Uşaqların İnternetdə informasiya təhlükəsizliyini təmin edən sistemin konseptual modeli

Əliquliyev R.M., Ocaqverdiyeva S.S.

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

[1]secretary@iit.ab.az, [2]allahverdiyevasabira@gmail.com

Xülasə– **Məqalədə verilənlərin sanitarizasiyası metodundan istifadə etməklə ziyanlı informasiyanın qarşısının alınması üçün konseptual model təklif olunmuşdur. Məqsəd intellektual analiz metodlarından istifadə etməklə İnternet şəbəkəsində uşaqların təhlükəsizliyinin təmin edilməsini nəzərdə tutan sistemin yaradılmasıdır.**

Açar sözlər– uşaqların təhlükəsizliyi, sanitarizasiya metodu, konseptual model, veb-separator, veb-total.

I. GİRİŞ

Müasir dövrdə informasiya texnologiyaları insanların demək olar ki, bütün fəaliyyət sahələrini əhatə edir və həyat səviyyəsinin dəyişməsinə öz təsirini göstərir. İnternetin sürətli inkişaf tendensiyası isə bu prosesə daha da təkan verir. Genişzolaqlı İnternetin tətbiqi istifadəçilərə hər hansı məkan və qurğudan asılı olmayaraq istənilən kontentə çıxışı təmin edir. Nəticədə informasiyanın həcmi get-gedə artmağa başlayır. Bu informasiya bolluğunun qarşısında ənənəvi məlumat emal vasitələrinin imkanları demək olar ki, məhdudlaşır və onları Big Data texnologiyaları əvəz edir.

İnternet istifadəçilərə məhdudiyyətsiz, müxtəlif məzmunlu informasiya əldə etmək üçün unikal imkanlar təklif edir və onların informasiya cəmiyyətinin fəal üzvü kimi formalaşmasında mühüm rol oynayır. İnternetdə müxtəlif məzmunlu məlumatların olması uşaqların virtual məkanda təhlükələrlə qarşılaşmasını reallaşdırır. Virtual məkanda, əsasən də sosial mediada son zamanlar geniş yayılan pornoqrafiya, işgəncə, qəddarlıq səhnələri, narkotik, spirtli içkilərin, terrorizm, pis vərdişlərin təbliğatı və s. kimi bəzi məlumatlar arzuolunmaz mənəvi və əxlaqi keyfiyyətləri aşılayır. Bədniyyətli şəxslər tərəfindən uşaqlara hədə-qorxu, təcavüz kimi informasiya-psixoloji təsirlərin göstərilməsi hallarına rast gəlinir. Bu isə İnternetdən istifadənin üstünlükləri ilə yanaşı informasiya təhlükəsizliyi ilə bağlı bir sıra problemlərin yaranmasına yol açır və informasiyanın emalı prosesini mürəkkəbləşdirir. Bu təhlükələrin yaratdığı problemlər təkcə texnoloji deyil, eyni zamanda sosial məsələlərin həllini də tələb edir.

İnternetdə uşaqların təhlükəsizliyinin təmin olunması təkcə məlumatlandırma və maarifləndirmə işlərinin aparılması ilə bitmir. Həyata keçirilən tədbirlər indiki vəziyyətdə yalnız tövsiyə xarakteri daşıyır və onlayn mühitdə tam qorunma üçün kifayət etmir. Hal-hazırda uşaqların İnternetdən təhlükəsiz istifadəsi problemlərinin həllinə yönəlmiş çoxlu sayda proqram təminatları və təhlükəsizlik sistemləri mövcuddur.

İnternetdən gələn təhlükələrin qarşısını almaq üçün bəzi yanaşmalarda şəbəkə təhlükəsizliyi monitorinqi (ŞTM) sisteminin işlənməsi təklif edilir. ŞTM şəbəkə haqqında informasiyanın toplanması, analizini aparmaqla müxtəlif şəxslərə və ya sistemlərə yönləndirən, proqram və aparat komplekslərindən ibarət olan mürəkkəb bir sistemdir. ŞTM sistemindən istifadə etməklə İnternet istifadəçilərinin təhlükəsizliyi, konfidensiallığı və mühafizəsini həyata keçirmək mümkündür [1].

