

UOT[002:004]:316.774

MÜXTƏLİF KİBERTƏHLÜKƏSİZLİK KODLARI İLƏ KİBERTƏHDİDLƏRƏ QARŞI GÜCLÜ TƏHLÜKƏSİZLİYİN TƏMİN EDİLMƏSİ

¹Mirzəyeva G.R., ²Mirzəyev A.R., ³Allahyarova N.Z.

¹“Azərbaycan Dövlət Dəniz Akademiyası” PHŞ

²Bakı Ali Neft Məktəbi

³Azərbaycan Dövlət Neft və Sənaye Universiteti

E-mail: gulnar.mirzayeva@gmail.com, mirzayev.araz@gmail.com

Xülasə. Kiber dünyada texnologiyanın və internetin sürətli tərəqqisi inkişaf edən kibercinayətləri də özü ilə gətirir. Təhlükəsizlik kodları (captcha) bu cinayətlərin qarşısını almaq üçün yaradılmış təhlükəsizlik təbəqəsi kimi istifadə olunur. Bu, girişin istifadəçi tərəfindən edilib-edilmədiyini ayırd etmək üçün nəzərdə tutulmuş təhlükəsizlik mexanizmidir və zərərli bot programlarından qorunmaq üçün istifadə olunur. Bu səbəbdən girişin insan və ya bot proqramı tərəfindən edilməsi vacibdir.

Abstract. The rapid development of technology and the Internet in cyberspace entails the development of cybercrime. Security codes (captcha) are used as a layer of security created to prevent these crimes. This is a security mechanism designed to determine if a user is accessing or not and is used to protect against malicious bots. For this reason, it is important that the system is logged in by a human or a bot.

Аннотация. Быстрое развитие технологий и Интернета в киберпространстве влечет за собой развитие киберпреступлений. Коды безопасности (капча) используются в качестве уровня безопасности, созданного для предотвращения этих преступлений. Это механизм безопасности, предназначенный для определения того, осуществляется ли доступ пользователем или нет, и используется для защиты от вредоносных ботов. По этой причине важно, чтобы вход в систему осуществлялся человеком или программой-ботом.

Açar sözlər: turing, kibertəhlükəsizlik, Captcha, bot, təhlükəsizlik

Key words: turing, cybersecurity, Captcha, bot, security

Ключевые слова: тьюринг, кибербезопасность, Капча, бот, безопасность

Giriş. İnternet texnologiyalarının inkişafı və geniş yayılması ilə bu sistemlərin təhlükəsizliyi də mühüm elementə çevrilmişdir. Təhlükəsizliyə yönəlmiş əməliyyatlar inkişaf etdikcə, sistem zəifliklərinə qarşı mübarizə aparan zərərli proqramlar da ortaya çıxdı. Bu bot hücumlarının qarşısını almaq üçün doğrulama sistemləri lazımdır.

Turing testi ilk dəfə 1950-ci ildə Alan Turingin “Hesablama maşınları və kəşfiyyat” adlı məqaləsində qeyd edilmişdir. Turing testinin məqsədi kompüterin düşünüb-düşünmədiyini müəyyən etməyin mümkünlüyünü yoxlamaqdır. Turing testinə görə sual verənin sual verməklə respondentlərdən hansının kompüter, hansının insan olduğunu müəyyən etmək cəhdidir. Dindiricinin sualları yalnız klaviatura vasitəsilə yazmaqla göndərilir. Təkrar testlər nəticəsində müstəntiq cavabdehin insan olub-olmadığını müəyyən edir.

Məsələnin qoyuluşu. Təhlükəsizlik kodu (Captcha-Completely Automated Public Turing test for Computers and Humans Apart) avtomatik qeydiyyat, spam və ya zərərli bot proqramlarının qarşısını almaq üçün istifadə olunur.

Təhlükəsizlik kodu (captcha) internet səhifələrindəki formalara daxil olarkən, mesaj göndərərkən gündəlik internet istifadəsi zamanı bir çox yerdə rast gəlinən mürəkkəb kodlarla fərqli texnikalarla oxunması çətinləşdirilən insan və botları ayırd etmək üçün hazırlanmış bir layihədir.

