UOT 04:37

Ocaqverdiyeva S.S.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
allahverdiyevasabira@gmail.com

İNTERNET MÜHİTİNDƏ UŞAQLARIN TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ MƏSƏLƏLƏRİ

Məqalədə uşaqların İnternetdə qarşılaşdığı təhlükələr, onların təsnifatı və bu təhlükələrdən qorunması yolları araşdırılır. Uşaqların yaş xüsusiyyətlərindən asılı olaraq rəqəmsal aləmdə davranışları şərh olunur. Beynəlxalq səviyyədə problemin həllinə dair yanaşmalar analiz edilir. Milli təhlükəsiz İnternet mərkəzlərinin fəaliyyəti tədqiq olunur. Azərbaycanda problemin həlli üçün görülən işlər təhlil edilir, müvafiq tövsiyə və təkliflər irəli sürülür.

Açar sözlər: *uşaqların təhlükəsizliyi, kibertəhlükə, İnternet asılılıq, Milli Təhlükəsiz İnternet Mərkəzləri, təhlükəsiz İnternet.*

Giriş

İnformasiya-kommunikasiya texnologiyaları (İKT) çox sürətlə imkişaf edərək, həyatımızın ayrılmaz bir hissəsinə çevrilmişdir. İKT-nin ən perspektivli sahələrindən biri olan İnternet insanların bir-biri ilə daha tez və asan əlaqə yaratdığı, eyni zamanda, informasiya mübadiləsi apardığı bir məkandır. İnternetdə *WEB 2.0* platformasının tətbiqi öyrənmə, yaradıcılıq və sosial ünsiyyət üçün imkanları əhəmiyyətli dərəcədə genişləndirmiş və çoxlu sayda sosial şəbəkələrin yaranmasına səbəb olmuşdur. Bu isə daha çox istifadəçiləri (ilk növbədə isə, uşaq və yeniyetmələr arasındaa) İnternetə cəlb etmişdir. Cəmiyyətin qorunmağa daha çox ehtiyaacı olan təbəqəsinin – uşaq və yeniyetmələrin İnternetdən geniş istifadəsi onların informasiya təhlükəsizliyi ilə bağlı bir çox problemlərin yaranmasına səbəb olmuşdur [1].

Qlobal şəbəkədə ziyanlı məlumatlarla zəngin səhifələrin mövcud olması uşaqların cinsi istismarına, aqressiyanı və zorakılığı təbliğ edən mətnlərlə rastlaşmalarına gətirib çıxarır. Onlar İnternetdə aldadılır, zorakılığa məruz qalır, qeyri-etik davranışla qarşılaşır, texniki və sosial-psixoloji təhdidlərlə üzləşirlər. Beləliklə, onlar kibercinayətkarların qurbanına çevrilirlər.

İnternet uşaqları yaxınlarından uzaqlaşdırır, ailələrin tərbiyə etdiyi kimi deyil, virtual aləmin "diktə" etdiyi kimi hərəkət etməyə sövq edir. Uşaqlar ətrafa qlobal aləm kimi yanaşaraq kosmopolit düşüncələrlə yaşayırlar. Bu proses gənclərin dünyaya baxışlarını dəyişərək onlarda vətənsizləşmə hissləri yaradır. Qlobal şəbəkədən aldığı məlumatlar birbaşa azyaşlı istifadəçinin şüuruna təsir edir, müxtəlif cəmiyyətə, həyat tərzinə rəğbət oyadır, ürəkaçan, "xoşbəxt bir mühiti, yaxud vərdişləri" təbliğ edir. Bu isə bir növ uşaqlarda "beyin yuyulması" (*ing.brain wash*) işini həyata keçirir [2].

Məqalədə virtual mühitdə uşaqların təhlükəsizliyinin təmin edilməsi ilə əlaqəli beynəlxalq səviyyədə problemin həllinə olan yanaşmalar şərh edilir. Milli təhlükəsiz İnternet mərkəzlərinin fəaliyyəti və onların apardıqları siyasətlər, uşaqların İnternet mühitində qarşılaşdığı təhlükələr və onların həlli yolları araşdırılır.

Uşaqların İnternetdə qarşılaşdığı təhlükələrin təsnifatı

İnternet istifadəsi zamanı uşaqların həm şəxsi təhlükəsizliyinə, həm də istifadə etdikləri kompüterin təhlükəsizliyinə yönəlmiş müxtəlif təhlükələrin baş verməsi mümkündür. Bu təhlükələri aşağıdakı kimi təsnifatlandırmaq olar:

- ✓ cinayətkarların hədəfinə çevrilmə;
- ✓ zərərli informasiya ilə məlumatlandırma;
- ✓ İnternet-asılılıq;
- ✓ zərərli oyunlar;
- ✓ *Phishing* texnologiyası;

- ✓ zərərli proqramlar.