Lakin bu tip sistemlərin tətbiq olunmasına baxmayaraq, şəbəkədə uşaqların təhlükəsizliyinin təmin edilməsi üçün daha optimal üsulların, ehtibarlı proqram vasitələrinin və mexanizmlərin yaradılmasına ehtiyac duyulur.

Məqalədə İnternetdən daxil olan ziyanlı kontentin qarşısının alınması məqsədini daşıyan konseptual model verilir. Model sanitarizasiya metodundan istifadə etməklə ziyanlı informasiyanın qarşısının alması və müvafiq qərarın qəbulu üçün nəzərdə tutulmuşdur.

II. KONSEPTUAL MODELİN ÜMUMİ SXEMİ

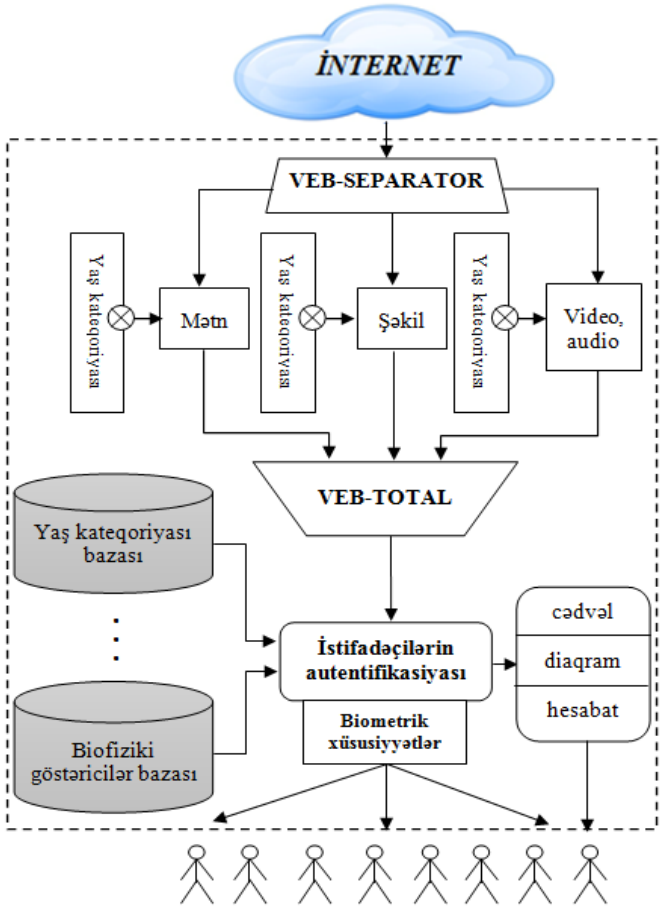
Şəkil 1-də təqdim olunan model İnternetdən əldə olunan veb-səhifələrin trafikinin sanitarizasiyası əsasında yaradılmışdır. Məqalədə uşaqların informasiya təhlükəsizliyinin təmini üçün verilənlərin sanitarizasiyası (*Data Sanitization*, VST) metodundan istifadə etməklə daha əhəmiyyətli, faydalı və yaşa uyğun İnternet resurslarının təqdim olunması nəzərdə tutulur. Verilənlərin sanitarizasiyası İnternet qlobal şəbəkəsindən daxil olan təhlükələrdən qorunma metodlarından biridir. Bu metodun mahiyyəti həssas, sensativ, fərdi, məxfi, tövsiyə olunmayan və s. məlumatların geniş ictimaiyyətə çatdırılmasının qarşısını almaqdan və ya müəyyən məhdudiyyətlərin tətbiq olunmasından ibarətdir [2].