Təsdiq olmadan təcavüzkarların seçdikləri veb-saytlara zərər verməsi, parol bərpa formalarına kobud güc hücumundan istifadə edərək parolları sındırması və botların mesaj formalarında reklam və ya zərərli paylaşımları paylaşması çox asan ola bilər. Bu vəziyyətlərin qarşısını almaq üçün oxunması çətin, əyri, trapezodial, fərqli rənglərdə olan və ya fərqli üsullarla dəyişdirilən bu doğrulama tətbiqləri, görüntü emal vasitələri və müəyyən edilə bilməyəcəyi düşünülmən bu doğrulama tətbiqləri ilə istifadə olunur.

Təhlükəsizlik kodu (captcha) təhlükəsizliyi və dizaynı bir çox işçi qrupları tərəfindən tədqiq edilmişdir. Mövcud təhlükəsizlik kodları (captcha) mətn əsaslı, şəkil əsaslı və səs əsaslı olaraq üç kateqoriyaya bölünə bilər. Mətnə əsaslanan Captcha adətən ingilis hərfləri və ərəb rəqəmlərinə əsaslanır və maşının tanınmasının qarşısını almaq üçün mürəkkəb təhrif, fırlanma və ya səs-küy müdaxiləsindən istifadə edir [1-3].

Mürəkkəb əyrilik: Mətn əsaslı captchalarda müəyyən edilməsi arzu edilir.

Fırlanma: Mətn əsaslı captchalardakı simvolların açıq şəkildə fırlandığı və hər simvolun fərqli fırlanma bucağı olduğu vəziyyətlərdə istifadə olunur.

Səs-küy: Mətnə əsaslanan captcha simvollarındakı simvoldan eyni və ya fərqli rəngli piksellərin və ya simvola bitişik piksellərin əlavə edilməsi arzuolunmazdır və OCR sorğularında oxunmasını çətinləşdirir.

Şəkil əsaslı və audio əsaslı Captcha kateqoriyası ilə müqayisədə mətn əsaslı Captcha ən çox istifadə edilən sxemdir. Bu geniş istifadə onun aşkar üstünlükləri ilə bağlıdır, həmçinin mətn əsaslı Captcha təhlükəsizlik kodlarının ən qədim formasıdır.

Təhlükəsizlik kodunun (captcha) inkişafı və növləri. Təhlükəsizlik kodu (captcha) tətbiqlərinin yayılması ilə kibercinayətkar qruplar tərəfindən təhlükəsizlik kodu (captcha) tətbiqləri inkişaf etdirildi və bununla da proqnozlaşdırılan virtual müharibə başladı. Bu qrupların daim inkişaf edən kiberhücumlarına qarşı çıxmaq üçün hazırlanmış təhlükəsizlik kodu (captcha) tətbiqləri daha mürəkkəb səviyyələrə çatır [2].

1. Sadə Təhlükəsizlik Kodu (captcha)

Bu növ Captcha çox sadə və səssiz mətn əsaslı Captcha-nın ilk nümunələrindən biridir. Bu cür təhlükəsizlik kodları (captcha) zərərli proqramlar tərəfindən xüsusi olaraq hədəf alındıqda çox asanlıqla yan keçə bilər.

2. Cari Təhlükəsizlik kodu (captcha)

Sadə Captcha-nın xakerlər tərəfindən sındırılması ilə, Captcha tərtibatçıları Captcha strukturlarının daha bulanıq, səs-küylü, əyri və təsviri müxtəlif ikona, qaralama və formalarla dolduran daha mürəkkəb variantlarını hazırlamağa başladılar.

3. Riyaziyyat Təhlükəsizlik Kodu (captcha)

Sadə riyazi əməliyyatlara əsaslanır, “8+5” cəminin tayıması kimi əməliyyatların nəticəsinin daxil edilməsi xahiş olunur. Məqsəd bütün ənənəvi botları bloklamaqdır. Lakin veb sahifəyə xas botlar sadəcə maneəni keçə bilər.

