə də, Azərbaycanda qəbul edilmiş qanunlar vətəndaşları məsuliyyətli olmağa, bu problemin ətrafında sıx birləşməyə çağırır. Valideynlərin üzərinə vəzifələr qoyur. Hər bir uşağı onlayn təhlükələrdən qorumaq üçün valideyn, müəllim, himayədar və digər şəxslər özlərinin informasiya savadlılığını artırmalı və bu təhlükələr barədə məlumatlı olmalıdır. Həmçinin dövlətin, cəmiyyətin və fərdi şəxslərin təhlükəsizliyinə zərər verən kontentlərlə bağlı biliklərə malik olmalıdırlar.

Ədəbiyyat

1. Воробьев Г.А. Безопасность детей и молодежи в современной цифровой среде: угрозы и методы защиты, <http://www.pglu.ru>
2. Global kids online Argentina, <http://www.globalkidsonline.net>
3. Global kids online Serbia, <http://www.globalkidsonline.net>
4. Лаборатории Касперского. <https://www.kaspersky.ru>
5. Ocaqverdiyeva S.S. İnternet mühitində uşaqların təhlükəsizliyinin təmin edilməsi məsələləri // İnformasiya cəmiyyəti problemləri, 2018, № 1. s. 99-107.
6. Котова С.А. Дети в интернете: контентные и коммуникационные риски / Поведение риска: современные направления исследования и профилактики Материалы Международной научно-практической конференции 24 февраля 2012, с. 232-245.
7. Солдатов Г., Зотова Е., Лебешева М., Шляпников В. Интернет: возможности, компетенции, безопасность Методическое пособие для работников системы общего образования, Москва, 2013, 167 ст.
8. Cenat J., Blais M., Lavoie F, Caron P., Hebert M. Cyberbullying victimization and substance use among Quebec high schools students: The mediating role of psychological distress // Computers in human behavior, vol. 89, 2018, pp. 207-212.
9. Samantha C., Sarah B., Elizabeth G.. Sexual grooming of children: Review of literature and theoretical considerations // Journal of Sexual Aggression, 2006, Vol. 12, pp. 287-299.
10. Əliquliyev R.M., Mahmudov R.Ş. İnformasiya asılılığı problemləri və onlarla mübarizə yolları, Ekspress-informasiya, İnformasiya Texnologiyaları nəşriyyatı, Bakı, 2009, 62 s.
11. Hong J. The state of phishing attacks // Communications of the ACM, 2012, vol. 55, №1, pp. 74-81.
12. Child Online Protection, <http://www.itu.int/en/cop/Pages/default.aspx>
13. Directive 2013/34/EU - EUR-Lex - Europa EU, <http://www.eur-lex.europa.eu>
14. Children's Internet Protection Act (CIPA), <https://www.fcc.gov>
15. Safer İnternet programme, <http://www.saferinternet.org>
16. Better İnternet for kids, <http://www.betterinternetforkids.eu/web/portal/home>
17. COPPA - Children's Online Privacy Protection Act, <http://www.coppa.org/coppa.htm>
18. Adam Walsh Child Protection and Safety Act, <http://www.ncsl.org>
19. Internet censorship in Germany, <http://www.en.wikipedia.org>
20. Executive Summary Italy, <https://www.ecpat.org>
21. Закон Республики Беларусь “О правах ребенка”, <http://www.pravo.by>
22. Закон Республики Казахстана “О защите детей от информации, причиняющей вред их здоровью и развитию” (не введен в действие), <http://www.online.zakon.kz>
23. Republic Of Lithuania Law On The Protection Of Minors Against The Detrimental Effect Of Public Information, <http://www.e-eimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.363137>
24. Защита детей от информации, которая может причинить вред их здоровью и развитию, <http://www.pravo.by>
25. “İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında” Azərbaycan Respublikasının Qanunu, <http://www.e-qanun.gov.az/framework/3525>

26. “İnformasiya əldə etmək haqqında” Azərbaycan Respublikasının Qanunu, <http://www.e-qanun.az/framework/11142>
27. “Fərdi məlumatlar haqqında” Azərbaycan Respublikasının Qanunu, <http://www.e-qanun.gov.az>
28. Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya, <http://www.president.az>
29. “Telekommunikasiya haqqında” Azərbaycan Respublikasının Qanununda dəyişikliklər edilməsi haqqında” Azərbaycan Respublikasının Qanunu, 29 aprel 2016-cı il, <http://www.e-qanun.az/framework/32956>
30. “Uşaqların zərərli informasiyadan qorunması haqqında” Azərbaycan Respublikasının Qanunu, <http://www.president.az/articles/30815>

УДК 04:37

Оджагвердиева Сабирә С.

Институт Информационных Технологий НАНА, Баку, Азербайджан
allahverdiyevsabira@gmail.com

О технологических решениях, вытекающих из законодательства о защите детей от интернет-угроз

Сегодня в мире безопасность детей в интернет-среде является одним из важных вопросов информационной безопасности. Каждое государство заинтересовано в том, чтобы иметь более здоровое будущее поколение. В статье анализируются угрозы, с которыми сталкиваются дети в Интернете, а также рассматриваются международные и отечественные меры, нормативные документы и законы, связанные с обеспечением информационной безопасности детей. Определены технологические задачи, вытекающие из соответствующих законодательных актов. Разработаны технологические предложения по принятию эффективных мер для обеспечения защиты детей от вредной информации.

Ключевые слова: безопасность детей, вредная информация, кибернасилие, киберзапугивание, интернет-зависимость, фишинг.

Sabira S. Ojagverdiyeva

Institute of Information Technology of ANAS, Baku, Azerbaijan
allahverdiyevsabira@gmail.com

About the technological duties derived from the legislation in protecting children from Internet threats

Today, safety of children on the Internet environment is one of the important issues of information security in the world. Each state is interested in having healthier and more valuable future generation. The article analyzes the threats faced by children on the Internet and examines the international and domestic measures, normative documents and laws related to the provision of children's information security. The technological duties arising from relevant legislative acts are defined. Suggestions on taking technological measures to ensure efficient protection of children from harmful information are put forward.

Keywords: child safety, malicious information, cyberviolence, cyberbullying, Internet addiction, phishing.