UOT 04:37 DOI: 10.25045/jpis.v11.i2.07

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

VEB-KONTENTİN FİLTRASİYASI MƏSƏLƏLƏRİ

İnformasiya bolluğu şəraitində İnternet mühitində istifadəçilərin zərərli məlumatlardan (aqressiya, terrorizm, pornoqrafiya, ekstremizm və s.) qorunması problemi son illər daha da aktuallaşmış və dünyadakı sosial-iqtisadi proseslərə təsiri getdikcə artmışdır. Zərərli məlumatlardan qorunmaq, onların mənbəyini aşkarlamaq, veb-kontentin zərərli olmasını müəyyən etmək üçün müxtəlif elmi yanaşmalar və texnologiyalar mövcuddur. Məqalədə zərərli veb-kontenti aşkarlamaq üçün geniş tətbiq olunan kontent-filtrasiya metodunun mahiyyəti və tətbiqinin əhəmiyyəti haqqında məlumat verilir, veb-kontentin filtrasiya səviyyələri müəyyənləşdirilir. Zərərli məzmuna malik olan veb-saytların bloklanması üçün statik və dinamik yanaşmaların mahiyyəti və onlar arasında olan fərq göstərilir. Tədqiqatın məqsədi virtual məkanda mövcud olan informasiya təhlükəsizliyi, kibercinayətkarlıq və bu tip digər məsələlərin həllində kontent-filtrasiya metodunun tətbiqi əhəmiyyətini və veb-resursların ziyanlı kontentdən təmizlənməsinin vacibliyini göstərməkdir. İşdə uşaqların zərərli məlumatlara girişini məhdudlaşdıran proqram vasitələrinin inkişafına yönəlmiş, İnternetdən daxil olan informasiya trafikindən uyğunsuz məzmunun seçilməsi, süzülməsi və istifadəçiyə təqdim edilməsinin qarşısının alınması üçün analiz, müqayisəli təhlil və sistemli yanaşma metodlarından istifadə edilmişdir. Məqalədə əldə edilən nəticələr elektron dövlət platformasında təhsil müəssisələrində, Milli Təhlükəsiz İnternet mərkəzlərində və s. məkanlarda uşaqların zərərli informasiyadan qorunması üçün istifadə edilə bilər.

Açar sözlər: *veb-kontentin filtrasiyası, informasiya təhlükəsizliyi, zərərli məlumatlar, filtrasiya səviyyəsi, URL filtrasiya.*

Giriş

Müasir dövrdə həyatımızı informasiya texnologiyaları olmadan təsəvvür etmək çox çətindir. Artıq informasiya texnologiyaları müxtəlif məlumatları əldə etmək üçün unikal imkanlar yaradır. Kompüter texnologiyaları insan fəaliyyətinin bütün sahələrinə tətbiq edilir, şəbəkələr qurulur, böyük həcmli məlumatlar ötürülür, istifadəçilər məkandan asılı olmayaraq qlobal şəbəkəyə giriş imkanları ilə təmin olunurlar. İnternet istifadəçilərinin sayının getdikcə artması, virtual mühitə yerləşdirilən resursların sayının çox, həcminin və sürətinin böyük olması Big Data problemlərini daha da aktuallaşdırır.

İnternetdən əldə edilən faydalı məlumatlarla yanaşı, uyğunsuz məzmunla qarşılaşma halları müşahidə olunur. İnternetdə uyğunsuz məzmun dedikdə uşaq pornoqrafiyası, insanları terrora cəlb edən materiallar, irqi ayrıseçkilik yaradan saytlar və s. nəzərdə tutulur. Belə məlumatlar uşaq auditoriyası üçün çox təhlükəli hesab olunur. Belə təhlükələrin qarşısının alınması məqsədilə, hər bir istifadəçinin, xüsusilə uşaq və yeniyetmələrin İnternetdən istifadəsi ilə bağlı müxtəlif qabaqlayıcı tədbirlər həyata keçilir. Buraya təşkilati, maarifləndirici və texniki tədbirləri aid etmək olar. Lakin indiki vəziyyətdə İnternet təhlükələri ilə bağlı məlumatlandırma tədbirləri daha çox tövsiyə xarakteri daşıyır. Bu faktorlar İnternetdən əldə olunan zərərli məlumatlardan istifadəçini qorumaq üçün texnoloji üsullardan istifadəni zəruri edir.

İnternetdəki zərərli məlumatlardan istifadəçilərin qorunması üçün əsas texniki tədbir vasitəsi kimi məlumatın filtrasiyasından istifadə edilir. Məlumat filtrasiyası sistemlərinin malik olduğu xüsusiyyətlərin müxtəlifliyi bu sistemlərin qurulmasını fərqli yollarla həyata keçirməyə imkan verir [1].

Kontent filtrasiyası müəyyən sözləri, şəkilləri və s. onlayn məzmunu ekranlaşdıran və bloklayan proqramdır [2]. İnternet məlumatları hər kəsə daha əlçatan olduğundan nəticə etibarilə

şəbəkədə olan bütün faydalı və ya zərərli məlumatlara açıq giriş mümkündür. Ona görə də ədəbsiz, təhqiredici ifadələr, jarqon danışıqlar, vulqar sözlər daxil edilmiş materiallarla uşaqların qarşılaşma ehtimalı daha çoxdur. Kontent filtrasiyası istifadəçinin müəyyən İnternet resurslarına girişini məhdudlaşdıran, İnternet saytlarını süzgəcdən keçirmək üçün hazırlanmış bir "hardware" modulu və ya bir proqramdır. Kontenti filtrasiya edən vasitələr bütün İnternet trafikinin keçdiyi şəbəkənin hissələrinə yerləşdirilir.