4. Kompleks Təhlükəsizlik Kodu (captcha)

Bu cür Captcha dizaynları müasir və təhlükəsiz olsa da, fərqli və daha çətin dizaynlara ehtiyac olduğunu iddia edərək, daha mürəkkəb dizaynlardan istifadə etməyə üstünlük verənlər də var. Bu dizaynın ən yaxşı nümunəsi kimi Quantum Random Bit Generator (IRB,2018) verilə bilər. Quantum Random Bit Generator xidmətinin üzvü olmaq istəyənlər kompleks Təhlükəsizlik kodunu (captcha) keçmək üçün kompleks modeli həll etməlidirlər. Bu isə öz növbəsində çox çətin prosesdir, vaxt baxımından idarəolunma problemi yarada bilər.

5. Obyekt Təhlükəsizlik Kodu (captcha)

Sistemlərini kiberhücumlardan qorunmaq üçün qoruyan tərəflərin bəziləri çətin təhlükəsizlik kodlarından (captcha) istifadəyə üstünlük verir, digərləri isə daha sadə, lakin hələ də təhlükəsizliyi

pozacağı düşünülməyən fərqli üsullardan istifadə edir. Bu cür Captcha növündə uyğunlaşma üslubunda olduğu kimi, müxtəlif bucaqlarda əyilmiş klassik hərf və rəqəmlərdən başqa, onun rəsmlərində iştirak etdiyi tətbiqlər də var.

6. Şəkil Təhlükəsizlik Kodu (captcha)

Təhlükəsizlik kodu (captcha) keçidi üçün istifadə edilən strukturlarda mənasız hərf-rəqəm birləşmələrindən istifadə məhdudiyyətləri aradan qaldırıldıqdan sonra obyektlərdən daha çox Security code (captcha) tətbiqlərində istifadə olunmağa başlandı. İnternet sürətinin və server saxlama imkanlarının artması ilə çox daha təhlükəsiz olduğu düşünülen və zəhlətökən olmayan şəkil Təhlükəsizlik kodu (captcha) daha çox istifadə olunmağa başladı.

7. Slider Təhlükəsizlik Kodu (captcha)

Tətbiqə daxil olmaq üçün sistemə daxil olan istifadəçilərdən slayderi sağa sürüşdürmələri xahiş olunur. Sürgü göndərmə seçiminə gətirildikdə, göndərmə düyməsi aktiv olur, beləliklə, keçid təmin edilir. Ancaq xüsusi ehtiyacları olan insanlar üçün bu təhlükəsizlik səviyyəsini məğlub etmək çətin olacaq. Bu cür istifadələr javascript və ya flash texnologiyalarından istifadə etdiyi üçün ehtiyat yoxlama mexanizmi tələb edir.

8. reCaptcha Təhlükəsizlik Kodu (captcha)

Google Təhlükəsizlik kodu (captcha) xidmətini satın aldıqdan sonra bu xidmətə yeni funksiyalar əlavə etdi. reCaptcha 2009-cu ildə təcavüzkarlar tərəfindən yaradılmış zərərli avtomatlaşdırılmış proqram botlarını bloklamaq üçün hazırlanmışdır. Mətn əsaslı məlumatların rəqəmləşdirilməsində istifadə edilmək üçün əldə edilən OCR çıxışlarını istifadəçilərə yönəldilməsi üçün reCaptcha kimi təhlükəsizlik kodu yenidən təşkil edildi. Doğrulama mərhələsində əvvəllər təsdiqlənmiş söz və ikinci naməlum söz göstərilir. Əvvəlcədən təyin edilmiş sözə uyğun olaraq, insan ayrı-seçkiliyi edildikdən sonra Google Kitabxanaları və digər reCaptcha yoxlamaları üçün ikinci sözü müəyyən edilir. Beləliklə, Captcha proqramlarının yoxlanılması zamanı daha etibarlı sistem keçidi təmin edilir.

Təhlükəsizlik kodu (captcha) ümumi məntiq və əməliyyat. Təhlükəsizlik kodu (captcha) proqramlarında captcha botların aşkar edə bilmədiyi təsadüfi şəkli serverdən alır və üzərindəki mətnin yoxlanılması üçün istifadəçidən onu müəyyən etməyi xahiş edir. Bu yoxlama tamamlanana qədər həm şəxs, həm də botlar sistemdə irəli gedə bilməz.