Cinayətkarların hədəfinə çevrilmə. İnternetdə ünsiyyət virtual şəxslə qurulduğundan iştirakçılar fiziki olaraq təqdim olunmurlar, yəni virtual aləmdə müxtəlif şəkildə təqdim edilirlər. Cinayətkarlar uşaq psixologiyasını, maraqlarını, yaşa uyğun tələblərini öyrənir, onlara diqqət, qayğı və mehribanlıq göstərir, onlarla "dostluq" münasibətləri qurur, öz planlarını həyata keçirməyə çalışır və daha çox uşaqlarla real həyatda görüşməyə cəhd edirlər. Aparılan bir sorğunun nəticələrinə görə, İnternet istifadəçisi olan 9-16 yaş aralığındakı uşaqların 30%-i əvvəlcədən tanımadıqları insanlarla real həyatda görüşdüklərini və bunun riskli, amma əyləncəli olduğunu söyləmişlər. 9-10 yaş aralığındakı uşaqlar isə virtual aləmdə nə qədər yaxın münasibət qursalar da, real aləmdə görüşməkdən ehtiyat etdiklərini və hətta belə görüşə gedənlərin 31%-i bundan narahat olduqlarını bildirmişlər [2].

Zərərli informasiya ilə məlumatlandırma. Zərərli informasiya yerləşdirən şəxslər İnternet üzərindən dini, irqi, milli, sosial nifrəti aşılayan, cinsi istismar xarakterli informasiya yayırlar. Buraya narkotikdən istifadə və onun hazırlanmasına, müxtəlif zərərli və partlayıcı maddələrin ev şəraitində düzəldilməsinə, terrora təhrik etməyə dair məlumatlar aid edilir [3]. Veb-səhifələrdə çağırış xarakterli videoçarxlar, filmlər yerləşdirərək yeniyetmələri terrorçu qruplara cəlb edə, diqqət çəkən reklam çarxı, qeyri-etik, jarqon ifadələr, pis vərdişlər uşaq maraqlarını tamamilə qeyri-sağlam bir mühitə cəlb edə bilər.

İnternet-asılılıq. Bəzi uşaqlar bütün günü şəbəkələrdə oyun oynamaqla, informasiya axtarışı ilə məşğul olurlar [4]. Onların texnologiyaya olan həddsiz marağı özlərinin sağlamlığını və psixologiyasını korlayır. Saatlarla vaxtını kompüter arxasında keçirən uşaq fiziki olaraq dəyişir, dayaq-hərəkət sistemi pozulur və bu, müxtəlif xəstəliklərin yaranmasına səbəb olur, onlar fiziki görünüşcə sanki "pinqvinləşirlər".

Yaxın məsafədən kompüterin ekranına baxmaq göz fokusunu pozur. Nəticədə istifadəçi göz sağlamlığını itirir. Digər tərəfdən, bu maraqlar daha da dərinləşərək onları İnternetdən asılı vəziyyətə salır. İnternetdə informasiya asılılığına məruz qalanlar müxtəlif kibercinayətlərin həm obyekti, həm də subyekti kimi çıxış edə bilərlər [5].

Uşaqların virtual aləmdə olan "tanışları" və "dostları" ilə hər gün ünsiyyət qurması və interaktiv oyunlara aludəçiliyi onları zaman, məkan, reallıq hisslərindən uzaqlaşdırır, ətrafdakılara qarşı inamsızlıq yaradır, gündəlik rejimləri pozulur və dərslərini zəif oxuyur. Onlar bu aləmə o qədər aludə olurlar ki, kompütersiz özlərini depressiyada hiss edir və ondan asılı vəziyyətə düşürlər. İnternet asıllığı artıq bir çox ölkələrdə xəstəlik kimi qəbul edilmişdir [6].

Valideyn övladını İnternetdən asılı vəziyyətdən qurtarmaq üçün mütləq idman, rəsm və s. sahələrdə uşağın istedadını inkişaf etdirərək onu bu vəziyyətdən xilas edə bilər. İnternetdən asılı vəziyyətə düşməmək üçün uşaqların informasiya mədəniyyəti formalaşmalı, onlara informasiya ilə davranış normaları aşılanmalıdır [7].

Zərərli oyunlar. İnternetdə uşaqların təfəkkürünü inkişaf etdirən öyrədici xarakterli, intellektual, məntiqi, şəkilli, əyləncəli, oyunlarla yanaşı, həm də onlara zərər verə bilən oyunların olması gənc nəslin tərbiyəsinə və sağlamlığının pozulmasına təsir edir [8].

Zərərli oyunlardan danışarkən, həqiqi pullarla oynanılan qumar oyunlarını qeyd etmək olar. İdeologiya xarakterli oyunlar isə şiddəti, zorakılığı, dini, irqi ayrı-seçkiliyi təbliğ edir, uşaq və yeniyetmələri öz təsiri altına alaraq, onları aqressiv hərəkətlər etməyə yönəldir, onların gələcəkdə cinayətkar kimi yetişmələrinə və s. pis vərdişləri mənimsəmələrinə səbəb olur [9]. Oyunlar istifadəçiyə mütləq bir mesaj verir, yad mədəniyyətləri təbliğ edir, gənc nəsli milli dəyərlərdən, öz xalqının adət-ənənələrindən uzaqlaşdırır.

