UOT 004.89

Qasımova R.T.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
rena.gasimova@science.az

İNTERNETDƏ QLOBAL DOMEN İNFRASTRUKTURUNUN TƏHLÜKƏSİZLİYİ

Müasir şəraitdə domen adları sistemində ((Domain Name System, DNS) sorğuların ələ keçirilməsi, saxtalaşdırılmanın və digər təhlükələrin aradan qaldırılmasında DNS təhlükəsizliyinin təkmilləşdirilməsi (DNS Security Extensions, DNSSEC) texnologiyasından istifadə edilir. Məqalədə bu texnologiyanın təhlükəsizlik aspektləri tədqiq olunur, domen infrastrukturuna tətbiqinin zəruruliyi əsaslandırılır və DNS-serverə olunan hücumların analizi aparılır. Eyni zamanda DNSSEC texnologiyasının həyata keçirilməsi problemləri, üstünlükləri və təhlükəsizliklə bağlı imkanları müəyyən olunur. Bu texnologiyanın tətbiqi ilə bağlı statistika və proqnozlar analiz edilir və onun reallaşdırılması istiqamətində bir sıra tövsiyələr verilir.

Açar sözlər: *domen adları sistemi, DNS-server, informasiya təhlükəsizliyi, elektron imza, qeydiyyatçı, yüksək səviyyəli domenlər, Crypto Officer.*

Giriş

Bu gün hər bir dövlətin başlıca vəzifələrindən biri onun öz informasiya məkanına nəzarət etmək uğrunda mübarizəsidir. Burada söhbət həm də iqtisadi, siyasi, mədəni, milli-mənəvi, hərbi və digər sahələrdə dəyərlərimizin müdafiəsindən gedir. Məlumdur ki, cəmiyyətin müasir tələblərə uyğun inkişafı, dövlət idarəçiliyinin təkmilləşdirilməsi və şəffaflığının təmin edilməsi, milli informasiya resurslarının yaradılması, milli maraqların, milli dəyərlərin virtual məkanda mühafizəsi, biliklərə əsaslanan iqtisadiyyatın inkişafı, bütün sahələrdə yeni texnologiyaların geniş tətbiqinə nail olunması, informasiya təhlükəsizliyi və azadlığının müdafiəsi, qlobal informasiya fəzasına inteqrasiyanın genişləndirilməsi ölkədə informasiya cəmiyyətinə (İC) keçidi təmin edəcək fəaliyyətin tərkib hissələridir.

İnternetdən istifadə etməklə insan fəaliyyətinin bütün sahələri: elm, təhsil, siyasət, biznes, istehsal, xidmət və s. inkişaf üçün yeni imkanlar əldə edir. İnternet ictimai baxışın formalaşmasında, siyasi, iqtisadi və hərbi sahədə qərarların qəbulunda, düşmənin informasiya resurslarına təsirində və həmçinin, xüsusi hazırlanmış dezinformasiyaların yayılmasında geniş imkanlara malikdir. İnternet şəbəkəsindən informasiya müharibəsi aparmaq üçün aktiv istifadə edilməsi, onun ənənəvi üsul (kütləvi informasiya vasitələri) və texnologiyalardan daha üstün olması ilə izah olunur. Bununla yanaşı, araşdırmalar göstərir ki, hazırda informasiya resurslarından və texnologiyalarından cinayət və terror məqsədləri ilə istifadə etməyin qarşısının alınması, intellektual mülkiyyətin, insan hüquqlarının, eyni zamanda domen adlarında əmtəə və xidmət nişanına olan hüquqların qorunması, milli təhlükəsizliyin təminatı, fərdi məlumatların toxunulmazlığı İnternet məkanında qarşıya çıxan əsas problemlərdəndir [1].

Son bir neçə ildə İnternet kommunikasiya və kommersiya işini qlobal şəkildə həyata keçirən məkana çevrilməkdədir. Yəqin elə bu səbəbdəndir ki, dünya əhalisinin üç milyarddan çoxu İnternet istifadəçisidir. İnternetdə ünvanların idarə edilməsi DNS vasitəsi ilə həyata keçirilir. Bu gün DNS milyardlarla sorğunu gündəlik emal edən ən böyük paylanmış verilənlər bazasıdır. İnternetdə DNS-in işini təmin etmək üçün 13 kök server fəaliyyət göstərir və onlar Təyin Olunmuş Adlar və Nömrələr üzrə İnternet Korporasiyasının (Internet Corporation for Assgned Names and Numbers, ICANN) texniki mərkəzinə məxsusdurlar. Onlardan 10-u ABŞ-da, 1-i Yaponiyada, 1-i Hollandiya, 1-i İsveçdə yerləşir. 2012-ci ildə Azərbaycanda "L-root DNS" güzgü kök serveri işə salınıb [2–5].

