İnternetdə UşaqlarınTəhlükəsizliyini Təmin Edən Proqram Vasitələrinin Təhlili

Tofiq Kazımov[1], Sabirə Ocaqverdiyeva[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]*tofig@mail.ru*, [2]*sabiraas@list.ru*

***Xülasə*— Məqalədə uşaqların İnternet mühitində təhlükəsizliyinin təmin olunması üçün mövcud proqram təminatları araşdırılır. Geniş istifadəçi auditoriyası qazanmış proqram vasitələri analiz olunur və onların üstün cəhətləri göstərilir.**

Açar sözlər*— *ziyanlı informasiya, kontent filtrasiyası, İnternet təhlükələri, uşaq brauzeri, proqram vasitələri

I. GİRİŞ

İnformasiya texnologiyalarından istifadə insanların informasiya ilə təmin olunması üçün qeyri-məhdud imkanlar yaradır, istifadəçilərin İnformasiya Cəmiyyətinin (İC) fəal üzvü kimi formalaşmasında mühüm rol oynayır. İstifadəçilər informasiya texnologiyalardan istifadə etməklə bir çox problemlərin, məsələlərin həllində öz sözünü demək imkanı qazanmaqla yanaşı, uzaqda yaşayan yaxınları, dostları ilə əlaqə saxlaya, öz əyləncəsini təşkil edə, biliklərini paylaşa bilir və s. Lakin, İnternetdən istifadənin faydaları ilə yanaşı, təhlükələrəsəbəb olan bir çox cəhətləri də mövcuddur.

Təhlükələrin istər real həyatda, istərsə də İnternet mühitində mövcudluğu problemlərin yaranmasına təkan verir. İnternetdə uşaqların təhlükəsizliyinin təmin edilməsindən danışılırsa bu problem kompleks yanaşma tələb edir.

İnternet mühitində uşaqların təhlükəsizliyinin təmin olunmasında məlumatlandırma və maarifləndirmənin həyata keçirilməsi onların tam qorunması üçün kifayət etmir. Bu problemin həllini həm təşkilati həm də, texniki səviyyədə həyata keçirmək lazım gəlir.

Azərbaycan Respublikasının prezidentinin 2014-cü il 2 aprel tarixli sərəncamı ilə təsdiq edilmiş “Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya”da informasiya təhlükəsizliyinin təmin edilməsi bir istiqamət kimi təyin 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 [1].

Hazırda bütün dünyada uşaq və yeniyetmələrin İnternetdən təhlükəsiz istifadə problemlərinə yönəlmiş çoxlu sayda proqram təminatından istifadə olunur. Bu proqramlarda kibertəhlükələr haqqında məlumatlar verilir, təhlükələrdən qorunmaq üsulları göstərilir və hətta kiberhücumların qurbanlarına psixoloji dəstək də göstərilir. Bütün bunlarla yanaşı sosial şəbəkələrdə, forumlarda və s. virtual məkanlarda insanların qarşılıqlı münasibətlərini nəzərə alan proqram təminatlarının yaradılmasına ehtiyac duyulur. Aqressiv şəxsləri təyin edən, psixodiaqnostik analiz xassələrinə malik olan, verilən kontenti süzgəcdən keçirən və uşaqlara təhlükəsiz İnterneti təmin edən proqramların olması vacib məsələlərdəndir.

Məqalədə uşaqların İnternetdə təhlükəsizliyinin təmin olunması üçün və ziyanlı kontentin qarşısının alınmasında istifadə olunan proqram vasitələrinin funksiyaları göstərilmişdir. Kompüterin və qlobal şəbəkənin müəyyən resuslarına çıxışın məhdudlaşdırılması üsullarının təsnifatı verilmişdir.

II. KONTENT FİLTRASİYASI

Uşaqların psixologiyasına və sağlamlığına təsir edən məlumatlar, həmçinin onların təbliğatını aparan kontentlər ziyanlı informasiya daşıyıcıları hesab olunur.

Ziyanlı informasiyanın və bilavasitə azyaşlı İnternet istifadəçisinə yönəlmiş təhlükələrin qarşısının alınması məqsədilə müxtəlif texnoloji üsullardan, mexanizmlərdən və ya proqram vasitələrindən istifadə tələb olunur.