VST-dən adətən, çap olunmuş materiallar üzərində, gündəlik onlayn mediada və kompüterdə də istifadə edilir. Məxfiliyin qorunmasını da nəzərdə tutan bu metod əsasən məxfi olmayan və müəllif hüquqları ilə qorunmayan məlumatların konfidensiallıq səviyyəsini azaldır və əlyetərli edir [3].

Şəkildə göstərilən modelə əsasən istifadəçisi uşaqlardan ibarət olan auditoriyaya onların yaşı, marağı, səhhəti, bilik

DOI: 10.25045/NCInfoSec.2017.19

səviyyəsi, psixoloji vəziyyəti və s. əlamətləri nəzərə alınmaqla süzgəcdən keçirilmiş veb-səhifələr təqdim olunur. Təklif olunmuş konseptual modelin bir sistem şəklində fəaliyyətini təmin etmək məqsədilə iyerarxik düzülmüş müəyyən komponentlərdən istifadə olunur: veb-separator, veb-total, istifadəçinin autentifikasiyası və s.



Şəkil 1. Trafikin sanitarizasiyasının konseptual modeli

Məlumdur ki, İnternetdən istifadə edən uşaqlar maraqlarına və yaş qruplarına görə fərqlənir. İstər sosial şəbəkələrdə, istərsə də rəqəmsal əşyalarla münasibətdə bu fərqlər özünü göstərir. Bəzi tədqiqatlarda İnternetdən istifadə edən uşaqlar aşağıdakı kateqoriyalar üzrə yaş qruplarına bölünür [4]:

- 7 yaşadək;
- 7-10 yaş;
- 10-13 yaş;
- 13-17 yaş.

Belə nəticəyə gəlmək olar ki, təqdim olunan informasiya uşaq auditoriyasına görə fərqli xüsusiyyətlər daşıyır. Uşaqların yaş psixologiyası və s. nəzərə alınmaqla veb-kontenti aşağıdakı kimi kateqoriyalara bölməklə məlumatlar üzərində müvafiq qiymətləndirmələrin aparılması mümkündür:

1. Yaş;
2. Mövzu;
3. Maraq dairəsi;
4. Fizioloji imkanları;
5. Kontentin tipi;
6. Valideyin nəzarəti;
7. Uşağın psixoloji profili.

Yuxarıda göstərilən kateqoriyalar milli, dini, irqi, etnik, coğrafi məkan və s. xüsusiyyətlərə görə artırıla və ya dəyişdirilə bilər.

III. VEB-SEPARATOR

Veb-separator – kontent analizi, yaxud informasiyanın məzmununun təhlili, mətn və qrafik məlumatların öyrənilməsi üçün formalaşdırılmış bir metoddur. Məlumatların kəmiyyət göstəriciləri üzərində aparılan formal müşahidə və statistik prosedurdur [4].

Separatorlar bir növ kontentin bölücü, ayrıcı funksiyasını yerinə yetirir. Tədqiqatda veb-separatorlardan veb-kontentin tipinə görə bölünməsi üçün istifadə olunur. Veb-kontentin tipinə görə sorğuların toplanması və semantikanın müəyyən edilməsi üçün veb-separatordan sistemin girişində istifadə olunması nəzərdə tutulur. Müasir veb-səhifələrdə reklam, audio, video, şəkil və s. multimedia fayllarının, onlayn xidmətlərin geniş yayılması bu səhifələrin məzmununu daha da zənginləşdirir.

Səhifələrin əsas aparıcı mövzusundan başqa əlavə mövzuların formalaşması üçün səhifənin dizaynında olan dəyişikliklər isə onun strukturunu mürəkkəbləşdirir. Müxtəlif əlavə elementlərin daxil edilməsi veb-səhifələrin quruluşunu zənginləşdirməklə yanaşı, onların analizini daha da çətinləşdirir. Veb-səhifələri təhlil etmək üçün bəzi yanaşmalarda səhifə üfüqi və şaquli xətlər vasitəsilə çərçivələrdən ibarət hissələrə bölünür [5]. Digər yanaşmalarda isə veb-səhifələrin kontent-analizi mövzuya uyğun olaraq klasterləşdirmə metodlarına əsaslanır [6].