Məzmun filtrləri, konkret kateqoriyaya aid olan məlumat nəzərə alınmaqla, veb səhifələri və e-poçt mesajlarını yoxlayaraq uyğunsuz hesab edilən məlumatların istifadəçilərin kompüterlərində görünməsini məhdudlaşdırır.

Kontentin filtrasiya siyasəti dedikdə, ümumiyyətlə informasiya təhlükəsizliyini təmin etmək məqsədi ilə serverlərə daxil olan xüsusi filtrlərin yerinə yetirdikləri funksiyalar nəzərdə tutulur. Fərqli səviyyələrdə və müxtəlif növ şəbəkələrdə informasiya mənbələrinə girişi əngəlləmək üçün çoxlu sayda proqram və aparat vasitələrinin olmasını özündə ehtiva edir. Həmçinin istifadəçilər qarşısında müəyyən vəziyyətlərdə həm texniki, həm də iqtisadi baxımdan yeni vəzifələr qoyur.

Kontent filtrasiyasının prinsipi, tələb olunan saytın URL-ni adi ifadələrdən istifadə etməklə qara siyahılar tərtib edərək onların yoxlanılmasından ibarətdir. Zərərli məlumatlarla zəngin informasiya mənbələrinin sayı sürətlə artdığından belə siyahıların daim yenilənməsinə ehtiyac yaranır.

Məqalədə kontent filtrasiyasının tətbiqi üsulları şərh edilir. Kontent filtrasiyasının yerinə yetirilməsi sahəsində müxtəlif ölkələrin həyata keçirdiyi siyasətlər müzakirə olunur. Qabaqcıl elmi nəşrlərin mövzu ilə əlaqədar işləri araşdırılır, problemlər müəyyənləşdirilir.

Veb-kontent filtrasiyasının istiqamətləri

Günümüzün reallığı belə deməyə əsas verir ki, müasir uşaqlar rəqəmsal mühitdə böyüyürlər. İnformasiya cəmiyyətinin inkişaf etdiyi bir dövrdə təhsil sistemində İnternetdən geniş istifadə olunur. Belə bir şəraitdə təhsil müəssisələrində veb-məzmunun filtrasiyası məsələsi aktualdır. Məhdudlaşdırıcı tədbirlər uşağın məktəbdə müvəffəqiyyət dərəcəsinin təhlilinə və ya onun sağlamlığının vəziyyətinə əsasən qəbul edilə bilər. Məzmun və URL filtrasiyasını yalnız kitabxanalarda, məktəblərdə və universitetlərdə deyil, uşaqların İnternetə daxil ola biləcəkləri bütün müəssisələrdə tətbiq etmək məqsədəuyğundur. Bu zaman məktəb məlumat bazası və ya elektron sağlamlıq kartı vasitəsilə şagirdin biometrik məlumatlarından istifadə edilə bilər.

Məlumdur ki, uşaqlar smartfon, telefon və digər rəqəmsal vasitələrlə istər-istəməz sosial şəbəkələrə, forumlara, bloqlara və s. virtual məkanlara daxil olur və bu zaman zərərli kontentlə qaşılaşma halları baş verə bilər. Təhsil müəssisələrində ziyanlı kontentin filtrasiyasının təşkili korporativ şəbəkə mühitində bu problemin həllinə kömək edə bilər. Bununla da uşaq və yeniyetmələrin sağlamlığına, psixologiyasına dəyən zərərin qarşısı nisbətən alınar. Digər məkanlar (İnternet kafe, ev və s.) haqqında isə bunu demək çətindir.

Hazırda kibertəhlükəsizliyin təmin olunmasında kifayət qədər problemlər mövcuddur. Bu faktlara əsaslanaraq demək olar ki, həddindən artıq təhqiredici və zərərli saytları daha dəqiq müəyyənləşdirə biləcək, məzmunun effektiv şəkildə filtrasiyasını həyata keçirən sistemlərə böyük ehtiyac var. Beləliklə demək olar ki, İnternetə çıxışı idarə etmək üçün veb-saytın məzmunun filtrasiyası təkcə hər hansı zərərli kontentin qarşısının alınması deyil, eyni zamanda kibertəhlükəsizliyin qorunmasının vacib bir elementidir [3]. Veb-kontentin filtrasiyasından informasiya təhlükəsizliyi məsələlərinin həllində geniş istifadə olunur. Onlardan istifadədə məqsəd məxfi məlumatların yayılmasının qarşısını almaq, istifadəçilərin fərdi məlumatlarına müdaxiləni məhdudlaşdırmaqdan ibarətdir. Ondan, həmçinin spam və viruslarla mübarizədə, poçt resurslarından sui-istifadə hallarının qarşısının alınmasında da effektiv mübarizə üsulu kimi istifadə olunur.

Veb-kontent filtrasiyası bir neçə səviyyədə həyata keçirilir. Bunlara dövlət, provayder, İnternet-şlüz və fərdi kompüter səviyyəsində filtrasiyanı aid etmək olar [4–7].