"Balıqovu"(ing.Phishing) texnologiyası. Başqa bir təhlükə də İnternet dələduzları tərəfindən istifadə edilən "Balıqovu" texnologiyasıdır [10]. Hakerlər tərəfindən yaradılmış bu metod istifadəçini saxtakarlıqla düzəldilmiş e-poçt məktubunu açmağa həvəsləndirir. İstifadəçi elektron poçtda olan linki seçməklə zərərli proqramları aktivləşdirir və hakerlər bundan istifadə edərək bilavasitə şəxsi məlumatları öyrənir. Virtual dələduzlar kompüter istifadəçilərini aldadaraq, kredit

kartı nömrələrini, parol və şifrələri, hesab nömrələrini, İnternet bankçılığında istifadə olunan istifadəçi kodu və şifrələri əldə edərək istifadəçilərə ziyan vururlar.

Zərərli proqramlar. Məlumdur ki, veb-səhifələri açarkən avtomatik reklam və pulsuz proqram təminatları yaddaşa yüklənir. Bu proqramlara misal olaraq parolları oğurlayan, "arxa-qapı" (*ing. back-door*), klaviatura-casus proqramlarını, "troya atları"nı və s. göstərmək olar. Kompüter virusları da bu cür təhlükəli proqramlardandır. Hakerlər tərəfindən *MSWord, MS Excel* və s. üçün makroviruslar, yükləmə virusları, skript viruslar, skript troyanları və s. kimi hər gün yüzlərlə zərərli proqram təminatı yaradılır. Bu proqramlar istifadəçinin kompüterinə ziyan vura, informasiyanı korlaya, yaxud tamamilə məhv edə bilər.

Təhlükələrin texnoloji səviyyədə qarşısının alınması üsulları

Ziyanlı informasiyanın və bilavasitə azyaşlı İnternet istifadəçisinə yönəlmiş təhlükələrin qarşısının alınması məqsədilə müxtəlif texnoloji üsullardan, mexanizmlərdən və proqram vasitələrindən istifadə olunur. Ziyanlı informasiya ilə mübarizə aparmaq üçün kontent filtrasiyası tətbiq edilir. Bu metod həm şirkətlər, həm də ailələr tərəfindən istifadə edilir [11].

Microsoft şirkəti *Windows 7* əməliyyat sistemindən başlayaraq, valideynlərə uşaqların İnternetdə zərərli saytlardan müdafiəsinə və onları nəzarətdə saxlamağa imkan verən *"Windows Family Safety"* adlı proqram təminatı hazırlamışdır. Bu proqram vasitəsilə valideynlər İnternetdən istifadə zamanı bir sıra saytlara qadağalar qoya və məhdudiyyətləri tənzimləyə bilirlər [12].

Windows ailəsinə məxsus olan *Windows 10*-dan əvvəlki əməliyyat sistemlərində təhlükəsizliklə bağlı məsələlər əlavə yazılan proqram təminatı vasitəsilə həyata keçirilirdi. *Windows 10* əməliyyat sistemində isə bu problem mövcud deyil və sistemin üzərinə inteqrasiya olunmuş "*Windows Hello*" kimi proqramlardan istifadə olunur.

Sürətli informasiya mübadiləsi və eyni zamanda, şəbəkəyə tez-tez daxil olma kompüterdə virusların aktivləşməsinə səbəb olur. Viruslardan müdafiə ilə yanaşı, həm də filtrləməyə böyük ehtiyac yaranır. *McAfee, Norton, Avg* kimi məşhur antivirus proqramları, həm də filtrləmə funksiyalarını yerinə yetirir.

McAfee Family Protection və *Norton Family* tipli proqramlar vasitəsilə də uşaqlar üzərində valideyn nəzarəti təmin oluna bilər. Bu proqramlar aşağıdakı funksiyaları yerinə yetirirlər:

- ✓ veb-saytların filtrlənməsi;
- ✓ sosial şəbəkələrin filtrlənməsi;
- ✓ axtarış saytlarının filtrlənməsi;
- ✓ məlumatın göndərilməsinə və qəbul olunmasına nəzarət;
- ✓ onlayn alış-satış məsələlərinin təhlükəsizliyi və s.

Kaspersky Lab şirkətinin mütəxəssisləri tərəfindən 2015-ci ilin əvvəlində aparılmış monitorinqin nəticələrinə görə, 2014-cü il ərzində istifadəçilər tərəfindən kompüterlərə İnternet təhdidləri əleyhinə istifadə edilən "Valideyn İdarə Modulu" (*ing. Parental Control module)* yenidən tətbiq edilmişdir [13]. Əsas məqsəd uşaqların İnternetdə üzləşdikləri təhdidləri müəyyən etmək və təhlükənin əsas mənbəyini üzə çıxarmaq idi. Proqramın tətbiqi nəticəsində aşağıdakı nəticələr əldə olmuşdur:

- "Valideyn İdarə Modulu" il ərzində ən azı bir dəfə *Kaspersky Lab* istifadəçisi tərəfindən tətbiq edilmişdir və orta hesabla 127 dəfə işlədilmişdir;
- İnternetdə azartlı oyunlar oynamağa meylli olanların dörddə birindən çoxu (26,6%) və hər beş istifadəçidən biri saytların bu cür xüsusi "silahlarına" qarşı çıxa bilmir və tələyə düşür;
- İstifadəçiləri İnternet təhlükələri ilə daha çox qarşılaşan ölkələr arasında Rusiya, Hindistan və Çin ilk üçlükdədir. Çin, ABŞ, Almaniya, İngiltərə və Rusiya isə belə təhlükələrə qarşı "Valideyn İdarə Modulu"-nu ən çox və tez-tez tətbiq edən ölkələrdir.