Ziyanlı kontentin qarşısının alınması dedikdə, İnternetdə mübahisəli hesab edilə biləcək kontentlərin görünməsinin və onlara çıxışın məhdudlaşdırılması başa düşülür. Bu tip kontentlərlə mübarizə aparmaq üçün kontent filtrasiyasından istifadə olunur[2].

Kontent filtrasiyası yerinə yetirilibsə istifadəçi şəbəkəyə daxil olan zamanı müəyyən kodlarla arzuolunmayan kontent göstərilir və bununla üzləşdikdə avtomatik bu tip kontentlər silinir. Belə proqramlarla bağlı əsas tənqid onunla əlaqədardır ki, bu kodları adətən proqramdan silmək olur. Bu metod həm şirkətlər tərəfindən, həm də ailələr tərəfindən istifadə edilir.

Kompüterdə olan zərərli proqram və ya arzu olunmayan kontentlə rastlaşmanın qarşısını almaq üçün filtr proqramlarından istifadə olunur. Bu proqramlar vasitəsilə valideyn İnternetdən istifadə zamanı bir sıra saytlara qadağalar qoya və məhdudiyyətləri tənzimləyə bilir. Uşağın yaşa uyğun olmayan saytlara, sosial şəbəkələrə, azartlı oyunlara girişinin qarşısını alır, lazımsız yükləmələrin edilməsinə, alış-veriş saytlarına və s. daxil olmasına mane ola bilir.

Araşdırmalara görə İnternet istifadəçiləri arasında 9 milyondan çox istifadəçion dörd yaşına çatmamış uşaqlardan ibarətdir. Bu uşaqların demək olar ki, dörddə biri üzərində valideyn nəzarəti yoxdur. Onların təxminən 40%-i ziyanlı kontentlərə müraciət edir, 20% uşaq isə İnternet üzərindən

DOI: 10.25045/NCSoftEng.2017.80

cinsi zorakılığın qurbanı olur. Yalnız onların az bir hissəsi uşaqlar üçün nəzərdə tutulmuş saytlardan istifadə edir [3].

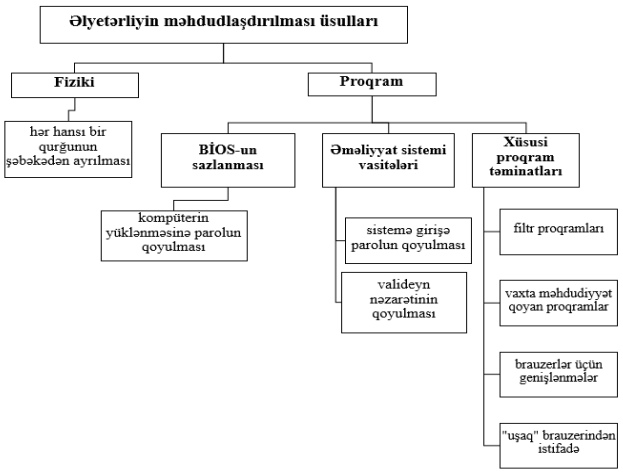
III. İNTERNETƏ ÇIXIŞIN MƏHDUDLAŞDIRILMASI YOLLARI

Veb səhifələr müxtəlif məzmunlu məlumatlarla intensiv olaraq zənginləşdirilir. Hər bir istifadəçi bununla bağlı fərqli problemlərlə qarşılaşır. Qəbul etməliyik ki, İnternet doğrudan da təhlükəsiz bir məkan deyildir və valideyn İnternetdə olan təhlükələrdən məlumatlı olub, övladının texnologiyalardan istifadəsinə daim nəzarət etmiş olsa belə, istənilən an təhlükələrlə onun qarşılaşma ehtimalı yüksəkdir. Onların əksəriyyəti bu işdə köməyi məktəbdən gözləyir [4]. Başqa bir yanaşma kimi valideyn uşaqlarla birlikdə “ağ siyahılar” tərtib edə bilər, lakin tez-tez yeni saytların meydana gəlməsi ilə əlaqədar olaraq bəzən, bu siyahılar da problemin həll edilməsində öz əhəmiyyətini itirir və yenidən eyni situasiya ilə qarşılaşma ehtimalı yaranır.