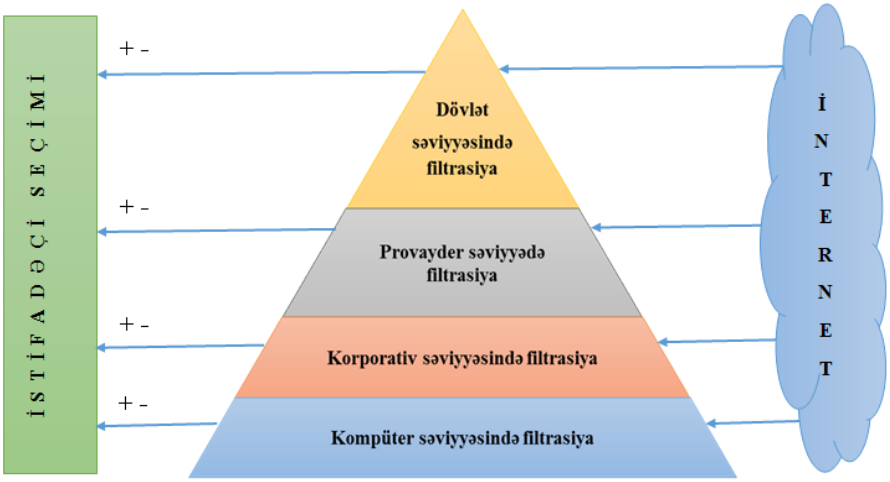
Dövlət səviyyəsində filtrasiya. Beynəlxalq miqyasda filtrasiya olmaqla, daxil olan İnternet trafikinin məzmununun süzgəcdən keçirilməsini həyata keçirən mərkəzləşdirilmiş bir dövlət yanaşmasıdır. Bu tam nəzarəti yerinə yetirən və dövlətin informasiya məkanının təhlükəsizliyini nəzərdə tutan vahid bir senzura yanaşmasıdır. Lakin belə süzgəclərin tətbiq edilməsi çox yüksək maliyyə xərcləri tələb edir.

Provayder səviyyəsində filtrasiya. Provayderlər tərəfindən dövlət qeydlərinə, məhkəmə qərarlarına diqqət yetirilərək və qadağan edilmiş mənbələrin siyahısını yaratmaqla həyata keçirilir. Bu səviyyədə filtrasiyanın xərcləri nisbətən aşağı olmasına baxmayaraq, kifayət qədər yüksək etibarlıdır. Lakin İnternet resurslarına çıxış zamanı məlumatın emal sürəti aşağı olur.

Korporativ səviyyədə filtrasiya. Daha çox dövlət və təhsil müəssisələrində, özəl şirkətlərdə istifadə edilir. Xüsusi proqram təminatını quraşdırmaqla və ya qaydalar tətbiq etməklə məzmunu izləmək mümkündür, eyni zamanda İnternetə çıxışı sürətlidir. Bu səviyyədə filtrasiya yüksək biliklərə malik mütəxəssislər heyətinin olmasını tələb edir.

Kompüter səviyyəsində filtrasiya. Kiçik təşkilatlarda, evdə fərdi kompüterlər üçün istifadə olunur. Bu zaman proqram birbaşa istifadəçilərin kompüterlərinə quraşdırılır. Bu nisbətən ucuz başa gələn filtrasiya üsuludur. Lakin belə proqramlar zaman keçdikcə köhnəlir və aktuallığını itirir. Bir çox hallarda virusların hücumuna məruz qalaraq düzgün işləmir.

Veb-kontent filtrasiyasının modeli Şəkil 1-də verilmişdir.



Şəkil 1. Veb-kontent filtrasiyasının səviyyələri

Veb-kontentin bütün səviyyələrdə filtrasiyası maliyyə cəhətdən bahalıdır və informasiyanın əldə edilməsi sürətinin azalmasına təsir edir. Bu səbəbdən filtrlərin hamısının deyil, müəyyən hissəsinin istifadə olunması daha məqsədəuyğundur. Şəkil 1.-də göstərilən "+" və "–" işarələri onu göstərir ki, filtrasiya səviyyəsinin seçilməsi istifadəçiyə həvalə edilir. Burada "+" işarəsi istifadəçi tərəfindən seçilən və istifadə olunan filtrlərə verilir. "-" işarəsi isə bunun əksinə olan prosesdir.

Yuxarıda göstərilən filtrlərdən başqa URL filtrasiyasından da istifadə edilir. URL filtrasiyası əsasən, kompüter səviyyəsində yerinə yetirilir ki, bu da vaxta qənaət etməklə ucuz başa gəlir. URL filtrasiyasından istifadə xarici təhdidləri bloklamaqla təhlükəsiz tərkibə keçməyə imkan verir. Hal-hazırda, uyğun olmayan məzmundan qorunma probleminin həlli üçün statik və dinamik filtrasiya yanaşmaları da mövcuddur.

Statik yanaşmanın əsas nüvəsi qara və ağ siyahıların tətbiqi ilə daim yenilənən məlumat bazaları əsasında arzuedilməyən veb-resursların bloklanmasıdır. Bu yanaşmalar arasındakı fərq yalnız "qara" və "ağ" siyahıların yaradılması, çeşidlənməsi, qruplaşdırılması, həmçinin səhifənin analiz edilməsində olan kiçik dəyişikliklərdir [8].