Tədqiqatlar göstərir ki, hazırda aparılan elm-tədqiqat işlərinin əksəriyyəti DNS-də təhlükəsizlik probleminin aşkarlanmasına yönəlmişdir. Bu işlərdə DNS-serverlərin yüklənməsinin qarşısının alınması yolları göstərilmiş, DNS-ə olan hücumların metodları təhlil

edilmiş, müasir müdafiə texnologiyaları araşdırılmış və konsepsiyalar işlənmişdir. Elmi-texniki ədəbiyyatın analizi göstərir ki, hazırda sayt haqqında DNS-in saxtalaşdırılmış cavabları ilə mübarizə aparmağa imkan verən təsirli tədbirlər görülməmişdir. Lakin saxtalaşdırmanın qarşısını almaq üçün metodlardan biri kimi DNSSEC texnoloji təşəbbüsü hesab edilir [6–10]. DNSSEC DNS protokolunun DNS-ünvanın dəyişməsi ilə bağlı hücumları minimallaşdırmağa imkan verən genişlənməsidir.

Öz növbəsində digər tədqiqat işlərində DNS verilənlərini fasiləsiz qorumaq üçün müasir təhlükəsizlik sisteminin standart yanaşması olan kriptoqrafik mexanizmlərdən (elektron imza) istifadə məsələsinin aktuallığı göstərilmiş və ən

çox istifadə olunan hücum metodlarının statistikası verilmişdir. Lakin, istismar baxımından DNSSEC-in həyata keçirilməsində bəzi həll edilməmiş problemlər də mövcuddur. Aparılan təhlillər onu göstərir ki, DNSSEC-in istifadəsi, idarəçiliyi və qeydiyyatı prosesində problemlər tam həllini tapmamışdır [11–13]. Mövcud problemlər onların həll zərurətini aktual məsələ kimi ortaya qoyur.

DNSSEC texnologiyasının meydana gəlməsi

DNSSEC təhlükəsizlik sertifikatları zəruri müdafiəni təmin etmək üçün İnternet layihələndirilmələrin xüsusi qrupu (İnternet Engineering Task Force, IETF) tərəfindən təklif edilmişdir. O, DNS-kliyentlərə DNS-sorğulara autentik cavablar verilməsinə və onların bütövlüyünün təminatına istiqamətlənmişdir. Bu zaman açıq açarlı kriptoqrafiyadan istifadə olunur. Verilənlərin əlçatanlığı və sorğuların konfidensiallığı təmin olunmur. DNS-in təhlükəsizliyinin təmin olunması bütövlükdə İnternetin təhlükəsizliyi üçün mühüm əhəmiyyət kəsb edir [14].

Araşdırmalar göstərir ki, DNS sisteminin problemlərindən biri, onun əlçatanlığı və tamlığına təsir edən hər cür hücum üçün həssas olmasıdır. Bədəməllər asan şəkildə istifadəçilərin sorğularını simvol adı ilə düzgün olmayan serverlərə göndərir, beləliklə parollara, kredit kartlarının nömrələrinə və digər konfidensial informasiyaya çıxış əldə edirlər. Brauzerin sətrindəki yazı və sayt istifadəçinin gözlədiyi kimi olduğundan, əksər hallarda sorğunun başqa istiqamətə istiqamətləndiyini bilmirlər. Son nəticədə fişinq saytlarına, onlara məxsus olmayan İnternet-bankinqə rast gələ bilirlər. DNSSEC texnologiyası kliyentlərin saxta DNS verilənlərindən müdafiə olunması üçün işlənmişdir. DNSSEC-dən olan cavablar rəqəm imzaya malikdirlər. Rəqəm imzasının yoxlanması zamanı DNS-kliyent informasiyanın doğruluğunu və bütövlüyünü yoxlayır. DNSSEC cari DNS sistemi və proqramların ilk versiyalarına uyğun olub, verilənləri şifrələmir və onların idarəsini dəyişmir. DNSSEC DNS-də saxlanan ümumi təyinatlı kriptoqrafik informasiyanı təsdiq edə bilir. DNSSEC verilənlərin konfidensiallığını təmin etmir, yəni bütün DNSSEC cavablar autentifikasiya olunur, amma şifrələnmirlər. Digər standartlar DNS serverləri arasında göndərilən böyük həcmli verilənlərin təmini üçün istifadə edilir. DNSSEC spesifikasiyaları cari DNSSEC protokolunu ətraflı təsvir edir [15].