Uşaqların İnternetdə üzləşdikləri təhdidləri aydınlaşdırmaqla və əsas mənbələrini üzə çıxarmaqla onların təhlükələrə nə qədər yaxın olmasını müəyyən etmək olar.

Uşaqların yaş psixologiyası və rəqəmsal mühitdə davranışları

Uşaqların İnternetdə qarşılaşdığı təhlükələrlə bağlı aparılan araşdırmalara görə, qlobal şəbəkədən istifadə zamanı onların əksəriyyətinin öz təəssüratlarını valideynləri ilə deyil, dostları, yaşıdları ilə bölüşdüyü məlum olmuşdur. Təhlükələrlə qarşılaşmış uşaqların yarıdan çoxu isə bu mövzu barəsində heç kimlə fikir mübadiləsi aparmır. Uşaqların İnternetdən istifadəsi real həyatda olduğu kimi onların yaş qruplarına görə fərqlidir. İstər sosial şəbəkələrdə, istərsə də virtual əşyalarla münasibətdə bu fərqlər özünü göstərir. Mütəxəssislər İnternetdən istifadə edən uşaqları aşağıdakı intervallar üzrə yaş qruplarına bölürlər [15]: 7 yaşadək; 10-13 yaş; 14-17 yaş. Müəyyən yaş qruplarında uşaqların İnternetdə hansı təhlükələrlə qarşılaşdığını nəzərdən keçirək.

7 yaşadək uşaqların İnternet təhlükəsizliyi. Bu yaşda uşaqlar oyunları daha çox sevir və virtual əşyalardan istifadə etməyi yaxşı bacarırlar. Onlar oxumağı, yazmağı yeni öyrəndikləri üçün saytlarda axtarış apara bilmir, İnternetə yalnız valideynlərinin iştirakı ilə daxil olurlar.

7-10 yaş arası uşaqların İnternet təhlükəsizliyi. Mütəxəsislərin fikrincə, bu yaş qrupunda olan uşaqların yaş psixologiyasından asılı olaraq, onlar yalnız özləri istədikləri işləri görməyi xoşlayırlar. Bu yaşda olan uşaqlar texnologiyanı sürətlə öyrənir, onlarda valideynlərinin icazə vermədikləri saytlara, çatlara baxmaq, qeyri-etik videoçarxları, zərərli və təhlükəli faylları, proqramları yükləmək istəyi güclü olur. İnternetdə "dost" axtarışında olduqlarında təhlükəli şəxslərlə və cinsi istismarçılarla qarşılaşma ehtimalı da yüksək olur. Valideynlər onların informasiya təhlükəsizliyinin təmin edilməsi məqsədilə və uşaqların iştirakı ilə "Ağ siyahı" tərtib etməlidir. "Ağ siyahı" uşağın yaşına uyğun saytların siyahısıdır, belə ki, onlar məhz uşağın təhlükəsizliyinin təmin olunması üçün nəzərdə tutulub.

10-13 yaş arası uşaqların İnternet təhlükəsizliyi. Bu yaş qrupundan olan uşaqlar İnternet və orada mövcud olan informasiya haqqında məlumatlıdırlar. Həmin informasiyanı əldə etmək, oxumaq və eşitmək istəyi güclü olur. Bu yaşda uşaqlar İnternetdən ən çox dərslərini hazırlamaq məqsədilə istifadə edirlər. Uşaqlar şəbəkə oyunları oynayır, kompüterdən asılı ola bilirlər [16]. Bu məqsədlə onların kompüterdə işləmə müddəti valideyn tərəfindən müəyyən edilməlidir. İnternetə qoşulmuş kompüterin ümumi otaqda valideyn nəzarətində olması və valideyn nəzarəti proqramının kompüterə yazılması vacibdir.

14-17 yaş arası uşaqların İnternet təhlükəsizliyi. Bu yaş qrupundan olan uşaqlar valideynlərindən daha çox İnternetlə ünsiyyətdə olurlar, onlara nəzarət etmək valideyn üçün artıq xeyli mürəkkəbləşir. Ona görə də, valideynlə övlad arasında İnternet təhlükəsizliyi qaydalarına riayət etmək barədə bir növ razılaşma olmalıdır. Bu yaşda olan yeniyetmələr axtarış sistemlərindən, elektron poçtdan, mesajların ani mübadilə sistemlərindən aktiv istifadə edir, musiqi və filmlər yükləyir, oyunlar oynayır və s. Müvafiq yaş kateqoriyasına aid olan oğlanlar hər şeylə maraqlanır, qızğın oyunlara, yaşa uyğun olmayan şəkillərə baxmağa üstünlük verirlər. Qızlar isə daha çox çatda ünsiyyət yaratmağa, yaşlarına uyğun olmayan mövzulara aid məlumatlara üstünlük verirlər [16].

Valideynlər onların İnternet fəaliyyəti haqqında hesabatlarını nəzərdən keçirməlidirlər. Onlara spamdan qorunma yollarını göstərməlidirlər. Valideynlər yeniyetmənin həqiqi elektron ünvanını İnternetdə qeyd etməsini, arzu olunmayan məktublara cavab verməməsini və xüsusi poçt süzgəclərindən istifadə etmələrini tövsiyə etməlidirlər. Yeniyetmənin ziyarət etdiyi saytlar ilə valideyn mütləq tanış olmalıdır.