Dinamik yanaşma URL filtrasiyasına alternativdir. İstənilən sayta giriş zamanı kontent (İnternet saytının məzmunu, ümumiyyətlə, bir domen adı, müxtəlif metadata, mətn, şəkillər və s. ola bilər) dərhal analiz edilir. Uyğunsuz kontent aşkarlanmış saytın səhifələrinin brauzerə yüklənməsi bloklanır.

Dinamik kontent filtrasiyasında vacib olan elementlərdən biri mətn komponentini təhlil edən alqoritmlərdir. Bu alqoritmlərin vəzifəsi, təhlil olunan səhifə mətninin müəyyən bir mövzuya uyğun olub-olmamasını müəyyən etməkdir. Bu isə qərarverməni sürətləndirir və uyğunsuz məzmunun dəqiqliklə seçilməsinə şərait yaradır. Aydın olur ki, səhifənin mətni arzuolunmaz mövzulardan birinə uyğundursa, istifadəçinin bu səhifəyə girişi bloklanır [9].

İnternet kontentinin filtrasiyası sahəsində xarici ölkələrin təcrübəsi

İnternetə nəzarət məsələsi son onilliklərin aktual mövzularındandır. İnternet şəbəkəsinin dinamikliyi, informasiya axını və qlobal xüsusiyyətlərə malik olması şəbəkədəki məlumatların idarə edilməsində müəyyən çətinliklər yaradır. Müxtəlif kontent filtrlərindən istifadə edən ölkələrin sayı ilbəil artmaqdadır.

İnternetin imkanlarının artması, sürətli inkişafı müxtəlif növ onlayn xidmətlərin yaranmasına və təşəkkülünə səbəb oldu. Bu prosesin genişlənməsi, elektron ticarətin populyarlıq qazanması İnternetdə hüquqi münasibətlərin tənzimlənməsi üçün qanun normalarının tətbiq olunmasını tələb edir. Müxtəlif ölkələrdə İnternetin yayılmasından asılı olaraq məzmun filtrasiyası ilə bağlı fərqli siyasətlər həyata keçirilir. İnternetin yayılmasından asılı olaraq hər bir ölkənin öz qanunları və filtrasiya sistemləri mövcuddur. Buraya dövlət tərəfindən məzmunun süzülməsinə nəzarət edən mərkəzləşdirilmiş bir yanaşma daxildir [10].

Fransada Təhsil Nazirliyi iki "qara siyahı" tərtib edərək məktəblərdə məzmunun avtomatlaşdırılmış və mərkəzləşdirilmiş kontent filtrasiyasını reallaşdırır. Burada, birinci siyahıda pornoqrafik resurslar, ikincidə isə irqçiliyi və antisemitizmi təbliğ edən saytlar qeyd edilir [11].

Kanadada "Təmiz əlaqə" layihəsi çərçivəsində 2006-cı ildən başlayaraq proqramda könüllü olaraq iştirak edən provayderlər "qara siyahı"ya keçidləri əngəlləyirlər. Bu siyahılar Kanadada Uşaqların Müdafiəsi Mərkəzində analitiklər tərəfindən tərtib edilir. Resursun necə bloklanacağına təchizatçılar özləri qərar verirlər (IP ünvanı və ya domen adı) [12].

Rusiyada 2012-ci ilin iyul ayında Dövlət Duması ikinci və üçüncü oxunuşda ölkədə beynəlxalq hüquq və dövlət tərəfindən zərərli hesab olunan saytların vahid reyestrinin yaradılması haqqında qanun qəbul etdi. Həmin ilin noyabr ayında zərərli məzmunun qanunvericilik səviyyəsində tənzimləməsi üçün filtrasiya tətbiq edilmişdir [13] .

Almaniyada əksər axtarış sistemləri (Google, Lycos Europe, MSN Deutschland, AOL Deutschland, Yahoo!, T-Online və T-info) "Multimedia xidmət təminatçıları üçün könüllü özünü idarəetmə" müqaviləsinə qoşulmuşdur. Federal Media Resursları İdarəsi tərəfindən gənclər üçün zərərli hesab olunan veb saytların siyahısı tərtib edilir və onlara giriş bloklanır [13].

Çin ən çox kontent filtrasiyasının tətbiq olunduğu ölkədir [14,15]. Bu ölkədə çox sayda İnternet resursları fərqli səbəbdən bloklanmışdır (məs. Vikipediya, Youtube, Facebook, BBC və s.). Ayrı-ayrı veb-saytların bloklanması milli səviyyədə həyata keçirilir və ölkənin siyasi platforması ilə əlaqəlidir. İnsan hüquqları, müxalif siyasi hərəkatlar, Tayvan və Tibetin müstəqilliyi ilə əlaqəli İnternet məkanında mövcud veb-resursların ölkənin sosial-siyasi tarazlığını pozduqları səbəb göstərilərək hakimiyyət orqanları bu bloklanmaların düzgün olduğunu bildirir. Ölkə vətəndaşlarını "ziyanlı" veb-kontentdən qorumaq üçün Çində "Zərərli Məlumat İdarəetmə Mərkəzi" yaradılmışdır. Bu mərkəz ölkədə milli səviyyədə İnternet filtrasiyasını həyata keçirən orqandır. Çin əhalisinin 1,5 milyarda yaxın olduğunu və əhalinin çox hissəsinin mobil telefonlardan və İnternet şəbəkəsindən istifadəsini nəzərə alsaq veb-kontentin milli səviyyədə filtrasiyasının çox mürəkkəb olması və dövlətə böyük maliyyə vəsaiti hesabına başa gəlməsi aydın məsələdir. Buna baxmayaraq, ölkə əhalisinin virtual məkanda fəliyyətinə nəzarət etmək mümkün

olur. Əsasən pornoqrafiya, separatçı məlumatları təbliğ edən veb-resurslara və dövlət siyasətinə qarşı yönəlmiş materialların yayılmasına filtrasiya tətbiq edilir.