Aparılan tədqiqatlar göstərir ki, DNS yaranan zaman sistem serverin cavabında informasiyanın dəyişməsinə qarşı müdafiə mexanizmlərinə malik deyildi. Belə ki, 1980-ci illərdə İnternetin təhlükəsizliyi aktual deyildi. Yəni, DNS protokolu təhlükəsizlik məqsədi ilə deyil, miqyaslanan paylanmış sistemlərin yaradılması üçün işlənmişdi. Bu halda kliyentlər alınan informasiyanın doğruluğunu ikibaytlı identifikatora görə təyin edirdilər. Beləliklə, bədəməldən "keşi pozmaq" üçün 65536 qiyməti araşdırmaq tələb olunurdu. Bu o demək idi ki, DNS sistemində verilənlər bilərəkdən və ya səhvən zədələnmişdir, DNS-server isə onları cəldliyi optimallaşdırmaq üçün keşləşdirir (keş "pozulmuş"olur) və bu qeyri-autentik verilənləri kliyentlərə göndərir. 1990-cı ildə Steven Bellovin təhlükəsizlikdə ciddi çatışmazlıqlar aşkarladı və 1995-ci ildə bu problemlə bağlı məruzə nəşr etdirdi. Qeyd etmək lazımdır ki, bu sahədə tədqiqatlar 1995-ci ildə, məruzə nəşr edildiyi vaxtdan tam sürətlə başlamış və bu günə qədər də aparılır [16, 17].

DNSSEC-in birinci redaksiyası RFC 2065 (Request for Comments) IETF-də 1997-ci ildə nəşr olunmuşdu. Bu spesifikasiyanın reallaşdırma cəhdləri 1999-cu ildə yeni RFC 2535

spesifikasiyasının yaranmasına səbəb oldu. DNSSEC IETF RFC 2535-ə əsaslanaraq reallaşdırmaq planlaşdırıldı. Təəssüf ki, IETF RFC 2535 spesifikasiyasının bütün İnternetə miqyaslanması ilə bağlı ciddi problemi vardı. 2001-ci ilə aydın oldu ki, bu spesifikasiya iri şəbəkələr üçün yararlı deyil. Normal iş halında DNS serverlər tez-tez valideynləri ilə (iyerarxiyadakı yuxarı səviyyədəki domenlərlə) sinxron olmurdu və bu da problem sayılmırdı. Lakin qoşulmuş DNSSEC-də sinxron olmayan verilənlər xidmətdən imtina (Denial of Service, DoS) effekti yarada bilərdi. DNSSEC ənənəvi DNS-ə nisbətən hesablama baxımından daha resurs tutumludur. DNSSEC-in birinci versiyası xələfinin dəyişməsi üçün altı məlumatdan ibarət kommunikasiya və böyük həcmli verilənlər tələb edirdi (xələfin DNS zonaları tamamilə valideynə verilir, valideyn dəyişiklik edib yenidən xələfə qaytarır). Bundan başqa, ümumi açarda dəyişikliklər katastrofik effekt ala bilərdi. Məsələn, əgər COM zonası açarını dəyişsə, onda 25 milyon yazı göndərmək lazım gələrdi (belə ki, bütün xələflərdə yazıları yeniləmək lazım idi). Beləliklə, DNSSEC-in RFC 2535 spesifikasiyası bütün İnternetə miqyaslana bilməzdi.

Bu çətinliklər öz növbəsində DNSSEC-in prinsipial dəyişiklikləri ilə yeni spesifikasiyaların (RFC 4033, RFC 4034, RFC 4035) yaranmasına səbəb oldu. Yeni versiya əvvəlkinin əsas problemini aradan qaldırdı, yeni spesifikasiyada açarın yoxlanması üçün əlavə işlər görmək lazım gəlsə də, o praktiki tətbiq üçün tamamilə yararlı oldu. Beləliklə, 2005-ci ildə bu gün də istifadə olunan DNSSEC-in mövcud versiyası yarandı.