Buradakı əsas və vacib məntiq ondan ibarətdir ki, təqdim olunan görüntü yalnız insanlar tərəfindən qəbul edilməli və botların onu tanıya bilməyəcəyi şəkildə yaradılmalıdır.

Təhlükəsizlik Kodu (captcha) kimi şəkil yaratma ardıcılığı:

- Bitmap obyektı yaradılır;
- Bu bitmap obyektinin şrift və şrift kimi xassələri redaktə edilir;
- Təsadüfi obyekt yaradılır və bu təsadüfi obyektin diapazon dəyərləri yaradılır;
- Sonra təsadüfi dəyişən yaradılır;
- Bu təsadüfi sətir sessiyaya daxil edilir və müqayisə üçün istifadəçinin düzgün daxil olub-olmadığı yoxlanılır;
- Nəhayət, istəyə uyğun səs-küy əlavə edilir və istədiyiniz zaman simvol müəyyən bir bucaq altında fırlanır.

Əvvəlcə sadə olan bu tətbiq tərzı, OCR (Optik Xarakter Tanıma) adlı optik xarakter tanıma proqramlarının inkişafı və proqramların daha yaxşı nəticələr əldə etməsi ilə təkmilləşdirilmişdir.

Şəkillər yalnız insanlar tərəfindən müəyyən edilmir və qeyri-adekvat olaraq qalır. Əks tətbiqlərlə yarış zamanı təhlükəsizlik kodu (captcha) fərqli tətbiq üslubları ortaya çıxsə da, əsasən tətbiqlərin məntiqi həmişə eynidir. Bu məntiq Turing testinə əsaslanır [3].

Captcha (təhlükəsizlik kodu) kodunun sındırılması. Klassik Captcha üçün fon səs-küyü və ya şəklin üzərindən keçən düz xətlər bərpa ediləcək ilk elementlərdir. Rəng səviyyələrini rəng fərqləri ilə dəyişdirərək və səviyyə diapazonlarını açmaqla mətn fondan ayrılabilir. Optik xarakter identifikasiyası bütün mətn və ya xarakter və xarakter ayrılıyına qarşı bir neçə dəfə təkrarlana bilər. PWNtcha

- Captcha Dekoderi (Türinq Kompüteri Deyil, İnsan Antaqonistiyik) tətbiqinin məqsədi bir çox captcha modellərinin səmərəsizliyini aşkar etməkdir. PWNtcha bunu edən bir neçə proqramdan yalnız biridir.

Daha mürəkkəb hallarda, məsələn, simvolların arxasına qaranlıq fiqurların yerləşdirilməsi kimi sayt üçün çox xüsusi öyrənmə və ya təcrübə üsullarından istifadə edən süni neyron şəbəkələrindən istifadə edilməlidir.

Səs yoxlamaları aparılarkən fon səsləri və səslər insan səsi və hərf təriflərinə görə fərqləndirilə bilər və bu düzəlişlərin öhdəsindən gəlmək olar. Yenə də bu, süni neyron şəbəkəsi məlumat emalı vasitəsilə həyata keçirilə bilən bir prosesdir.

Tədqiqat metodu. Məqalədə Captcha növləri və Təhlükəsizlik kodu (captcha) tədqiqatlarına əsaslanaraq daha təhlükəsiz təhlükəsizlik kodu (captcha) kombinasiya testi təqdim olunur. Təklif olunan yanaşma əsasən üç mərhələdən ibarətdir. Birinci mərhələdə istifadəçinin Təhlükəsizlik kodu (captcha) ilə testini çətinləşdirməmək üçün sadə mətn əsaslı təhlükəsizlik kodu (captcha) ilə sınaqdan keçirilməsi xahiş olunur. İkinci mərhələdə mətn və şəkillərə əsaslanan daha çətin captcha testi birinci mərhələdəki test uğursuz olduqda təqdim olunur.