İngiltərə Avropada məzmun filtrlənməsinə görə ən sərt tədbirləri tətbiq edir. Qadağan edilmiş İnternet məzmunu operator səviyyəsində bloklanır. Hətta Britaniya qanunları provayderlərdən qadağan olunmuş veb saytlara girişi dayandırmaq üçün tədbirlər görüb-görmədikləri barədə hesabat vermələrini tələb edir.

İnternet xidməti təqdim edənlər isə İnternet İzləmə Fonduna (IWF) və polisə şübhəli istifadəçilər və şəbəkə konfransları barədə məlumat göndərirlər. Bu bütün provayderlərə uşaq pornoqrafiyasının yayılması üzrə filtrasiya olunmasına aid edilir [13,15].

İranda kontent filtrasiyası provayder səviyyəsində yerinə yetirilir. İnternet tənzimləyici orqan kimi İnternet Senzura Komitəsi fəaliyyət göstərir. 2004-cü ildə İranda ”İnternetdəki cinayətlərə görə cəza haqqında qanun” qəbul edilmişdir. Buraya İnternet kontentin filtrasiyası nəticəsində dövlət siyasətinə zidd olan resuslar, homoseksualığı təbliğ edən saytlar, qadın hüquqlarını müdafiə edən veb-resurslar, pornoqrafiya və müəyyən siyasətin təbliği daxildir. İrandakı hər bir provayder (ISP) öz İnternet məzmunu filtrləmə sistemini tətbiq edir. Bu səbəbdən fərqli İSP-də fərqli məzmun filtrləmə profilləri vardır [16] .

Kubada ümumiyyətlə ölkə vətəndaşlarına İnternetdən istifadə ilə əlaqəli çoxlu qadağalar qoyulur. Kuba vətəndaşlarının Facebook və WhatsApp kimi sosial media platformalarından istifadəsinə yalnız 2018-ci ilin sonlarında, 3G texnologiyalarının inkişafından sonra icazə verilmişdir. Hətta, məlum olmayan bir səbəbdən ölkədə Skype belə bloklanır. Səlahiyyətlilərə və həkimlərə isə xüsusi icazə ilə İnternet şəbəkəsinə daxil olmaq olar. İnternet filtrasiyası bir neçə metodla işləyir və hər bir şirkət özünün uyğun hesab etdiyi metodan istifadə edir [15]. Kubada insan hüquqlarının pozulmasını işıqlandıran və ya siyasi sistemi tənqid edən yazarlara və bloqgerlərə qarşı bloklar da daxil olmaqla ciddi senzura mövcuddur. Belə qadağalar daha çox yerli təşkilatlara təsir göstərir, halbuki bir çox xarici satış məntəqələrinə bu icazələr verilir. Bu ölkədə İnternetdən istifadənin az da olsa artmasına baxmayaraq, İnternetdən istifadə hələ də baha başa gəlir [16].

Kontentin filtrasiyası məsələsi ilə əlaqədar bəzi elmi yanaşmalar haqqında

Qlobal şəbəkə istifadəçilərinin, əsasən də uşaqların onlayn mühitdə zərərli məzmunla qarşılaşma təhlükəsi getdikcə artır. Bu qarşılaşma erotika, təcavüz, zorakılığa, terrora çağırışlar, ziyanlı şəkil və videolar, onlayn cinsi istismar, jarqon ifadələr və s. mövzuları əhatə edir ki, bütün bunlar uşaqların psixikasına zərər vurmaqla yanaşı informasiya ekologiyasını korlayır. Bu problemi həll etmək üçün uşaqların belə məlumatlara girişini məhdudlaşdıran proqram vasitələrinin inkişafına yönəlmiş, İnternetdən daxil olan informasiya trafikindən uyğunsuz məzmunun seçilməsi, süzülməsi və istifadəçiyə təqdim edilməsinin qarşısının alınması ilə bağlı elmi araşdırmaların sayı artmaqdadır.

Hazırda süni intellekt metodlarından istifadə etməklə bu tip məsələlərin həlli üçün müxtəlif yanaşmalar vardır. Belə ki, obrazların tanınması üsulları vasitəsilə uşaqların İnternet üzərindən cinsi istismarını həyata keçirən, zorakılıq elementləri olan fotoşəkilləri və s. təbliğ edən saytları bloklamaq üçün təkliflər verilmişdir. Həmçinin təbii dildə işlənən jarqon ifadələri, qeyri-etik danışıqları özündə ehtiva edən səhifələrdə olan mətnlərin təhlili əsasında saytlara girişi məhdudlaşdırmaq üçün metodlar işlənilmişdir. Problemin həlli ilə bağlı son illər bir çox tədqiqatlar aparılır və əsasən də virtual mühitdə zorakılıq, irqçilik, terrorizm və s. kimi arzu edilməyən davranışları təbliğ edən veb-resursların araşdırılması üçün müxtəlif metod və alqoritmlər təklif olunur.