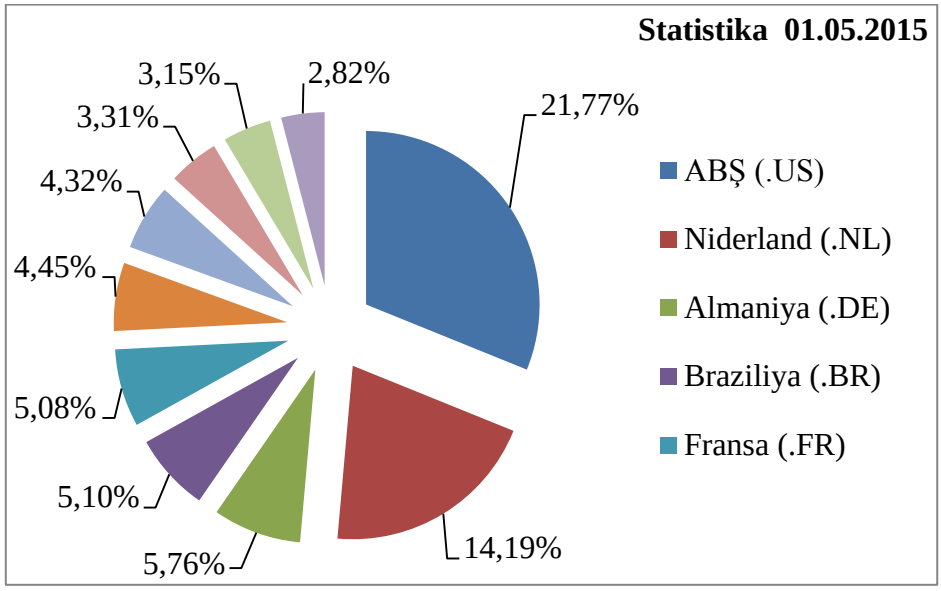
Kök zonasının imzası. DNSSEC-in köməyi ilə verilən bütün verilənlərin tam yoxlanması üçün DNS-in kök zonasından (.) gələn inam zənciri lazımdır. Düzgün imzalanmış kök zonasının DNS-in bütün kök serverlərinə tətbiqi müasir İnternetin dağılmasına səbəb ola bilərdi. Ona görə də IETF ICANN ilə birlikdə imzalanmış kök zonanın və açarların paylanma mexanizminin tədricən tətbiqi prosedurunu işlədi. Prosedur səkkiz aydan çox çəkmişdi və DNS serverlərinə əvvəlcə etibarsız elektron imza ilə imzalanmış kök zonanın addım-addım tətbiqindən ibarət oldu. Bu addım serverlərin yüklənmədə testləşdirməsini təmin etmək, köhnə proqram təminatı ilə əks uyğunluğu saxlamaq və əvvəlki konfiqurasiyaya qayıtmaq imkanını saxlamaq üçün lazım oldu.

2005-ci ildə ilk olaraq DNSSEC protokolunu İsveçin SE zonasında yoxladılar. 2007-ci ildə Braziliya (.BR), Bolqarıstan (.BG) və daha sonra 2008-ci ildə Çex Respublikası (.CZ) bu siyahıya əlavə olundu. 2009-cu ildə təhlükəsiz protokolu dəstəkləyən ORG zonası ümumi istifadəli yüksək səviyyəli domen zonalarından (Top Level Domen, TLD) birincisi oldu. 5 may 2010-cu ildə DNSSEC texnologiyasının bütün domen adları sisteminin 13 kök serverlərində tətbiq edilməsi başa çatdırıldı**.** 2010-cu ilin iyununa bütün kök serverlər etibarsız yoxlanmayan açarla imzalanmış zona ilə dəqiq işləyirdi. İyulda ICANN sonradan kök zonanı imzalayan elektron imza açarlarının generasiyasına həsr olunmuş beynəlxalq konfrans keçirdi. 15 iyul 2010-cu ildə kök zonanın imzalanması baş verdi və imzalanmış zonanın serverlərə tətbiqi başlandı. 28 iyulda ICANN bu prosesin qurtarması haqqında məlumat verdi. Kök zona elektron imza ilə imzalandı və DNS sistemində paylandı. 31 mart 2011-ci ildə İnternetdə ən böyük zona olan COM elektron imza ilə imzalandı. 2011-ci ildə artıq TLD zonalarında protokolu dəstəkləyənlərin sayı 59, növbət ildə isə 90-a qədər artdı və ABŞ hökuməti GOV zonasındakı bütün domenlərin bu protokola keçməsi haqqında qərar qəbul etdi. Hazırda ICANN İnternet korporasiyasının 10 aprel 2015-ci il məlumatına əsasən, mövcud olan 897 yüksək səviyyəli domenlərdən 726 domen zonası DNSSEC texnologiyasını dəstəkləyir [18–21].