Tədqiqatda lazım olan veb-səhifələrin aşkarlanması üçün bu səhifələrdəki kontentin separator vasitəsilə multimedia resuslarının tipinə görə kateqoriyalara bölünməsi nəzərdə tutulur:

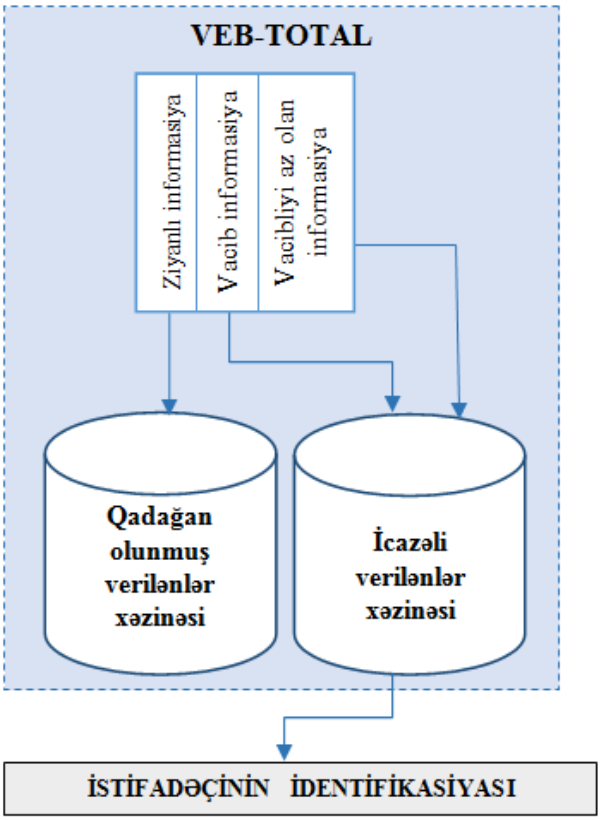
1. Mətn tipli informasiya;
2. Şəkil faylları;
3. Audio və video fayllar;

Separatorun süzgəcindən təmizlənmiş multimedia trafiki toplanır və məlumatların yenidən mövzuya uyğun olanlarının klasterləşməsinə ehtiyac yaranır. Beləliklə də, proses növbəti mərhələyə keçir.

IV. VEB-TOTAL

Təmizlənmiş multimedia trafiki veb-totalın girişinə daxil olur. İnternetdən daxil olan multimedia trafikinin üzərində təmizləmə, aqreqatlaşdırma və strukturlaşdırma işləri yerinə yetirilir. Veb-səhifələrin təmizlənməsi texnoloji səviyyədə aparılır. Şəkil 2.-də veb-səhifələrin məzmununa daxil olan məlumatların xüsusiyyətlərinə görə bölünməsi təsvir olunmuşdur. Həmin məlumatlar 3 yerə bölünür və bunlara aşağıdakılar daxildir:

1. Vacibliyi az olan informasiya;
2. Vacib informasiya;
3. Ziyanlı informasiya.



Şəkil 2. Veb-səhifələrin kontentə uyğun bölünməsi

Açılan əlavə pəncərələrə blokun qoyulması, əlavə JavaScript və Flash proqram təminatları vasitəsilə həyata keçirilir. Təqdim olunan kontent tələbləri ödəmirsə, yəni, səhifələrdə qadağan olunmuş teq, söz, jarqon ifadələr, şəkil və ya videoçarxlar mövcuddursa, həmin səhifələrin bağlanması və həmçinin uyğun olmayan reklamların bloklanması da nəzərə alınır [7].