İnternet istifadəçisinin tələbinə uyğun olmayan veb məzmunun aşkarlanması və filtrasiyası tez-tez mətn təsnifatı problemləri kimi formalaşdırılır. Mətn təsnifatı maşın təlimində daha maraqlı və geniş tədqiq edilmiş bir sahədir. Bununla əlaqəli xeyli elmi araşdırmalar vardır. Məsələn, text maining və klasterləşmə metodlarından istifadə etməklə internetdə terroristlərin aşkarlanması [17],

genetik alqoritmlərdən istifadə etməklə onlayn mühitdə informasiya müharibəsi aparan gizli sosial şəbəkələrin aşkarlanması [18] və s. tədqiqatlar mövcuddur.

Digər tədqiqatda maşın təlimi metodlarına əsaslanan pornoqrafik veb-saytların təsnifatı və WebGuard filtrasiya sistemi təklif edilir [19]. Burada semantikanı daxil etməklə təsnifatın səmərəliliyini, dəqiqliyini artırmaq və saxta pozitivləri azaltmaq üçün yeni təsnifat modelləri verilir. Xüsusiyyət vektoru çıxarmaq üçün veb-səhifələrin mətninin məzmunu, şəkilləri və URL ünvanının birgə kombinasiyasından istifadə edilir. Araşdırmada fərziyyələrin doğruluğunu yoxlamaq üçün eksperimentlərin aparılmasında ümumilikdə 400 veb-səhifədən istifadə olunmuşdur.

Kontentin filtrasiyasının keyfiyyətli yerinə yetirilməsi üçün digər yanaşmalarda maşın təlimi metodundan istifadə təklif olunur [20]. Bu metod filtrasiya üçün istifadə olunan funksiyaları minimallaşdırmaqla və veb-kontentin xüsusiyyətlərini nəzərə almaqla, dəqiqliyə zərər vermədən verilənlərin emalının sürətini artırır. Kontentin filtrasiyası məhdud qurğularla aparılsa da təklif olunan metod daha effektiv hesab olunur.

Pornoqrafik məzmun daşıyan kontentlərin ziyanlı olduğunu nəzərə alaraq rəqəmsal görüntünün emalı əsasında İnternetdə pornoqrafik məzmunun filtrasiyası təklif edilir [21]. İnternetdə pornoqrafik məzmunun aşkarlanması üçün müştəri-server modelinə əsaslanan iki tətbiqdən istifadə olunur. Müştərilərin daxil olduğu hər bir URL barədə məlumat verilir və server həmin URL daxilində aşkar edilmiş hər görüntünü emal edir. Eksperimentlərin aparılmasında 68 veb-səhifəyə baxılmış 5 təsnifat alqoritmindən (SVM,WIPE, Jones-Rehg, Fleck-Forsyth, TheNudity Detection Algorithm, RSOR Algorithm) istifadə edilmişdir. Rəqəmsal görüntülərdə çılpaqlığı aşkar etmək üçün RSOR alqoritminin daha effektiv nəticə verdiyi göstərilir.

Ədəbiyyat [22]-də mətn və struktur təhlilindən istifadə etməklə "WebAngels filter" adlı veb məzmun aşkarlama və filtrasiya sistemi təklif edilir. "WebAngels filter" veb-sayt təsnifatı üçün bir neçə məlumat alqoritmlərini birləşdirmək üstünlüyünə malikdir. İşdə maşın təlimi metodlarından istifadə etməklə filtrləmə performanslarını necə inkişaf etdirmək müzakirə olunur.

[23]-də veb-kontentdən mövzunun aşkarlanması, modelləşdirilməsi və sentiment analizini əks etdirməklə yanaşmalar təklif olunur. İnternetdə nifrət və zorakılıq məzmunu ifadə edən kontentin aşkarlanmasını həyata keçirən filtrasiya üsulu təklif edilir.Veb-məzmun təsnifatında mövzu təhlili və sentiment analiz ilə mübarizə aparılmasının perspektivli potensialı təklif edilir. Veb-məzmunun filtrasiyası və təhlükəsizliyi üçün mətn təsnifatı əsasında sinif balanssızlığı problemini həll etmək üçün təkmilləşdirilmiş bir yanaşma verilir. Bu işdə eksperimentlər zamanı 50 kateqoriyadan ibarət 80000 veb-səhifənin analizindən istifadə olunmuşdur.

Digər tədqiqatda spamların filtrasiyası problemi və onun həllinə ən çox rast gəlinən yanaşmalar müzakirə olunur [24]. Problemin həlli üçün süni intellekt metodlarına, xüsusən də süni neyron şəbəkəsinə əsaslanan bir yanaşma təklif olunur. Bu yanaşma, mesajların əhəmiyyətli xüsusiyyətlərini vurğulamaq, model parametrlərini təyin etmək, təsnifatın düzgünlüyünü qiymətləndirmək üçün təsnifatçıdan öyrədici test nümunələrinin hazırlanmasını tələb edir.

Yahoo şirkəti tərəfindən təhqiredici və uşaqlar üçün zərərli olan, arzuolunmaz NSFW (not suitable/safe for work) kontentli şəkillərin, əsasən pornoqrafik şəkillərin konvalyusiya neyron şəbəkəsindən (convolutional neural network, CNN) istifadə etməklə klassifikasiyası modeli təklif edilmiş və onun açıq kodu yaradılmışdır [25].