Beynəlxalq təcrübəyə nəzər salsaq, məsələn, Rusiyada Federal təhlükəsizlik proqramı çərçivəsində uşaqlar üçün nəzərdə tutulmuş xüsusi brauzer *Gogul* uşaqların İnternet resurslarından təhlükəsiz istifadəsini təmin etmək üçün nəzərdə tutulmuşdur. Brauzer uşaqları onların zəif uşaq psixologiyasına təsir edən saytlardan qoruyur, xüsusi seçilmiş təhlükəsiz saytlara girişə icazə verir [5,6].

Brauzerin fünksiyaları təhlükələrin qarşısının alınmasında tam olaraq effektli deyildir. Brauzerlərin təhlükələrə dayanıqlığını artırmaq üçün brauzer genişlənmələrindən istifadə məqsədə uyğun sayılır. Brauzerin təhlükəsizlik imkanlarını artırmaq üçün *AdBlock* pulsuz brauzer əlavəsi nəzərdə tutulmuşdur. O, susma rejimində ziyanlı kontentlərə, reklam və videolara süzgəc qoyur. Hətta *FaceBook* və ya *Youtube* kimi saytları da bura aid etmək olar [7].

BİOS-a və əməliyyat sisteminə parol qoymaqla dauşağın texnologiyalardan təhlükəsiz qalmasının qarşısının alınması mümkündür. Yuxarıda qeyd olunanları ümumiləşdirərək, təhlükələrin qarşısının alınması məqsədilə uşağın kompüterin və qlobal şəbəkənin resuslarına əlyetərliyinin məhdudlaşdırılması üsulları aşağıdakı şəkildə təsnifat etmək olar[8]:



Şəkil 1. Uşağın kompüterin və qlobal şəbəkənin resuslarına əlyetərliyinin məhdudlaşdırılması üsullarının təsnifatı.

Yuxarıda qeyd etdiklərimiz üsullardan əlavə digər üsullar var ki, uşaqların İnternetə çıxışını məhdudlaşdırmaq üçün nəzərdə tutulmuşdur. Ən əsası odur ki, valideynlərin özü texnologiyalardan istifadəni bilməli və İnternetdə olan təhlükələr barədə məlumatlı olmalıdır.

IV. TƏHLÜKƏLƏRİN TEXNOLOJİ ÜSULLARLA PROFİLAKTİKASI

İnternetdə və kompüterdə təhlükələrdən qorunmaq üçün Windows Vista əməliyyat sisteminin funksiyalarını nəzərdən keçirək. Bu əməliyyat sistemi üzərində olan “Valideyn Nəzarəti” Proqramı vasitəsilə aşağıdakı funksiyaları yerinə yetirmək mümkündür [9]:

1) uşağın kompüterdə işləməsinə məhdudiyyət qoyur, kompüterə daxilolma və çıxışının vaxtını müəyyənləşdirir, xüsusilə həftənin hansı günü, hansı saatda çıxışını təyin edə bilir. Qoyulmuş vaxt bitdikdən sonra sistemdən avtomatik “çıxış” reallaşır. Bu isə uşağın bir müddət sistemə daxil olmaq imkanını azaldır;

2) müəyyən proqramlara uşağın çıxışının qarşısını alır, yaş qiymətləndirilməsi əsasında qadağan olunmuş məzmun növünün seçilməsinə və ya müəyyən oyunlara daxil olmağa qadağalar qoyur;

3) uşağın İnternetdə aktivliyini və İnternetdə fəaliyyətini məhdudlaşdırmağı nəzərdə tutur. Veb səhifələrə girişə limit qoyur, yaş qiymətləndirməsi əsasında yükləmələrin yerinə yetirilməsinə qadağa qoyur yaxud icazə verir. Müəyyən kontentlərə süzgəc qoya bilir (hansından istifadəyə icazə var və ya yoxdur istifadəçi özü təyin edə bilir);

4) Uşağın kompüterdən istifadəsinin hesabatını aparmağa imkan verir.

Microsoft şirkəti *Windows 7* əməliyyat sistemindən başlayaraq valideynlərə uşaqların internetdə zərərli saytlardan müdafiəsinə və onları nəzarətdə saxlamağa imkan verən “*Windows Family Safety”* adlı proqram təminatı hazırlamışdır. Windows ailəsinə məxsus olan *Windows 10*-dan əvvəlki əməliyyat sistemlərində təhlükəsizliklə bağlı məsələlər daha çox sonradan yazılan proqram təminatı vasitəsilə təşkil olunurdu [10].