Süzülmə zamanı İnternetdən daxil olan müxtəlif məzmunlu kontentin mənbələri aşkarlanır və verilənlər xəzinəsinə yığılır. Bu zaman intellektual analiz üsullarından istifadə edilə bilər (text maining və s.). Əvvəlcədən qoyulmuş şərtə əsasən qadağan olunmuş və ziyanlı informasiya olan veb-səhifələr aşkarlanaraq “qadağan olunmuş verilənlər xəzinəsinəsi”-ə yığılır.

Vacibliyi az olan informasiya üzərində nəzarəti gücləndirmək üçün valideyin nəzarəti tələb olunur. Vacib olan məlumatlar umumi məlumatların bir hissəsi olmaqla uşaqlardan ibarət olan auditoriya üçün təhlükəsizdir. Analiz və təsnifatlandırma nəticəsində əldə olunmuş informasiya uşaqlara təqdim olunmazdan əvvəl onların biometrik xüsusiyyətləri nəzərə alınmalıdır.

IV. BİOMETRİK İNDENTİFİKASİYA

Müasir dünyada biometrik texnologiyalar müxtəlif xidmət növlərinin təqdimatında şəffaflığı, dəqiqliyi, həm də təhlükəsizliyi təmin edir. Biometrik texnologiyalardan istifadə etməklə eyni zamanda müxtəlif obyektlərə təhlükəsiz girişi əldə etmək olar. Biometrik eyniləşdirmə sistemin unikal biometrik parametrinin istifadəçisinin təqdim etdiyi məlumatdır və mövcud məlumatların bütün məlumat bazası ilə müqayisə edilməsi prosesidir.

Biometrika bir və ya daha çox bioloji və ya davranış xüsusiyyətlərinə görə insanların tanınma sistemini əhatə edir. İnformasiya texnologiyaları sahəsində biometrik məlumatlar giriş əlamətlərinin idarə edilməsi və giriş nəzarəti şəklində istifadə olunur. Biometrik sistem iki rejimdə işləyə bilər [8]:

1) Verifikasiya – bu doğrulama əvvəlcədən tərtib olunmuş biometrik şablon və ya standarta uyğunluğu müəyyən edir.

2) İdentifikasiya – biometrik məlumatları əldə etdikdən sonra şəxsiyyəti müəyyən etmək üçün biometrik baza ilə əlaqədən istifadə olunur. İdentifikasiya istifadəçiyə və ya müəyyən istifadəçinin adından fəaliyyət göstərən prosesə özünü adlandırmağa imkan verir.

Uşaqların biometrik xüsusiyyətləri nəzərə alınmaqla tərtib olunmuş şablona əsasən onlara sistemə daxil olmağa icazə verilir. Biometrik identifikasiyada kompüterin müxtəlif modullardan insan bədəninə zərərverici təsiri (görmə qabiliyyətinə təsir, sıxılmış vəziyyət, şüalanma, ruhi təsir, emosiya və s.) nəzərə alınmalıdır.

V. QƏRARLARIN QƏBUL EDİLMƏSİ

Konseptual modelin infrastrukturunu həm adminstratorun, həm də valideynlərin qərarlarını dəstəkləyən vasitələr təşkil edir. Sistem yanaşmada qərarların qəbul edilməsi müəyyənlik, qeyri-müəyyənlik, dəqiqlik, müqayisə və risk tələb edən məsələlərin həllində istifadə olunur [9]. Ehtimallarda dəqiq qərar qəbul etmədən bütün kriteriyaların nəzərə alınması vacibdir. Burada bütün mümkün hallar müqayisə olunur.