Bəzi tədqiqatlarda ziyanlı məzmunun qarşısının alınmasında dərin CNN-ə əsaslanan üsullardan istifadə edilir. Belə ki, pornoqrafik təsvirlərin aşkarlamasında neyron şəbəkələrdən istifadənin daha effektiv nəticə verdiyindən, tətqiqat [26]-da iki strategiyaya əsaslanan təlim alqoritmi verilir. Təklif edilən birinci alqoritm sabit olmayan tənzimləmə strategiyasına əsaslanır. Bu strategiyanın məqsədi təlim məlumatlarını uyğun vaxtda tənzimləməkdən ibarətdir. Eksperimentlərin aparılmasında sürüşmə pəncərə alqoritminə əsaslanan sürətli şəkildə görüntünü klassifikasiya edən metod təklif edilir [26].

Veb-kontentin filtrasiyası ilə əlaqədar tədqiqatların araşdırılması onu göstərdi ki, bu gün hesablama metodologiyası və texnologiyasının inkişafı nəticəsində İnternet resurslarının təhlili üçün bir çox yeni və daha səmərəli metod və alqoritmlər mövcuddur. Mətn, şəkil, səs və video şəklində olan bu resursların analizi və onların içərisindən ziyanlı kontentin filtrasiyası nəticəsində aşkarlanması mərhələli prosesdir. Böyük verilənlərdən ibarət kontenti səmərəli filtrasiya etmək üçün yuxarıda göstərilən yanaşmalar da nəzərə alınmaqla dinamik, az vəsait tələb edən və asan idarə olunan filtrasiya sisteminə ehtiyac vardır. Tədqiqatlar göstərir ki, veb-kontentin filtrasiyasında əsasən neyron şəbəkələr, maşın təlimi, ekspert sistem, text mining və dərin təlim metodlarından geniş istifadə olunur.

Nəticə

Son dövrlərdə müxtəlif təlim metod və vasitələrindən istifadə etməklə veb-kontentin analiz edilməsi, ziyanlı informasiyanın aşkarlanması, filtrasiya olunması, veb səhifələrin avtomatik təsnifatı geniş öyrənilməkdədir. Bu problemlə əlaqəli yüksək səviyyəli elmi nəşrlərin sayı getdikcə artmaqdadır. Belə demək mümkündür ki, bu tədqiqatlarda daha yaxşı təsnifat performansları üçün yeni təsnifat modelləri təklif edilir. Lakin araşdırmalar göstərdi ki, İnternetdə veb-resursların sayı artdıqca və "Big Data" problemi aktuallaşdıqca, İnternet istifadəçiləri arasında azyaşlıların sayı çoxaldıqca veb-kontentin filtrasiya olunması daha dəqiq, sürətli və effektiv analiz metodlarını tələb edir. Nəzərə alsaq ki, bu filtrasiya sistemləri əsasən uşaq auditoriyasını da əhatə edir, onda burada İnternet asılılıq məsələsi də nəzərə alınmalıdır. Belə olan halda, bu sistemdə sentiment analiz və verilənlərin sanitarizasiyası metodlarından istifadə etmək məqsədəuyğundur. Uşaq və yeniyetmələrin İnternet məkanda təhlükəsizliyini təmin etmək məqsədilə veb-kontentin filtrasiya olunması problemi hər bir dövlətin qarşısında duran vacib məsələlərdəndir.

Ədəbiyyat

1. Гут Р. В., Кирпичников А. П., Ляшева С. А., Шлеймович М. П. Методы Ранговой Фильтрации В Системах Видеонаблюдения // Вестник технологического университета, 2017, т. 20, №17, с. 71–73.
2. Online Safety & Content filtering, https://www.iinet.net.au/about/legal/filtering
3. Jinpeng W., Xiaolan Z, Glenn A.,Vasanth B., Peng N. Managing security of virtual machine images in a cloud environment // Proceedings of the 2009 ACM workshop on Cloud computing security, 2009, pp 91–96.
4. Alguliyev R., Ojagverdieva S., Conceptual Model of National Intellectual System for Children Safety in Internet Environment // Computer Network and Information Security, 2019, vol.11, No.3, pp. 40–47.
5. Фильтрация сетевого трафика , https://www.carbonsoft.ru
6. Типы контент-фильтров, https://xserver.a-real.ru/support/useful/tipy-kontent-filtrov
7. Чемодуров А. С., Карпутина А. Ю. Защита интернет-шлюза и фильтрация сетевого трафика корпоративной сети // «Концепт», 2015, № 1, с. 96–100.
8. Смирнов И.В., Соченков И.В., Суворов Р.Е., Тихомиров И.А. Фильтрация контента в интернете: современный уровень и перспективы // Искусственный интеллект и принятие решений, 2013, №2, с.54–62.
9. Стрекалов И.Э., Новиков А.А., Лопатин Д.В. Методы динамической фильтрации веб-контента // Вестник ТГУ, 2014, т.19, вып. 2, с. 668–669.
10. Контентная фильтрация: зачем и как это делать, https://www.habr.com/ru/company/smart_soft/blog/273095
11. French Safer Internet Centre. "No to harassment" – A French national plan of action against cyberbullying, https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=512910

