E-dövlətdə CERT-komandaları şəbəkəsinin yaradılması

Rəşad Həmzəyev[1], Yadigar İmamverdiyev[2]

[1]*AR XDMX Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Agentliyi*

[2]*AMEA İnformasiya Texnologiyaları İnstitutu*

[1]rashad@dmx.gov.az, [2]yadigar@lan.ab.az

***Xülasə*— E-dövlətdə informasiya təhlükəsizliyi insidentlərinin tezliyi artır və nəticələrinin miqyası genişlənir. CERT-komandaları informasiya təhlükəsizliyi insidentlərinin effektiv emalı üçün özünü təsdiqləmiş təşkilati formalardan biridir. Bu işdə e-dövlət mühitində CERT-komandalarının evolyusiyası, onların fəaliyyətinin əlaqələndirilməsi, vahid iyerarxik infrastrukturda birləşdirilməsi problemləri analiz edilir, kibertəhlükəsizlik təlimlərinin təşkili təcrübəsinə baxılır.**

Açar sözlər*— *informasiya təhlükəsizliyi; informasiya təhlükəsizliyi insidenti; CERT; EINSTEIN proqramı; kibertəhlükəsizlik təlimləri

I. GİRİŞ

Azərbaycan Respublikası Prezidentinin "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında" 26 sentyabr 2012-ci il tarixli fərmanı hazırkı dövrdə Azərbaycan Respublikasında informasiya təhlükəsizliyi sisteminin yaradılmasını nəzərdə tutur, bu istiqamətdə aparılan elmi-tədqiqat işlərinin yeni səviyyəyə yüksəldilməsini tələb edir [1].

İnformasiya təhlükəsizliyi insidentlərinin xarakterində - hədəflərində, icraçılarında, icraçıların motivasiyasında köklü dəyişikliklər baş verir: genişmiqyaslı, geniş yayılan insidentlər (məsələn, viruslar) öz yerini konkret hədəfə yönəlmiş, güclü alətlərdən (məsələn, botnetlərdən) istifadə edən insidentlərə verir. Son zamanlara qədər insidentləri törədən şəxslər "skript uşaqları" idisə, hazırda insidentlər yaxşı təşkil olunmuş peşəkarlar tərəfindən həyata keçirilir. Keçmişdə dəcəllik, özünütəsdiq, özünütanıtma motivasiyaları üstünlük təşkil edirdisə, indi kiberhücumların həyata keçirilməsində iqtisadi qazanc əldə etmək motivi üstünlük təşkil edir.

Bir sıra ölkələrdə artıq kibertəhlükəsizliklə peşəkar şəkildə məşğul olan hərbi hissələr yaradılmışdır. 2009-cu ildə kibertəhlükəsizlik üzrə bütün əməliyyatların mərkəzləşdirilmiş idarə edilməsi üçün ABŞ (Amerika Birləşmiş Ştatları) Müdafiə Nazirliyi nəzdində kiberkomandanlıq – USCYBERCOM (United States Cyber Command) yaradılmışdı. Kiberkomandanlıq ABŞ dövlət və mülki kompüter sistemlərinin və şəbəkələrinin təhlükəsizliyini təmin edir, eyni zamanda kiberhücumlar da həyata keçirə bilər. Bu komandanlıq tərəfindən 2013-cü ilin əvvəlində kibertəhlükəsizlik əməkdaşlarının sayının 5 dəfə (900-dən 4900-ə) artırılması qərara alınmışdır. Bu işin davamı kimi komandanlıq tərkibində ABŞ-ın kritik infrastrukturlarını dəstəkləyən kompüter sistemlərinin təhlükəsizliyi bölməsinin, Müdafiə Nazirliyi sistemlərinin təhlükəsizliyi bölməsinin və kiberhücmların planlaşdırılması və həyata keçirilməsi bölməsinin yaradılması nəzərdə tutulur.