Qeyd etmək lazımdır ki, DNSSEC texnologiyasının tətbiqində milli qeydiyyatçılar daha böyük fəallıq nümayiş etdirirlər. Belə ki, məsələn, SIDN şirkətinin 2014-cü il üçün apardığı statistik hesabata əsasən, DNSSEC protokolunun dəstəklənməsinə görə yüksək səviyyəli milli domenlər arasında Niderlandın milli domeni NL liderdir. Niderlandda 5,4 milyon domen adı qeydiyyatdan keçirilmişdir və onlardan 1,7 milyonu DNSSEC protokolunu dəstəkləyir. Şirkətin apardığı statistik məlumata əsasən, DNSSEC protokolunu dəstəkləyən zonaların reytinqində Çex Respublikasının CZ domeni ikinci yerdədir. CZ zonasında 1,2 milyondan çox domen qeydiyyata

alınmışdır ki, onlardan 450 mindən çoxu bu protokulu dəstəkləyir. 2013-cü ilin dekabrında Çexiya hökuməti təhlükəsiz protokolun inkişafının təmin edilməsi mədsədilə qətnamə qəbul etmişdir. Qətnamə 2015-ci ilin iyunun sonuna kimi bütün dövlət hakimiyyəti orqanlarının öz saytları üçün DNSSEC texnologiyasının dəstəyini təmin etməyi öhdəsinə qoyur. CZ administratorunun nümayəndələrinin fikrincə bu təhlükəsiz protokolun inkişafının təminatı üçün hökumət tərəfindən atılmış uğurlu bir addımdır [22, 23].

DNSSEC texnologiyasını dəstəkləyən ilk onluğa Braziliyanın BR (12,6%), İsveçin SE (8,7%), Avropa İttifaqının EU (6,2%), COM (8,4%), NET (1,8%) və ORG (0,9%) domen zonaları daxildır (şəkil 1). 2011-ci ilin payızında Rusiya Federasiyası SU zonasına DNSSEC tətbiq etməklə eksperiment aparmağa və paralel olaraq xarici təcrübəni öyrənməyə başlamağa qərar verdi. DNSSEC-in SU zonasında tətbiqi üç məqsəd daşıyırdı: maraqlı istifadəçilərə protokoldan istifadə imkanı vermək, eksperimentlər üçün əsas qoymaq və yeni texnologiyaya diqqəti cəlb etmək. 2012-ci ilin əvvəlində Rusiyanın РФ, sonunda RU zonası DNSSEC protokolunun tətbiqini imzaladı. Hazırda RU zonasının 300, РФ zonasının isə 40-a yaxın domenində DNSSEC imzalanmışdır [24].



Şəkil 1. DNSSEC texnologiyasını dəstəkləyən domen zonalarının top onluğu

Açarların infrastrukturu. Zona imzasının idarə edilməsi üçün ICANN elə model seçmişdir ki, bu proses İnternet ictimaiyyəti nümayəndələrinin (Trusted community representatives, TCR) nəzarəti altında həyata keçirilir. Qeyd edək ki, bu nümayəndələr DNS-in kök zonasının idarə edilməsi ilə bağlı olmayanlardan seçilir. Seçilmiş nümayəndələr kripto-zabitlər (Crypto Officer, CO) və bərpa açarı hissələrinin sahibləri vəzifələrini tuturlar (Recovery key shareholder, RKSH). CO-ya elektron rəqəm imzası ilə zona imzalanma açarının (Zone Signing Keys, ZSK) generasiyasını fəallaşdırmağa imkan verən fiziki açarlar təqdim edilir. RKSH isə kriptoqrafik avadanlıq daxilində istifadə olunan açar (Key Signing Key, KSK) hissəsindən ibarət smart-karta malik olur. İCANN-ın prosedurlarına uyğun olaraq, CO hər dəfə ZSK-nın generasiyasında (ildə 4 dəfəyə qədər), RKSH isə CO-nun açarları itirməsi zamanı, yaxud kök zonanın riskə məruz qaldığı halında cəlb oluna bilər.