Üçüncü mərhələ ilk iki mərhələdən daha mürəkkəb və istifadəçi dostudur. Tətbiq etmək üçün müxtəlif əsaslı təhlükəsizlik kodu (captcha) təklif olunur. Bu yanaşma ilə istifadəçi ilə bot arasındakı fərqi asanlaşdırmaq və yaradılmış təhlükəsizlik kodunun (captcha) birləşməsi ilə bot proqramlarının alqoritmindən imtina etmək olar.

Təhlükəsizlik kodu (captcha) yaxın gələcək. Təhlükəsizlik kodu (captcha) tətbiqləri indi spamın qarşısını almağa çalışarkən, funksionallıqlarını itirərək istifadəçinin qarşısını alan və qıcıqlandıran strukturdan xilas olur və ReCaptcha nümunəsindəki kimi daha müasirləşir və işlək hala gəlir. Bu, tələbə bağlı bir inkişaf kimi görünərsə də, əslində məcburi bir hərəkətdir. Bu gün hətta təhlükəsiz deyilən uyğunlaşmalar kifayət qədər olmaya bilər və onları inkişaf etdirmək lazımdır.

Qırılan sistemlərdən sonra edilən təkmilləşdirmələr və inkişafalar əslində tərəflər arasında müharibənin zolağını bir pillə yüksəldir və bu, son nəticədə proqram dünyasının və bəşəriyyətin xeyrinədir.

Hal-hazırda geniş istifadə edilməsə də, gələcəkdə video təhlükəsizlik kodu (captcha) tətbiqləri qəbul ediləcək və inkişaf edən sensor ekran sistemləri ilə şəkil təhlükəsizlik kodu (captcha) inkişaf etdiriləcək və əl işarəsi, rəsm yoxlamaları və uyğunlaşdırmalar geniş istifadə ediləcəkdir. Xüsusilə Microsoft kimi proqram nəhənginin bu gün böyük əhəmiyyət kəsb edən təhlükəsizlik kodu (captcha) xidmətinin sındırılması bunun ən böyük göstəricisidir.

3D Təhlükəsizlik kodu (captcha) insan təxəyyülünə və məkan perspektivinə əsaslanır. Əsas ideya fərqi 3D modeli çevirmək və düzgün fırlanma mövqeyini tapmaqdır. İstifadəçinin vəzifəsi modeli döndərmək və düzgün müşahidə nöqtəsini tapmaq üçün Captcha-nı uğurla deşifrə etməkdir. Ziyarətçiləri xoş bir Captcha oyunu ilə əyləndirir. Şəkilləki çatışmayan parçaları tamamlamağa imkan verən kiçik bir tapmaca oyunudur.

PlayThru - CPATCHA əsaslı HTML5 oyunu, İnsan olduğunuzu sübut etmək üçün oyunu uğurla tamamlamalısınız. Bu, ingilis dilini başa düşən hər kəs üçün asan başa çatdırmaq üçün çox çətin olmayan bir Təhlükəsizlik kodudur.

Google Yeni Təhlükəsizlik Kodu (captcha) Layihəsi. Google bildirir ki, uzun müddətdir istifadə edilən reCAPTCHA təhlükəsizlik addımı saytları qoruyur, lakin bu olduqca çətin bir tətbiqdır. Bunu nəzərə alaraq, "Mən robot deyiləm" qutusunun yaxın gələcəkdə tamamilə gizlədiləcəyini və ziyarətçilərin məzmunu çatma vaxtını sürətləndirmək üçün "Görünməz reCaptcha"-nın olacağını açıqladı (Google,2017) .

Görünməz reCaptcha istifadəçilərin IP ünvanını və fonda (ekranda) siçan hərəkətləri kimi dəyişənləri izləmək üçün nəzərdə tutulmuşdur. Bununla da google səhifədəki şəxsin insan və ya bot olduğunu ayırd edə biləcək. Beləliklə, istifadəçilər "Küçə işarəsi olan meydanları seçin.", "Şəkilləri

ağaclarla qeyd et." seçimlərini edə bilərlər və istifadəçilərə "Ekranı rəqəmləri daxil edin." kimi sorğular göndərilməyəcək.