Rusiya Federasiyası Müdafiə Nazirliyi nəzdində kiberkomandanlığın yaradılmasının birinci mərhələsini 2014-cü ilin sonuna kimi qutarmaq planlaşdırılır. Bu qurumun amerikan USCYBERCOM-un analoqu olacağı gözlənilir. Eyni zamanda amerikan DARPA (Defence Advanced Research Project Agency) fondunun analoqunun – Perspektiv Müdafiə Tədqiqatları Fondunun (Perspective Defence Advanced Research Project Agency, PDARPA) yaradılması da gözlənilir. Rusiya XİN-də (Xarici İşlər Nazirliyi) xüsusi işlər üzrə səfir ranqında İKT-nin siyasi məqsədlərlə istifadəsi məsələləri üzrə xüsusi əlaqələndirici vəzifəsi təsis edilib. ABŞ Dövlət Departamentində bu məsələ ilə bağlı bütöv bir şöbə məşğul olur.

Digər ölkələrdə də oxşar təyinatlı kiberqoşunların yaradılması üzrə intensiv işlər aparılır. Bu, kiberfəzanın hərbiləşdirilməsinə və kibertəhdidlərin ehtimalının artmasına, nəticədə informasiya təhlükəsizliyi insidentlərinin sayının çoxalmasına gətirib çıxarır. Belə insidentlərin vaxtında qarşısının alınması olduqca aktualdır və onlara qarşı mübarizə vasitələrindən biri də Kompüter Qəzalarını Cavablandırma Komandaları (Computer Emergency Response Team, CERT) kimi qrupların təşkilidir. Hazırda müxtəlif ölkələrdə çox sayda CERT komandaları fəaliyyət göstərir [2].

E-dövlət quruculuğu mərhələsində olan Azərbaycan Respublikasında CERT komandaların təşkili və onların işinin təkmilləşdirilməsi istiqamətində dövlət tərəfindən məqsədyönlü tədbirlər həyata keçirilir [3]. Ölkəmizdə yaradılan CERT-lərə elmi-metodoloji dəstək göstərilməsi məqsədi ilə təqdim olunan işdə müvafiq elmi-metodiki ədəbiyyat analiz edilir və qabaqcıl ölkələrdə bu sahədə toplanmış təcrübə ümumiləşdirilir, bir sıra tövsiyələr verilir.

II. İNFORMASİYA TƏHLÜKƏSİZLİYİ İNSİDENTLƏRİ

"İnformasiya təhlükəsizliyi insidenti" anlayışının müxtəlif təriflərinə rast gəlmək mümkündür. Geniş mənada informasiya təhlükəsizliyi insidenti informasiya sistemində baş verən istənilən qanunsuz, icazə verilməyən (o cümlədən, informasiya təhlükəsizliyi siyasəti ilə) və ya qəbuledilməz hərəkətlərə deyilir.

İnformasiya təhlükəsizliyi insidentlərinin idarə edilməsi üzrə ISO/IEC TR 18044 standartında insident anlayışı bir qədər dar mənada işlədilir. Bu standartda informasiya təhlükəsizliyi insidenti anlayışına informasiya təhlükəsizliyi hadisəsi anlayışından çıxış edərək tərif verilir.

İnformasiya təhlükəsizliyi hadisəsi – sistem, xidmət və ya şəbəkənin informasiya təhlükəsizliyi siyasətinin mümkün pozuntularını və ya mühafizə tədbirlərinin sıradan çıxmasını göstərən müəyyən vəziyyətinin məlum təzahürü, yaxud da təhlükəsizliklə bağlı ola biləcək, əvvəllər məlum olmayan vəziyyətinin meydana çıxmasıdır.

İnformasiya təhlükəsizliyi insidenti – arzuolunmaz və ya gözlənilməz informasiya təhlükəsizliyi hadisələrinin baş verməsi nəticəsində meydana gələn bir və ya bir neçə biznes-əməliyyatlarını nüfuzdan salma və informasiya təhlükəsizliyinə təhlükə yaratma ehtimalı böyük olan hadisədir.

İnformasiya təhlükəsizliyi insidentlərinin aşağıdakı kateqoriyalarını və misal olaraq aşağıdakı hadisələri göstərmək olar.

Qəsdən törədilmiş insidentlər: xidmətdən imtina; oğurluq; xakerlik; dələduzluq; resurslardan sui-istifadə; sabotaj/fiziki ziyan vurma; ziyankar kod və s.