DNSCEC-in tətbiq imkanları və problemləri

Qeyd etmək lazımdır ki, zonanı imzalamaq azdır, qeydiyyatçılar, provayderlər və abonentlər bundan istifadə etməyə başlamalıdırlar. Əsas çətinlik "inam zənciri" texnologiyasını son

müştəriyədək çatdırmaqdır. Yəqin ki, akkreditə olunmuş qeydiyyatçılar bununla fəal məşğul olurlar. Aparılan təhlillər zamanı məlum olmuşdu ki, DNSSEC-in tətbiqi aşağıdakı səbəblərə görə gecikir:

- DNS serverlər və kliyentlər DNSSEC-i dəstəkləməlidirlər;
- yüksək səviyyəli domenlərə (.com, .net) sahibliyə görə əsas oyunçular arasında anlaşılmazlığın olması;
- DNSSEC-lə işləyə bilən yenilənmiş DNS-resolverlər TCP-dən istifadə etməlidirlər;
- hər bir kliyent DNSSEC-dən istifadə etməzdən əvvəl bir inamlı açıq açar almalıdır;
- sorğuların ciddi artan trafikinə görə (6-7 dəfə) şəbəkənin yüklənməsinin artması;
- imzaların generasiyası və yoxlanması tələbindən serverin prosessoruna yüklənmənin artması (bu halda bəzi kifayət qədər güclü olmayan DNS serverlərin əvəz edilməsi tələb oluna bilər);
- imzalanan verilənlər çox yer tutduğuna görə ünvanlaşma haqqında informasiya xəzinəsi üçün tələblərin artması;
- server və kliyent hissələrinin proqram təminatını yaratmaq, testləşdirmək və əlavə etmək lazımdır (buna da İnternetdə vaxt və sınaqlar tələb olunur);
- DNS Amplification (DNS Gücləndirmə – yeni növ DoS-hücum) hücumunun təhlükəsinin kəskin artması və s.

Bu problemlərin böyük hissəsi texniki İnternet ictimaiyyəti tərəfindən həll edilmişdir. DNSSEC-in maksimal effektivliyi bu sistemin İnternet-iyerarxiyanın yüksək səviyyəsindən (kök zona və yüksək səviyyəli domenlər) ayrı-ayrı domen adları səviyyəsinədək yayılmasının birgə tətbiq edilməsi nəticəsində əldə edilir. Bu qlobal layihənin uğurlu tətbiqinə məsuliyyət reyesterlərin, qeydiyyatçıların, qeydiyyat sahiblərinin, aparat və proqram təminatı istehsalçılarının, hostinq şirkətlərinin, dövlət təşkilatlarının, texniki xidmətin və İnternet ictimaiyyətinin üzərinə qoyulur. DNSSEC texnologiyasının tətbiqi kliyentlərə, qeydiyyatçılara və provayderlərə yeni imkanlar verir və qarşılarına müxtəlif məsələlər qoyur. Bu texnologiyanın tətbiqi aşağıdakı imkanları verir:

- brend və kliyentlərin müdafiəsi;
- risklərin azalması;
- kliyentlərin inam və etibarlığının möhkəmlənməsi;
- domen adları sahiblərinin inam və loyallığının möhkəmlənməsi;
- ticarət nişanlı kliyentlər üçün şəbəkədə əlavə müdafiənin təmin edilməsi;
- təhlükəsizliyin təminində maraqlı olan kliyentlərin cəlb edilməsi və saxlanılması;
- İnternetdə inamın təmini vasitəsilə şirkətin əsas fəaliyyətinin müdafiəsi;
- yeni xidmətlərin yaradılması və təklifi (məsələn, domen adları sahibləri üçün zonanın imzalanması kimi);
- İnternetin təhlükəsizliyinin təmininin qabaqcıl metodlarından istifadə edən və kliyentlərinin müdafiəsinin qayğısına qalan şirkətin nüfuzunun yaradılması və s.