Windows 10 əməliyyat sisteminə əlavə olunmuş "*Windows Hello*" adlanan yeni təhlükəsizlik xüsusiyyəti sayəsində kompüter, istifadəçinin üzü, gözün tor qişası ya da barmaq izi ilə açılır. Əvvəllər biometrik vasitə kimi insan üzü və barmaq izi qismən də olsun istifadə edilirdi. Ancaq bu xüsusiyyətlər daha da inkişaf etdirildi və növbəti tanınma üsulu kimi gözün tor qişası əlavə olundu.

Yeni təhlükəsizlik xüsusiyyətlərindən sonra Windows 10 əməliyyat sisteminə daxil olarkən şifrə xatırlamağa ehtiyac qalmır. "*Windows Hello"* həmçinin əməliyyat sistemini kiber hücumlardan da qoruyur.

Microsoft şirkəti artıqWindows 10 əməliyyat sistemi ilə *İnternet Explorer* brauzerini yeni “*Spartan*” brauzer ilə əvəz etmişdir. ”*Spartan*” hal hazırda dünyada ən təhlükəsiz veb brauzerlərdən hesab olunur[11]. İstifadəçinin maksimum təhlükəsizliyini təmin edəcək mexanizmlərlə təchiz olunmuş ”*Spartan*” brauzeri, İnternetdən yoluxa biləcək virusların

DOI: 10.25045/NCSoftEng.2017.80

qarşısını almaqla yanaşı, təkmilləşdirilmiş "*https*" protokolundan istifadə etməklə məlumatın təhlüksizliyinin qorunması və valideynlər üçün uşaqların zərərli saytlardan tam müdafiəsini nəzərdə tutan informaiyanın filtirləməsi xüsusiyyətlərinə də malikdir [12].

Sürətli informasiya mübadiləsi və eyni zamanda şəbəkəyə tez-tez daxil olma kompüteri viruslardan müdafiə ilə yanaşı, filtrləməyə böyük ehtiyac olması zərurətini ortaya çıxarır.

Məşhur antivirus proqramlarının adlarını qeyd etmək olar ki, onlar şəbəkə və ya informasiya daşıyıcılarından kompüterə daxil olan virusların qarşısını almaqla yanaşı eyni zamanda, kontent filtrasiyası ilə bağlı funksiyaları da yerinə yetirir. *McAfee, Norton, Avg* kimi məşhur antivirus proqramlarını buna misal göstərmək olar.

McAfee Family Protection və *NortonFamily* tipli proqramlar vasitəsilə valideyn nəzarətinin tam təmin edilməsi mümkündür. Bu proqramlarınhəyata keçirdikləri aşağıdakı funksiyaların adlarını çəkmək olar:

- ✓ Veb-saytların filtrlənməsi;
- ✓ Sosial şəbəkələrin filtrlənməsi;
- ✓ Axtarış saytlarının filtrlənməsi;
- ✓ Məlumatın göndərilməsinə və qəbul olunmasına nəzarət;
- ✓ Onlayn alış-satış məsələlərinin təhlükəsizliyi və s.

Kaspersky Lab mütəxəssisləri tərəfindən 2015-ci ilin əvvəlində aparılmış monitorinqin nəticələrinə görə, 2014-cü il ərzində istifadəçilər tərəfindən kompüterlərə İnternet təhdidləri əleyhinə istifadə edilən *"Parental Control module"* (Valideyn İdarə Modulu) proqramının yenidən tətbiqinə əsasən, nəticələr aşağıdakı kimi olmuşdur:

– uşaqları belə təhlükələrdən müdafiə edən "Valideyn İdarə Modulu" il ərzində ən azı bir dəfə də olsa, Kaspersky Lab istifadəçisi tərəfindən tətbiq edilmişdir;

– internetdə azartlı oyunlar oynamağa meyilli olanların dörddə birindən çoxu (26.6%) və hər beş istifadəçidən biri saytların bu cür "silahlarına" qarşı gələ bilmir və tələyə düşür;

– "Valideyn İdarə Modulu" bir il ərzində orta hesabla 127 dəfə Kaspersky Lab istifadəçiləri tərəfindən işlədilib;

– 2014-cü ildə yalnız 10 ölkədə kompüterlərin təxminən 65% - ində "Valideyn İdarə Modulu" tətbiq edilib;

– istifadəçiləri belə təhlükələrlə daha çox qarşılaşan ölkələr arasında Rusiya, Hindistan və Çin ilk üçlükdədir;

– Çin, Amerika, Almaniya, İngiltərə və Rusiya isə belə təhlükələrə qarşı bu modulu ən çox və tez-tez tətbiq edən ölkələrdir.