Təsadüfi insidentlər: avadanlıqda nasazlıq; proqram təminatında nasazlıq; kommunikasiyada nasazlıq; yanğın; daşqın və s.

Səhvlər: əməliyyatlarda səhvlər; aparat təminatında səhvlər; proqram təminatında səhvlər; istifadəçilərin səhvləri və s.

İnsidentlərin emalına (ing. incident handling) insidentlərin aşkarlanması (hadisələr, insidentlər, həyəcan siqnalları haqqında məlumatların alınması və analizi), sistemləşdirmə (insidentlərə prioritetlərin verilməsi), analiz (nə baş verib, ziyan nə qədərdir, hansı təhdidə səbəb ola bilər, dəf etmək və bərpa üçün hansı addımlar atmaq lazımdır) və insidentlərin cavablandırılması (ing. incident response) daxildir. İnsidentlərin cavablandırılması planlaşdırma, koordinasiya və həyata keçirmə, koordinasiya və informasiya paylaşımı, əks əlaqə və dərs çıxarma funksiyalarını əhatə edir.

İnsidentlərin idarə edilməsi (ing. incident management) təkcə insidentlərin emalı və insidentlərin cavablandırılmasını deyil, onların qarşısının alınmasına yönəlmiş fəaliyyəti də bildirir. Bu fəaliyyətə boşluqların idarə edilməsi, artefaktların idarə edilməsi, istifadəçilərin təlimi və məlumat səviyyəsinin artırılması daxildir.

III. CERT KOMANDALARININ EVOLYUSİYASI

İlk kompüter insidentlərinin emalı komandası 17 noyabr 1988-ci ildə o zamankı İnternetin işini iflic edən Morris soxulcanı insidentindən dərhal sonra Karneqi-Mellon Universiteti Proqram Mühəndisliyi İnstitutunda yaradılmışdı. Sonralar bu komandanın adı CERT/CC-yə (CERT/Coordinating Center, CERT/Əlaqələndirmə mərkəzi) dəyişdirildi. 1989-cu ildə ABŞ-ın bir sıra nazirliklərində də CERT-komandaları yaradıldı. 1990-cı ildə komandalar arasındakı münasibətləri koordinasiya etmək üçün 11 təsisçi üzv (biri Fransadan olmaqla) FIRST (Forum of Incident Response and Security Teams) forumunu yaratdılar (http://www.first.org).

FIRST üzvləri etiraf edirlər ki, hazırda kompüter təhlükəsizliyi sahəsində insidentlər olduqca çoxdur və onların bir təşkilat və ya bir ölkə daxilində idarə edilməsi çətindir, daha effektiv cavablandırma FIRST-in digər üzvləri ilə əməkdaşlığı əsasında həyata keçirilə bilər. FIRST-də ən vacib anlayış informasiya mübadiləsi və bir-biri ilə qarşılıqlı əlaqə üçün iştirakçılar arasında inam münasibətləridir.

CERT komandaları öz potensiallarını insidentlərə sadə cavab verməklə başladılar. Sonralar onların təhlükəsizlik xidmətləri sırasına müxtəlif xəbərdarlıq xidmətləri, təhlükəsizlik üzrə tövsiyələr, treninqlər və təhlükəziklik sistemlərinin idarə edilməsi daxil oldu. Tezliklə «CERT» terminini yetərli hesab etmədilər. Nəticədə 1990-cı illərdə yeni «CSIRT» (Computer Security and Incident Response Team, Kompüter təhlükəsizliyi insidentlərini cavablandırma qrupu) termini qəbul edildi. Hazırda hər iki termin (CERT və CSIRT) sinonim kimi istifadə edilir, lakin CSIRT daha geniş termin hesab edilir.

CERT modeli tezliklə Avropada da qəbul edildi və 1992-ci ildə Danimarkanın SURFnet akademiya provayderi Avropada ilk SURFnet-CSIRT adlı CSIRT yaratdı. Hazırda Avropada 100-dən artıq CSIRT mövcuddur. Trusted Introducer (TI, Etibarlı Vasitəçi) qrupu Avropa CSIRT-lərinin vahid kataloqunu yaradaraq ona xidmət edir. Kataloqla yanaşı, TI akkreditasiya xidməti və 2010-cu ildən CSIRT-lərin sertifikasiyası xidmətini də göstərir.