Biometrik xüsusiyyətlərinə görə bölünən veb-kontent sonda istifadəçilərə ötürülsə belə onlar haqqında məlumatlar cədvəl, diaqram və hesabat şəklində verilənlər bazasında saxlanılır. Bu məlumatlardan isə müxtəlif qərar qəbuletmədə

istifadə oluna bilər. Onlardan əsas istifadə olunanlar aşağıdakılardır:

1. İstifadəçilərə ötürülən şübhəli veb-kontentin adminstrator tərəfindən dəqiqləşdirilməsi;
2. Ən vacib veb-kontentin dəqiqləşdirilməsi və gələcək müraciətlərdə onların analiz edilmədən istifadəçiyə ötürülməsi;
3. Sistemdə nəzərə alınmayan kriteriyaya görə müraciət əsasında qərarların qəbulu.

Uşaqların İnternetdə təhlükəsizliyi məsələsinin həllində bütün faktorların nəzərə alınması vacibdir. Adminstratorun qərar qəbul etməsi zamanı böyük həcmdə informasiyanın qavranması, tutuşdurulması və analizi mühitində ziyanlı veb-səhifələrin dəqiqləşdirilməsinin həyata keçirilməsi zəruriliyi yaranır.

NƏTİCƏ

Araşdırmalardan məlum olur ki, müasir dövrümüzdə İnternet yalnız maraqlı və əhəmiyyətli məlumatlarla deyil, həm də ziyanlı və təhlükəli veb-səhifələrlə də dolu olan qlobal bir məlumat bazasıdır. Bu informasiya xaosunun içərisindən uşaqlara zərərsiz olan veb-səhifələrin axtarışı, aşkarlanması və əldə olunması üçün xüsusi metod və vasitələrdən isifadə olunmalıdır.

Məqalədə təklif olunan konseptual model bu məqsədə xidmət edir. Uşaqların İnternetdə təhlükəsizliyinin təmin olunması ilə əlaqəli yaranmış problemlərin həllində, tədris proqramının seçilməsində və s. məsələlərdə bu konseptual modeldən istifadə etmək olar.

ƏDƏBİYYAT

[1] Əliquliyev R.M., İmamverdiyev Y.N., Nəbiyev B.R. Şəbəkə təhlükəsizliyinin monitorinqi metodlarının analizi // İnformasiya texnologiyaları problemləri, 2014, №1, 60–68.
[2] https://en.wikipedia.org/wiki/Sanitization_(classified_information).
[3] Allahverdiyeva S.S. "Uşaqların İnternetdə təhlükəsizliyinin təmin edilməsi problemləri", Bakı, İnformasiya Texnologiyaları, 2016, 91 səh.
[4] Егоров А.Ю., Игумнов С.А. Расстройства поведения у подростков. СПб:Речь, 2005, 436 с.
[5] Zheng L.W. Visual separator detection in web pages using code analysis,https://www.google.com/patents/US20130124684
[6] Alguliev R.M., Aliguliyev R.M., Alekperova I.Ya. Cluster approach to the efficient use of multimedia resources in information warfare in Wikimedia // Automatic Control and Computer Sciences, 2014, vol. 48, no. 2, pp. 97–108.
[7] Перевозчикова М.С., Сапегин А. Н. Способы контроля доступа школьников к компьютерным ресурсам // Концепт, 2014, № 10, с.56–60.
[8] https://ru.wikipedia.org/wiki/biometriya
[9] Фатхутдинов Р.А. Управленческие Решения, Москва ИНФРА 2002, 314 с.

CONCEPTUAL MODEL FOR INFORMATION SECURITY SYSTEM OF CHILDRENS ON INTERNET

Rasim M. Alquliyev[1], Sabira S. Ojagverdiyeva[2]
[1,2]Institute of Information Technology of ANAS,
Baku, Azerbaijan
[1]*secretary@iit.ab.az*, [2]*allahverdiyevasabira@gmail.com*

Abstract – On article has been propused a conceptual model by using of data sanitization method for preventing harmful information. The purpose is using intellectual analysis methods for creating a system to assure children safety on internet network.

Keywords – children safety, sanitization method, conceptual model, web-separator, web-total