Uşaqlara İnternetdən istifadə etməyi tamamilə qadağan etmək olmaz. Valideyn bunu qadağan etməkdənsə, uşaqlara nəyin zərərli, nəyin zərərsiz olduğunu izah etməli və ondan hansı müddətdə, necə istifadə etməyi başa salmalıdır.

Milli təhlükəsiz İnternet mərkəzlərinin təhlükəsizlik siyasəti

İnternetdə təhlükəsizliyin təmin olunması və eyni zamanda ,bu mühitin az təcrübəli üzvü olan uşaqlara yönəlmiş kibertəhlükələrin qarşısının alınması problemi dünyanın bir çox dövlətlərini, əlaqədar təşkilatlarını narahat edən vacib məsələlərdən biridir. Avropa Birliyi (AB) İnternet mühitinin bütün sahələrində uşaqların mühafizəsini dəstəkləyir və təhlükələrin qarşısının alınması üçün uyğun siyasət həyata keçirir. 1999-cu ildə Avropa Komissiyası tərəfindən "Təhlükəsiz İnternet Proqramı" (*ing. Safer İnternet Programme*) hazırlanmış və 2009-2013-cü illəri əhatə etmişdir [17]. Proqram 2013-cü ildən başlayaraq "Uşaqlar üçün daha yaxşı İnternet" (*ing. Better Internet for Kids*) adı altında fəaliyyət göstərir.

Proqram çərçivəsində təhlükəsizlik siyasəti AB-yə daxil olan ölkələrdə yaradılan Təhlükəsiz İnternet Mərkəzləri (TİM) vasitəsilə həyata keçirilir. Avropada əhalini İnternetdə olan təhlükələr barəsində məlumatlandırmaq məqsədilə *"İnsafe"*(Təhlükəsizlikdə) Təhlükəsiz İnternet Mərkəzləri Şəbəkəsi (TİMŞ) yaradılmışdır [17]. Buraya Avropanın 31 ölkəsində fəaliyyət göstərən TİM-lər daxildir. Adətən, TİM-lərin tərkibinə aşağıdakı xidmətlər daxil edilir [17]:

Maarifləndirmə mərkəzləri (*ing.Awareness Centre*) – səlahiyyətli insanları, valideynləri, himayədarları və müəllimləri uşaq və yeniyetmələrin İnternetdən istifadəsi zamanı yaranacaq potensial risklərlə bağlı məlumatlandırır və onların təhlükəsizliyini təmin edir [17].

Gənclik Panelləri (ing.Youth Panel) – bu qrup böyük yaşlı və İnternetdə olan təhlükələr barəsində məlumatlı olan gənclərdən təşkil olunmuşdur. Qrup üzvləri ölkədəki Milli İnternet şəbəkəsinin liderləri ilə görüşlər təşkil edir, səlahiyyətli şəxslərin diqqətini bu məsələlərə cəlb edərək onların məsləhət və təcrübələrindən bəhrələnirlər. Onlar İnternetin faydalı və ziyanlı tərəfləri ilə bağlı videoçarxlar, dərs vəsaitləri və s. hazırlayırlar [17].

Gənclik Panellərinin üzvləri hər il ənənəvi olaraq hər bir TİM və Ümumi Avropa Gənclik Panelinin (*ing. Pan-European Yoth Panel*) üzvlərini forumda iştirak etmək üçün dəvət edirlər. Bu tədbirdə 12–18 yaş arası gənclər, Maarifləndirmə mərkəzinin üzvləri, biznes nümayəndələri, siyasətçilər və digər maraqlı tərəflər mediadan istifadə ilə bağlı müxtəlif məsələləri müzakirə edir, rəqəmsal məsələlərlə bağlı məlumatlandırmalar aparırlar.

Yardım xətləri (ing. Helpline) – yardım xətləri "*İnsafe*" təşkilatı tərəfindən koordinasiya edilir. Onlar İnternetdə uşaqların təhlükəsizliyin təmin olunması ilə bağlı uşaq və yeniyetmələri, valideynləri, müəllimləri və himayədarları fərdi qaydada məlumatlandırırlar [17].

Qaynar xətlər (ing. Hotline) – insanlardan qanunazidd kontent (terrora cəlb edilmə, vandalizm və nifrət yaradan materiallar, narkotik vasitələrinin qeyri-qanuni istifadəsi və s.) və uşaqların cinsi istismarı ilə bağlı konkret faktlar haqqında məlumatları qəbul edirlər. Qanunazidd kontent aşkarlandıqda qaynar xətlər tərəfindən ölkənin hüquq-mühafizə orqanlarına, eyni zamanda, İnternet xidməti provayderinə məlumat verilir və prosedur qaydalarına uyğun ölçü götürülür. Əgər qanunazidd kontent başqa bir ölkədə saxlanılırsa, bu haqda həmin ölkənin qaynar xəttinə məlumat verilir [17].