12. Internet Filtering in the United States and Canada in 2006-2007, https://www.opennet.net/studies/namerica2007
13. Фильтрация и блокирование интернет-контента: мировой опыт, https://www.ria.ru/20120711/697151590.html
14. Paul B. Countries Have the Strictest Internet Censorship?, https://www.readwrite.com/2019/07/01/which-countries-have-the-strictest-internet-censorship
15. Фильтрация контента, https://www.sites.google.com/site/kyrsbez/48-1
16. Фильтрация контента в Интернете. Анализ мировой практики, http://civilfund.ru/Filtraciya_Kontenta_V_Internete_Analiz_Mirovoy_Praktiki.pdf
17. Alguliyev R.M., Aliguliyev R.M., Niftaliyeva G.Y. Filtration of Terrorism-Related Texts in the E-Government Environment //Cyber Warfare and Terrorism, 2018, issue 4, vol. 8., pp. 35–48.
18. Alguliyev R.M., Aliguliyev R.M., Alakbarova I.Y. Extraction of hidden social networks from wiki-environment involved in information conflict // International Journal of Intelligent Systems and Applications (IJISA), 2016, vol 8, no.2, pp. 20–27.
19. Hammami M., Chahir Y., Chen L. WebGuard: web based adult content detection and filtering system. Proceedings of the IEEE / Proceedings of the WIC International Conference on Web Intelligence, 2003, pp.574–578.
20. Suvorov R., Sochenkov I., Tikhomirov I. Training Datasets Collection and Evaluation of Feature Selection Methods for Web Content Filtering // Artificial Intelligence: Methodology, Systems, And Applications, 2014, vol. 8722, pp.129–138.
21. Colmenares-Guillen LE., Velasco FJA. Filter for Web Pornographic Contents Based on Digital Image Processing //Combinatorial optimization problems and informatics, 2016, vol.7, №2, pp. 13–21.
22. Guermazi R., Hammami M., Hamadou AB. WebAngels filter: A violent Web filtering engine using textual and structural content-based analysis /Computer Science, 2008, vol 5077, pp.268–282.
23. Liu S., Forss T. Text Classification Models for Web Content Filtering and Online Safety / Proceedings of the 2015 IEEE International Conference on Data Mining Workshop, 2015, pp. 961–968.
24. Ларионова А.В., Хорев П.Б. Метод фильтрации спама на основе искусственной нейронной сети // Науковедение, 2016, том 8, №3, с. 1–7.
25. Open Sourcing a Deep Learning Solution for Detecting NSFW Images, https://www.yahooeng.tumblr.com/post/151148689421/open-sourcing-a-deep-learning-solution-for
26. Nian F., Li T., Wang Y., Xu M., Wu J., Pornographic Image Detection Utilizing Deep Convolutional Neural Networks // Neurocomputing, 2016, vol. 2010, pp. 283–293.

УДК 04:37

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

Вопросы фильтрации веб-контента

В условиях обилия информации в последние годы проблема защиты интернет-пользователей от вредной (агрессия, терроризм, порнография, экстремизм и т.д.) информации стала более актуальной, т.к. возросло их влияние на социально-экономические процессы. Существуют различные научные подходы и технологии для защиты от вредоносной информации, определения ее источника, точного определения полезности веб-контентов. В статье представлена информация о сущности и преимуществах

широкоиспользуемого метода фильтрации контента, позволяющего различать вредоносный и полезный веб-контент, а также определяется уровень фильтрации веб-контента. Показана важность статического и динамического подходов к блокированию сайтов, содержащих вредоносный контент, и разницы между ними. Целью исследования является демонстрация важности использования метода фильтрации контента для решения проблем информационной безопасности, киберпреступности и других проблем, присутствующих в виртуальном пространстве, а также важность очистки веб-ресурсов от вредоносного контента.

При научном исследовании по данной теме были использованы метод анализа, сравнительный анализ и системный подход для выбора, фильтрации нежелательного контента из входящего информационного трафика Интернета.

Полученные в статье результаты могут быть использованы на платформе электронного правительства в учебных заведениях, национальных центрах безопасного интернета и др. местах для защиты детей от вредной информации.

Ключевые слова: *фильтрация веб-контента, информационная безопасность, вредоносная информация, уровень фильтрации, фильтрация URL.*

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

Web content filtering issues

Protecting users from harmful information (aggression, terrorism, pornography, extremism, etc.) on the Internet has become more topical in recent years in terms of information abundance and has affected the socio-economic processes around the world. There are various scientific approaches and technologies to protect against malicious information, to identify their source, to determine exactly which web content is useful or harmful. The article provides information on the essence and application benefits of a widely used content-filtering method to distinguish between harmful and useful web content, and defines the levels of filtering of web content. The essence of static and dynamic approaches for blocking the websites that contain malicious content and the difference between them are highlighted. The purpose of the study is to demonstrate the importance of effective use of the content-filtering method and to highlight the importance of cleaning the web resources from malicious content in solving information security, cybercrime and other problems existing in the virtual space.

The study uses a variety of analysis, comparative analysis and systematic approach methods that are directed at development of software tools that limit access of children to malicious information and select, filter, and prevent presentation of inappropriate content received from the Internet traffic.

The results obtained in the article can be used on the e-government platform in educational institutions, National Safe Internet Centers, etc. to protect children from harmful information.

Keywords*: Web content filtering, information security, malicious data, filtration level, URL filtering.*