DNSSEC-in reallaşması provayderə nəinki kliyentlərini müdafiə etməyə və İnternet istifadəçiləri üçün təhlükəsizliyin təmin edilməsi sahəsində liderlərin nüfuzunun möhkəmlənməsinə imkan verir, həm də uğurlu rəqabət aparmağa şərait yaradır. Beləliklə, DNSSEC texnologiyasının tətbiqi aşağıdakı məsələlərin həlli üçün nəzərdə tutulmuşdur:

- DNS-in müdafiə imkanlarını genişləndirir;
- DNS-ə olan hücumların qarşısını alır;
- DNS-in bütövlüyünü təmin edir;
- kliyentlər və əmtəə nişanları üçün şəbəkələrdə əlavə müdafiəni təmin edir;
- kibercinayətkarların hərəkətindən müdafiəni təmin edir;
- veb-saytların və ya elektron poçt istifadəçilərinin kredit kart verilənlərinin və ya istifadəçi parollarının saxta ünvanlara və veb-saytlara yönəldilməsinin qarşısını alır;
- istifadəçiləri son nəticədə fişinq saytlarından qoruyur;

- təşkilat üçün mühüm olan müdafiə səviyyəsini təmin edir;
- müasir müdafiə texnologiyalarına keçid metodlarından istifadəni reallaşdırır və s.

Nəticə

DNSSEC texnologiyasının sürətli tətbiqini şərtləndirən səbəb onun iqtisadi cəhətdən əlverişli olması, İnternetdə təhlükəsizliyin təminatı, istifadə üçün rahatlığıdır. Bu texnologiyanın imkanlarından istifadə edən kliyentlər, qeydiyyatçılar və provayderlər istifadəçinin biznesini dəstəkləyən və möhkəmləndirən məhsulların, xidmətlərin inkişafına əhəmiyyətli təsir edə bilərlər. Belə ki, şəbəkədə DNSSEC-i tətbiq etməklə istifadəçilərin yüksək səviyyədə təhlükəsizliyi və etibarlılığı təmin edilir, həmçinin müəyyən hücum növləri və yenidən yönləndirmənin qarşısı alınır. Bundan başqa, veb-sertifikatlar üçün (SSL/TLS (https:)) etibarlıq və verilənlərin tamlığının müdafiəsini artıran innovasiya imkanlarından istifadə imkanı verilə bilir.

DNSSEC şəbəkədə informasiya sorğularına cavablarını identifikasiya etməklə və bütövlüyünü yoxlamaqla informasiya təhlükəsiziyi məsələlərini əhəmiyyətli dərəcədə asanlaşdırır. DNSSEC sahəsində aparılan təhlilər göstərir ki, bu texnologiyanın tətbiqində milli qeydiyyatçılar daha böyük fəallıq nümayiş etdirsələr də problemlər hələ də qalmaqdadır. Bu onu göstərir ki, yüksək səviyyəli domen zona qeydiyyatçıları DNSSEC-in tətbiqi istiqamətində bir sıra işlər aparmalıdırlar. Belə ki, təhlükəsiz protokolun inkişafının təminatı üçün aidiyyatı dövlət qurumları tərəfindən addımlar atılmalı və bu proses beynəlxalq normalara və ölkə qanunvericiliyinə cavab verməlidir.

ƏDƏBİYYAT

1. Qasımova R.T. İnternetdə domen problemləri və onların həlli yolları. Bakı: AMEA "İnformasiya texnologiyaları" nəşriyyatı, 2012, 164 s.
2. Əliquliyev R.M., Qasımova R.T. Milli domen adları intellektual analiz sisteminin yaradılması // İnformasiya Texnologiyaları Problemləri, 2011, №1, s.29–36.
3. www.internetworldstats.com/stats.htm
4. Касумова Р.Т. Сравнительный анализ географических доменов верхнего уровня сети Интернет // Информационные технологии, 2011, №7, с. 18–23.
5. Alguliev R.M., Gasimova R.T. Identification of Categorical Registration Data of Domain Names in Data Warehouse Construction Task // Journal Intelligent Control and Automation, USA, 2013, vol.4, no.2, pp.227–234.
6. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsi üzrə tədqiqatların müasir vəziyyətinin analizi // İnformasiya cəmiyyəti problemləri, 2012, № 2, s.19–26.
7. İmamverdiyev Y.N. E-dövlətin informasiya təhlükəsizliyinin idarə edilməsinin konseptual modeli // İnformasiya Cəmiyyəti Problemləri, 2013, № 1, s.53–58.
8. Massey D., Denning D.E. Guest Editors' Introduction: Securing the Domain Name System // IEEE Security and Privacy, 2009, vol.7, no.5, pp.11–13.
9. Guanchen Chen, Matthew F. Johnson, Pavan R. Marupally, Naveen K. Singireddy, Xin Yin, Vamsi Paruchuri. Combating Typo-Squatting for Safer Browsing / WAINA '09 Proceedings of the 2009 International Conference on Advanced Information Networking and Applications Workshops/ Bradford, United Kingdom, 2009, pp.31–36.
10. Pappas V., Massey D., Zhang L. Enhancing DNS Resilience against Denial of Service Attacks / Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, Edinburgh, 2007, pp. 450–459.
11. Ariyapperuma S., Mitchell C.J. Security Vulnerabilities in DNS and DNSSEC / Proceedings of the Second International Conference on Availability, Reliability and Security, Vienna, 2007, pp. 335–342.
12. Chandramouli R., Rose S. Open issues in secure DNS deployment //IEEE Security and Privacy, 2009, vol.7, no.5, pp. 29–35.
13. Osterweil E., Zhang L. Inter-administrative challenges in managing DNSKEYs // IEEE