Mərkəzlər 2004-cü ildən başlayaraq ənənəvi olaraq ildə bir dəfə onlayn təhlükəsizlik üzrə Təhlükəsiz İnternet Forumunu təşkil edir, hər il fevral ayının ikinci çərşənbə axşamı "Təhlükəsiz İnternet Günü"nü (*ing. Safer Internet Day*) qeyd edərək, dövlət qurumlarını, kütləvi informasiya vasitələrini, qeyri-hökumət təşkilatlarını, ictimaiyyəti və s. bir araya gətirirlər. Qaynar xətlər Beynəlxalq Qaynar Xətlər Assosiasiyası tərəfindən (*ing. INHOPE*) *www.inhope.org* saytı vasitəsi ilə koordinasiya edilir [18].

Avropada nümunəvi MTİM-dən biri Böyük Britaniyanın Təhlükəsiz İnternet Mərkəzidir [18]. Mərkəz 3 təşkilatla tərəfdaşlıq quraraq maraqlı layihələr həyata keçirir:

- Təhsil üçün Cənub-Qərb şəbəkəsi (*ing. South West grid for learning*) – İnternetdən istifadəni öyrədir və müəllimlərlə işləyir;
- Uşaq şəbəkəsi (*ing. Childnet*) – İnternet mühitində təhlükəsizliyin təmin edilməsini öz fəaliyyətində missiya kimi qəbul edir;

- İnternet İzləmə Fondu (*ing.İnternet Watch Foundation, IWF*) – Qaynar xətt kimi fəaliyyət göstərir və kriminal kontentlərlə mübarizə aparır.

Mərkəz İnternetin və digər texnologiyaların təhlükəsiz istismarı ilə bağlı böyük miqyaslı təbliğat həyata keçirərək, ölkədə uşaqlara təhlükəsiz elektron mühitin yaradılması üçün peşəkarları işə cəlb edir, onlayn kriminal kontentlərə qarşı ölkə miqyasında əməliyyatlar aparır, "Təhlükəsiz İnternet" gününün təşkilinə cavabdehlik daşıyır, uşaqlar, valideynlər, himayədarlar və müəllimlər üçün onlayn resurslar hazırlayır.

Böyük Britaniyanın MTİM-i maraqlı layihələr həyata keçirir, müxtəlif yaş qrupundan olan uşaqlara, valideyn və himayədarlara, eyni zamanda, müəllimlərə təlimatlandırıcı məlumatlar verir. Mərkəz ölkənin 4 İnternet provayderi ilə əldə etdiyi razılığa əsasən, təklif edilən "ailə nəzarəti" paketlərinin tətbiqetmə və onlara qoşulma üsullarını təbliğ edərək, istifadəçilərə qurğularda təhlükəsizlik məsələlərinə dair tövsiyələr və resurslar təklif edir, peşəkarların təcrübəsindən bəhrələnir.

Almaniyada MTİM 2008-ci ildə yaradılmışdır. MTİM-də həm uşaqlar, həm də valideynlər üçün nəzərdə tutulmuş yardım xətti, iki qaynar xətt (*www.internet-beschwerdestelle.de* və *www.jugendschutz.ne*), maarifləndirmə mərkəzi (*alm. Klicksafe*) və gənclərlə iş mərkəzi fəaliyyət göstərir. Mərkəz valideyn, himayədar, müəllimlər və müxtəlif yaş qruplarından olan uşaqlarla iş aparır və uşaqların hüquqlarını qoruyur [19].

Rusiyada 2008-ci ildən MTİM İnternet Texnologiyaları Regional İctimai Mərkəzi, "*Ангел*" Koalisiyası və insan hüquqları hərəkatı konsorsiumu olan "*Сопротивление*" Rusiyanın qeyri-hökümət təşkilatlarının dəstəyi ilə fəaliyyətə başlamışdır. Mərkəz Rusiya Mülki Palatası və Uşaq Ombudsmanı idarəsinin rəhbərliyi tərəfindən dəstəklənir [20].

Rusiya MTİM-in arxtekturuna, başqalarında olduğu kimi, yardım xətləri, qaynar xətlər, maarifləndirmə mərkəzi, gənclərlə iş xidmətləri daxildir. Mərkəz öz veb səhifəsində uşaq və yeniyetmələrlə iş apararaq, kibertəhdidlərin müxtəlif növləri haqqında Rusiyanın aparıcı ekspert və analitiklərinin şərhini verir və istifadəçilərə konsaltinq xidmətləri göstərir.

Yuxarıda qeyd olunan TİM-lərin hər biri TİMŞ-ə qoşulmuş 31 Təhlükəsiz İnternet Mərkəzi ilə əlaqəli işləyir. Hər il fevral ayında "Təhlükəsiz İnternet günü"nü qeyd edir, forumlarda iştirak edərək birgə informasiya və təcrübə mübadiləsini həyata keçirir, hesabatlar hazırlayır və sosial sorğular keçirməklə daha yaxşı təhlükəsiz İnternet mühitinə nail olmağa çalışırlar.

Azərbaycanda uşaqların İnternetdə təhlükəsizliyi sahəsində görülən işlər

Ölkəmiz bütün sahələrdə olduğu kimi, uşaqların İnternetdə təhlükəsizliyi probleminin həll olunması məsələsində də dünyada gedən proseslərdən geri qalmır. Son illər İnternetdə uşaqların təhlükəsizlik problemi cəmiyyətin, dövlətin və səlahiyyətli şəxslərin diqqətini cəlb etməkdədir.