Maşın öyrənməsi və qabaqcıl risk analizinin birləşməsindən ibarət The Invisible reCaptcha-nın alqoritm strukturu təhlükəsizlik addımlarını çox daha sürətli yerinə yetirəcək və məzmunu ani girişi təmin edəcək [4].

Kiber təhlükələrə qarşı təhlükəsizlik kodu (captcha) test işi. Ümumiyyətlə, təhlükəsizlik kodu (captcha) sistemlərə daxil olmağa çalışan zərərli botlara qarşı fiziki dünyada olduğu kimi təhlükəsizliyi təmin edən, icazəsiz girişin qarşısını alan zireh kimidir. Bu kontekstdə qiymətləndirildikdə fiziki qoruma təmin edən zirehlər insanın daşıya biləcəyi qədər yüngüldür və nə qədər çox seçilsə, o qədər də istənilən dizayn və təsirlərə qarşı qorunur. Təhlükəsizlik kodu (captcha) zirehlər kimi davamlıdırsa, sistemin daşıya biləcəyindən daha az enerji sərf edirsə və istifadəçi dostudursa, onda tələb daha yüksək olacaq.

Təhlükəsizlik kodunun (captcha) keçmişdən bu günə qədər inkişafına nəzər saldıqda onun əsas məntiqi 3 əsas kateqoriyaya əsaslanır. Bunlar mətn, səs və şəkildir. Bu və ya onların birləşmələri götürülərək müxtəlif təhlükəsizlik kodları (captcha) yaradılmışdır. Bu yaradılmış Təhlükəsizlik kodu (captcha) bot proqramı, hətta ən çətin və mürəkkəb təhlükəsizlik kodunu (captcha) inkişaf etməkdə olan əksər texnoloji inkişaflarla, xüsusən də OCR sistemləri və maşın öyrənməsi, neyron şəbəkələri, dərin öyrənmə üsulları ilə sındıra bilmişdir. Bunların istifadəsi ilə təhlükəsizlik kodu (captcha) krekinqinə və inkişaf edən texnologiyaya paralel olaraq inkişaf edən və hədəflənən təhlükəsizlik kodu (captcha) modelinə doğru bir təhlükəsizlik kodu (captcha) təkamülü baş verdiyi görülür. İnkişaf etməkdə olan texnologiya sistem təhlükəsizliyini daha təsirli etməyə çalışarkən, qarşı tərəf adlanan zərərli bu inkişaf edən texnologiyadan istifadə edərək daha təsirli bot proqramları hazırlayırlar.

Təhlükəsiz və pozulmuş uyğunlaşmadan sonra daha mürəkkəb və təhlükəsiz tətbiqin inkişafı qaçınılmaz olsa da, təhlükəsizlik kodunun (captcha) belə inkişafı DeCaptcha-in təkamülünə səbəb olur. Daha yüksək, səs-küylü və çətin səs bu, təhlükəsizlik kodundan (captcha) yan keçə bilən və daha yüksək səsli mühitlərdə belə istifadəçinin səsini müəyyən edə bilən proqram təminatı deməkdir.

Sürətlə inkişaf edən kiber dünyada inkişaf edən kompleks təhlükəsizlik kodu (captcha) yaradılarkən, buna uyğun olaraq inkişaf etdirilən bot proqramı daha ağıllı olmağa başladı. Hazırlanmış kompleks təhlükəsizlik kodu (captcha) və istifadəçi dostu, interfeyslər (javascript, html, flash.. kimi ehtiyaclar) nəzərdə tutulmuşdur. Bu araşdırma təhlükəsizlik kodu (captcha) testlərinin çətinliyi və istifadəçinin testdən keçməkdə çətinlik çəkməsi səbəbindən istəksizliyin artması kimi problemlər nəzərə alınaraq hazırlanmışdır.