Uşaqların İnternetdə üzləşdikləri təhdidləri müəyyən etmək və təhlükələrin əsas mənbəyini üzə çıxarmaq üçün məsələ ilə bağlı göstərilən nəticələrə görə təyin etmək olur ki, uşaqlar təklükələrə nə qədər yaxındılar.

Digər proqram *KiberMama™* proqramını nəzərdən keçirək. Bu proqram uşaq və ve yeniyetmələrin kompüterdə işləyərkən vaxt məhdudiyyəti qoymaq üçün nəzərdə tutulmuşdur. Uşağın kompüterdə təhlükəsiz işləməsi üçün cədvəl tərtib etməyə imkan verir. Yaşa uyğun olmayan oyunlara, proqramlara və s. girişə qadağa qoyur [13].

Uşaqların smartfonda məşğuliyyətlərini izləmək üçün istifadə olunan proqramlardan bir neçəsinin adını qeyd etmək olar. *Parental Control Board* proqramı uşağın mobil telefondakı işlərini izləməyə və idarə etməyə kömək edir, daxil olan və xaric olan zənglərə nəzarəti təmin edir[14].

Screen Time uşağın nə qədər "ekran vaxtı"əldə etdiyini göstərən köməkçi proqramdır, vaxta əsasən müxtəlif proqramları bloklayır [15].

SecureTeen proqramı vasitəsilə valideyn uşağa məhdud zaman intervalında qurğudan istifadə etməyə imkan verir [16]. Bu proqramlarla yanaşı bir çox proqramların adını qeyd etmək olar ki, həmin proqramlardan isifadə etməklə kompüter, mobil telefon və planşetlərdə uşaqların təhlükəsiz qalması mümkündür.

NƏTİCƏ

Müasir dövrdə uşaqların informasiya texnologiyalarına olan maraqları çox böyükdür. Lakin, azyaşlı istifadəçilərin əksəriyyəti İnternetdə mövcud olan təhlükələrdən o qədər də məlumatlı deyillər. Onlar İnternetdən istifadənin verdiyi zərərlərin həyatda indi və gələcəkdə hansı problemlər yaradacağını lazımi qədər hiss edə bilmirlər.

Mütəxəsislər müxtəlif proqram vasitələri ilə şəbəkədə uşaqların təhlükəsizliyini təmin etmək üçün daha optimal üsullar tapmağa çalışır. Mövcud proqram vasitələrinin olmasına baxmayaraq, hal-hazırda daha ehtibarlı proqram vasitələrinə və ya mexanizmlərin yaradılmasına ehtiyac duyulur.

ƏDƏBİYYAT

[1] Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya, 02 aprel 2014-cü ilwww.president.az

[2] Контент-фильтр, https://ru.wikipedia.org

[3] Интернет контроль: Безопасность детей в интернете

[4] www.internet-kontrol.ru

[5] Г.Солдатова, Е.Рассказова, Ребенок в Интернете: запрещать, наблюдать или объявнять? // Дети в информационном обществе: информационно-аналитический журнал. 2012, № 10

[6] www.3dnews.ru/578826

[7] www.bestfree.ru/soft/inet/kids-browser.php

[8] www.adblockplus.org/#footnote

[9] М. С.Перевозчикова, А. Н.Сапегин, Способы контроля доступа школьников к компьютерным ресурсам, Концеп– 2014, № 10

[10] Функции, решаемые с помощью родительского контроля Windows Vista, http://5informatika.net

[11] www.microsoft.com/en-us/windows/features

[12] Spartan Nedir? Spartan Ne İşe Yarar?, www. teknovi.com, 2015

[13] S.S. Allahverdiyeva, "Uşaqların İnternetdə təhlükəsizliyinin təmin edilməsi problemləri", Ekspress-informasiya, 2016. 91 s.

[14] КиберМама™ - компьютер и ребенок: http://www.cybermama.ru

[15] Parental Control Board:https://docs.parentalboard.com

[16] Screen Time Parental Control:https://play.google.com

[17] iTunes Preview: https://itunes.apple.com

DOI: 10.25045/NCSoftEng.2017.80