Security and Privacy, 2009, vol.7, no.5, pp.44–51.
14. Мамаев М.А., Петренко С.К. Технологии защиты информации в Интернете, СПб.: Питер, 2002, 243 с.
15. Радивилова Т.А., Бушманов В.С. Анализ основных атак на DNS-сервер и методы использования DNSSEC при защите DNS-сервера // Технологический аудит и резервы производства, 2013, № 1(10), том 2, с.16–19.
16. Carl Landwehr, Dan Boneh, John Mitchell, Steven M. Bellovin, Susan Landau, Mike Lesk. Privacy and Cybersecurity: The Next 100 Years / Proceedings of the IEEE, PP(99):1–15, May 13th, 2012, vol.100, pp.1659–1673.
17. Steve Bellovin. Using the Domain Name System for System Break-Ins / SSYM'95 Proceedings of the 5th conference on USENIX UNIX Security Symposium, 1995, USENIX Association Berkeley, CA, USA, vol.5, pp.18–28.
18. Metzger P., Simpson W.A., Vixie P. Improving TCP security with robust cookies / Proceedings of the 26th Large Installation System Administration Conference (LISA‘12), 2009, vol.34, № 6, pp.86–97.
19. Ballani H., Francis P. Mitigating DNS DoS Attacks / Proceedings of the 15th Conference on Computer and Communications Security, Virginia, 2008, pp.189–198.
20. Arends R.L., Austein R.U. DNSSecurity Introduction and Requirement // RFC 4033, 2005, 47 p.
21. www.root-d nssec.org/
22. www.dnssec.cz/
23. www.sidn.nl/annualreport/dot
24. http://stats.research.icann.org/dns/tld_report/

УДК 004.89

Касумова Рена Т.
Институт Информационных Технологий НАНА, Баку, Азербайджан
rena.gasimova@science.az

Безопасность глобальной домен-инфраструктуры в Интернете

DNSSEC – это расширение системы DNS, используемое для предоставления DNS-клиентам аутентичных ответов на DNS-запросы и их целостности, путем устранения фальсификаций и обеспечения безопасности систем доменных имен. В этой статье обоснована необходимость применения DNSSEC-технологии, проводится анализ атак на DNS-серверы. В статье исследованы существующее состояние и проблемы в реализации технологии DNSSEC, преимущества и возможности обеспечения безопасности систем DNS. Анализируются статистика и прогнозы при применении этой технологии и дан ряд рекомендаций по ее реализации.

Ключевые слова: *система доменных имен, DNS-сервер, информационная безопасность, электронная подпись, регистратор, домены верхнего уровня, Crypto Officer.*

Rena T.Gasimova
Institute of Information Technology of ANAS, Baku, Azerbaijan
rena.gasimova@science.az

Security of global domain infrostructure in the Internet

DNSSEC technology is used in preventing DNS search result hacks, eliminating falsifications and ensuring security of domain name systems. The article analyses attacks undertaken to DNS server and justifies the necessity of DNSSEC technology application. The article researches the present state and problems in implementation of DNSSEC technology, advantages and scope of solvency in ensuring the security of DNS systems. Recommendations for realization of these technologies are proposed.

Keywords: *domain names system, DNS server, information security, E-signature, registrar, top level domains, Crypto Officer.*