Bunun nəticəsində istifadəçinin sistemdə qalma müddətini uzatmayan və ona virtual oğru kimi baxan əsas təhlükəsizlik kodu (captcha) səviyyəsindən başlayaraq istifadəçinin istifadəçi olub-olmamasından asılı olmayaraq Təhlükəsizlik kodu (captcha) müxtəlifliyindən istifadə edilir. İnsan və ya bot. Nəticəyə əsasən, getdikcə çətinləşən təhlükəsizlik kodu (captcha) növbəti səviyyəyə keçir və sistemin təhlükəsizliyi daha da çətinləşdirilən testlə təmin edilir. Beləliklə, sistem və istifadəçi dostu təhlükəsizlik kodu (captcha) testi yaradılır. Bu araşdırmanın əsas məqsədi bot hücumlarında təhlükəsizlik kodunun (captcha) müxtəlifliyini artırmaqla bot proqram təminatının alqoritm strukturuna meydan oxumaq və bununla da daha təhlükəsiz təhlükəsizlik kodu (captcha) testini təmin etməkdir.

Nəticə. Texnologiyanın sürətli inkişafı ilə paralel olaraq virtual aləmdə kiber müharibə proporsional olaraq artır. Bu çərçivədə texnologiyanın müsbət və mənfi tərəflərinin eyni vaxtda inkişafı, istifadəçilərin virtual aləmdə daha rahat və təhlükəsiz hərəkət etməsi üçün müxtəlif təhlükəsizlik tədbirləri görüldü. Bu təhlükəsizlik tədbirlərindən əsas olanı Təhlükəsizlik kodu (captcha) sistemləridir.

Təhlükəsizlik kodu (captcha) tətbiqlərinin qeyri-kafi olduğu hallarda təkamülü nəticəsində öhdəsindən gəlmək daha çətin ola biləcək sadə üsullardan biridir. Xüsusi süni intellekt nümunələri ilə cüzi tələblər ortaya çıxır və bu çətinlikdə süni intellektin öyrənilməsi ilə strukturları həll etmək

bacarığı hadisəni Təhlükəsizlik kodu (captcha) yoxlama səhnəsindən fərqli bir ölçüyə aparır. Aydındır ki, təhlükəsizlik kodu (captcha) bu cür süni neyron şəbəkələri ilə inkişaf edənlər üçün gündəngünə inkişaf edən və çətinləşən yaxşı bir sınaq vasitəsidir. Onun inkişafı ərzində fərqli xüsusiyyətlər qazansa belə təklif olunan yanaşma ilə təhlükəsizlik kodu (captcha) əsas növlərinə əsaslanır

Çətinlik səviyyəsinə görə əməliyyatlar istifadəçini sıxışdırmadan və sistemi məcbur etmədən addımlarla həyata keçirilir. Ən əhəmiyyətli rəy baş verə biləcək bot hücumlarında istifadə edilən təhlükəsizlik kodu (captcha) çeşididir və zərərli proqramın alqoritmik strukturunu məcbur edərək sistemi qoruyur. 2017-ci ildə Microsoft Təhlükəsizlik koduna (captcha) edilən hücumda istifadə edilən alqoritmin bir növ Təhlükəsizlik kodu (captcha) strukturunun öhdəsindən gəlmək üçün nəzərdə tutulduğunu və sındırıldığını nəzərə alsaq, məcbur etmək mümkündür. Təhlükəsizlik kodunun müxtəlifliyi (captcha) ilə bot proqram təminatının alqoritmi onun sistem təhlükəsizliyi baxımından əhəmiyyəti daha yaxşı başa düşüləcək.

Ədəbiyyat

1. L. von Ahn, M. Blum, N. Hopper, and J. Langford. *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, page 294--311. Springer-Verlag, (2003)
2. https://static.hlt.bme.hu/semantics/external/pages/%C3%A1ltal%C3%A1nos_mesters%C3%A9ges_intelligencia/en.wikipedia.org/wiki/CAPTCHA.html
3. Bursztein, Elie; Aigrain, Johnathan; Mosciki, Angelika; Michell, John C. (August 2014). The End is Nigh: Generic Solving of Text-based CAPTCHAs. WoOT 2014: Usenix Workshop on Offensive Security.
4. <https://www.2captcha.com>.

Məqalə qəbul olunub: 20.10.23
Təvsiyə edib: prof. Həsənov V.H.