Azərbaycan Respublikası Prezidentinin 2 aprel 2014-cü il tarixli sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya"da informasiya təhlükəsizliyinin təmin edilməsi, elektron mühitdə yarana biləcək təhlükələrin qarşısının alınması bir istiqamət kimi müəyyən edilir. Milli Strategiyada nəzərdə tutulmuş "Uşaqların qanunazidd və təhlükəli kontentdən qorunması üçün "təhlükəsiz İnternet" mexanizminin işlənilməsi və tətbiqi" ölkəmizdə uşaqların elektron mühitdə təhlükəsizliyinin təmin edilməsinə dair görüləcək işlərə təkan verir [21].

2008-ci ildə Azərbaycan İnternet Forumu, Təhsil Nazirliyi və *Microsoft* şirkətinin Azərbaycandakı nümayəndəliyi tərəfindən "Uşaqların İnternetdə Təhlükəsizliyi" adlı layihə həyata keçirilmişdir. Layihənin məqsədi uşaqların İnternetdə təhlükəsizliyi və onların zərərli informasiyalardan qorunması ilə bağlı müəllimlər, valideynlər və uşaqlar üçün metodiki-informasiya dəstəyi göstərməkdən, ictimaiyyətin diqqətini bu problemə cəlb etməkdən ibarət olmuşdur [22].

2012-ci ildən başlayaraq İnternet-servis-provayderi "*Sazz*" *AzEduNet* təhsil şəbəkəsi ilə birlikdə "Məktəblilər üçün təhlükəsiz İnternet" layihəsi həyata keçirir. Layihənin məqsədi elektron

mühitdə uşaqları arzuolunmaz kontentdən – zorakılığı, ekstremizmi, ədəbsiz leksikanı özündə saxlayan resurslardan müdafiə etməkdir [2].

Azərbaycan Nəqliyyat, Rabitə və Yüksək Texnologiyalar Nazirliyinin (RYTN) dəstəyi ilə Azərbaycan Respublikası Təhsil Nazirliyi tərəfindən təhsil müəssisələrində filtrasiya sistemi tətbiq edilmiş, cəmiyyətdə informasiya təhlükəsizliyi ilə bağlı maarifləndirici tədbirlər və bəzi məktəblərdə treninqlər keçirilmişdir [2].

Müəyyən qurumlar tərəfindən həyata keçirilən tədbirlərin məqsədi Azərbaycanda yaşayan uşaqların İnternet mühitində olan təhlükələrdən xəbərdar olması və kiberməkanda olan cinayətkarlarla qarşılaşmasına mane olmaqdan ibarətdir.

Nəticə

İnternetdə uşaqlar real həyatda olduğundan daha müdafiəsizdirlər. Valideynlərin üzərinə düşən ilk vəzifə özlərinin kompüter savadlılığı və İnternetin resurslarından istifadə bacarıqlarını artırmaqdır. Uşaqları İnternetdəki təhlükələrdən qorumaq üçün onların istifadə etdikləri kompüterlərə "ailə nəzarət sistemləri", antivirus proqramları yazılmalı, uşaqların müəyyən kontentlərə çıxışı məhdudlaşdırılmalıdır.

Azərbaycanda MTİM-in yaradılması həlli vacib olan məsələlərdən biridir. Artıq kibertəhlükəsizlik üzrə maarifləndirmənin aparılmasına, informasiya və texnologiyalardan təhlükəsiz istifadə mədəniyyətinin yüksəldilməsinə ehtiyac duyulur. Cəmiyyətdə kibertəhlükələr haqqında maarifləndirmənin aparılması, yardım və qaynar xətlərin yaradılması, uşaqların qanunazidd və təhlükəli kontentdən qorunması üçün mexanizmlərin işlənilməsi bu sahədə görüləcək ilk işlərdən biri olmalıdır.

İnternetdəki təhlükələrdən qorunmaq üçün ailə-məktəb-dövlət əməkdaşlığı kompleks şəkildə fəaliyyət göstərməli və bununla bağlı müxtəlif tədbirlər həyata keçirilməlidir. Bunlara aşağıda sadalanan tədbirləri aid etmək olar:

- KİV vasitəsilə İnternetdəki təhlükələrin uşaq və yeniyetmələrə vurduğu psixoloji zərərlə bağlı təbliğatın gücləndirilməsi;
- beynəlxalq təcrübənin öyrənilməsi və tətbiqi;
- *Insafe* təşkilatı ilə əməkdaşlığın yaradılması;
- uşaqların İnternetdə təhlükəsizliyinin təmin olunmasına dair saytın yaradılması;
- müvafiq sahədə ixtisaslaşan elmi kadrların hazırlanması;
- uşaqlar üçün nəzərdə tutulan sosial şəbəkələrin yaradılması;
- uşaqlar üçün maarifləndirici kitabçaların hazırlanması;
- valideynlər, müəllimlər üçün İnternetin təhlükəsizlik məsələlərinə dair vəsaitlərin, kitabçaların, bukletlərin hazırlanması və kursların təşkili;
- təhlükələrin yaratdığı zərərli nəticələri göstərən videoçarxların hazırlanması;
- kurikulum proqramına İnternetin təhlükələri barədə dərslərin salınması;
- "Təhlükəsiz İnternet Günü"nün məktəblərdə qeyd edilməsi, məktəblilər arasında bu problemlərə həsr olunmuş müxtəlif müsabiqələr, görüşlər, seminarlar keçirilməsi müsbət nəticələrə gətirib çıxara bilər.

Valideynlər, məktəblər və müvafiq səlahiyyətli şəxslər uşaqları İnternetdə olan təhlükələrdən mühafizə edə və yaxud yaranmış təhlükələrin qarşısını almaq məqsədilə müxtəlif vasitələrlə bu problemin düzgün həllinə öz töhfələrini verə bilərlər.

Ədəbiyyat:

1. Соколов И. А., Колин К. К. Развитие информационного общества в России и актуальные проблемы информационной безопасности // Информационное общество. –2009, № 4-5, с.98-106.
2. Allahverdiyeva S.S. Uşaqların İnternetdə təhlükəsizliyinin təmin edilməsi problemləri, Ekspress-informasiya, Bakı, İnformasiya Texnologiyaları, 2016, 91 s.
3. Çelen F.K., Çelik A., Seferoğlu S.S. Çocukların İnternet Kullanımları ve Onları Bekleyen Çevrim-İçi Riskler // Malatya Akademik Bilişim, 2011, 2-4 Şubat, s.645–652.
4. Dombrowski S.C., Gischlar K.L., Durst Th. Safeguarding young people from cyber pornography and cyber sexual predation: a major dilemma of the Internet // Child Abuse Revue, no.3, pp.153–170.
5. Chou C., Condron L., Belland J.C. A Review of the Research on Internet Addiction // Educational Psychology Review, 2005, vol.17, iss. 4, pp.363–388.
6. Əliquliyev R.M., Mahmudov R.Ş. İnformasiya asılılığı problemləri və onlarla mübarizə yolları. Ekspress-informasiya, Bakı, İnformasiya Texnologiyaları, 2009, 61 s.
7. Young K. Internet addiction: the emergence of a new clinical disorder // Cyber Psychology & Behavior, 1998, vol.1, pp. 237–244.
8. Voiskounsky A.E. Internet: Culture, Diversity and Unification // Javnost – The Public. Journal of the European Institute for Communication and Culture. 1999, vol. VI (4), pp.53–65.
9. Богданова Д.А., Федосеев А.А. Внимание – Интернет // Открытое образование, 2010, №2, с.89–99.
10. Buckingham D., Whiteman N, Willett R., Burn A. The Impact of the Media on Children and Young People with aparticular focus on computer games and the Internet. Centre for the Study of Children, Youth and Media, Institute of Education, London, 2007, pp.77.
11. Lord N. What is a phishing attack? Defining and identifying different types of phishing attacks, http://www.digitalguardian.com
12. Контент-фильтр, http://www.ru.wikipedia.org
13. 7 Windows 10 Security Features & How to Use Them, http://www.microsoft.com
14. Reports in Kaspersky Anti-Virus 2015, http://www.support.kaspersky.com
15. Егоров А. Ю., Игумнов С.А. Расстройства поведения у подростков, СПб:Речь, 2005, 436 с.
16. Griffiths M., Hunt N. Dependence on computer games by adolescents // Psychological Reports, 1998, vol.82, pp.475–480.
17. Safer İnternet Programmer, http://www.saferinternet.org
18. http://www.inhope.org
19. UK Safer Internet Centre, http://www.saferinternet.org/united-kingdom
20. Germany Safer Internet Centre, http://www.saferinternet.org/germany
21. Russian Safer Internet Centre, http://www.saferunet.ru
22. Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya, http://www.president.az
23. Azərbaycanda "Uşaqların İnternetdə Təhlükəsizliyi" adlı layihə həyata keçirilir, http://www.azertag.az

УДК 04:3

Оджагвердиева Сабира С.
Институт Информационных Технологий НАНА, Баку, Азербайджан
allahverdiyevasabira@gmail.com

Вопросы обеспечения безопасности детей в интернет-среде

Обеспечение безопасности детей в Интернете является одной из наиболее важных проблем. В статье показаны угрозы, с которыми сталкиваются дети в Интернете, их классификация и способы защиты от них. Предоставляется информация о поведении детей в цифровом мире в зависимости от их возрастных особенностей. Изложены подходы к решению этой проблемы, существующие на международном уровне. Исследуется деятельность национальных центров безопасности Интернета. Анализируется работа, проделанная для решения данной проблемы в Азербайджане, выдвигаются рекомендации и предложения.

Ключевые слова: *безопасность детей, киберопасность, интернет-зависимость, национальные центры безопасного Интернета, безопасный Интернет.*

Sabira S. Ojagverdiyeva
Institute of Information Technology of ANAS, Baku, Azerbaijan
allahverdiyevasabira@gmail.com

Ensuring child safety in Internet environment

The article outlines the dangers faced by child on the Internet, their classification and ways to protect them from these dangers. The article provides information on the behavior of child in the digital world, taking into account the age characteristics of child. The article describes existing approaches to this problem on international level. The activities of National Safer Internet Centers are being investigated. Furthermore, the implementations to solve this problem in Azerbaijan are analyzed and some suggestions are made.

Keywords*: safety of child, cyber threat, Internet addiction, National Safer Internet Centers, safer Internet.*