NATO özünün CERT mərkəzinin yaradılması işlərinə 2000-ci illərdə başlamışdı, Kompüter İnsidentlərini Cavablandırma üzrə NATO Koordinasiya Mərkəzi (NATO Computer Incident Response Capability, NCIRC) adlandırılan bu mərkəz hazırda fəaliyyət göstərir.

Avropa ölkələrində irimiqyaslı və regional şəbəkələrdə təhlükəsizlik sahəsində insidentlərlə mübarizə üçün tədbirlərin birgə işlənməsi məqsədilə 2001-ci ilin noyabrında Avropa dövlət CERT-ləri qrupu (European Government CERTs Group, EGC) yaradılmışdır.

ENISA (European Network and Information Security Agency, Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi) 2005-2010-cu illərdə "CERTs in Europe" adlı beş seminar təşkil etmiş, CSIRT komandalarının yaradılmasını dəstəkləmək üçün bir sıra açıq istifadəli sənədlər işləmişdir.

Asiya-Sakit Okean ölkələrinin CSIRT-komandaları bu regionda təhlükəsizlik məsələləri üzrə məlumatlılığı yüksəltmək və insidentlərə cavab potensialını gücləndirmək üçün 2003-cü ilin fevralında APCERT (Asiya Pacific Computer Emergency Response Team) regional birliyini yaratdılar.

IV. CERT KOMANDALARININ TƏŞKİLATİ MODELLƏRİ

CERT komandaları akademik; dövlət; hərbi; milli; kritik infrastruktur; kommersiya; daxili; kiçik və orta biznes; ticarət kimi sektorlarda tətbiq edilir.

CERT üçün beş əsas təşkilati model mövcuddur. Müxtəlif şərtlər, məsələn, ətraf mühit, maliyyə imkanları və

insan resursları nəzərə alınmaqla təşkilat üçün ən əlverişli CERT modeli seçilməlidir:

1. Təhlükəsizlik xidməti modeli;
2. Daxili paylanmış CERT modeli;
3. Daxili mərkəzləşdirilmiş CERT modeli;
4. Hibrid paylanmış və mərkəzləşdirilmiş CERT modeli;
5. Koordinasiya CERT modeli.

Koordinasiya CERT-i hibrid CERT-də paylanmış xidmətlərin funksiyalarını gücləndirir. Koordinasiya CERT-i modelində hibrid CERT xidmətlərinin əməkdaşları şəbəkəyə qoşulma, coğrafi sərhədlər və s. kimi xarakteristikalar üzrə müstəqil CERT-lərdə qruplaşdırılır. Bu model təşkilatın daxili fəaliyyəti üçün, eləcə də xarici təşkilatlarla sıx əməkdaşlıq və dəstək üçün tətbiq edilə bilər. Koordinasiya CERT modeli milli CERT üçün də uyğun təşkilati modeldir.

Milli səviyyədə işləyən CERT informasiya təhlükəsizliyi üzrə əsas əlaqələndirici şəxs kimi çıxış edir.

Hazırda dünyada yetkinliyin müxtəlif mərhələlərində olan 30-50 milli CERT mövcuddur [4]. Onların çoxu Amerika, Asiya və Avropadadır, bir neçəsi son dövrlər Yaxın Şərqdə yaradılıb. Milli CERT-lərə misal olaraq US-CERT (ABŞ), CCIRC (Kanada), JRCERT/CC (Yaponiya), CNCERT/CC (Çin), KrCERT/CC (Cənubi Koreya) və s. göstərilə bilər.

Milli CERT bir və ya bir neçə ölkəyə təsir edən böyük miqyaslı və/və ya kritik informasiya təhlükəsizliyi insidentlərinin cavablandırılması ilə məşğul olurlar.

Kritik informasiya təhlükəsizliyi insidentləri iqtisadiyyata, kritik infrastruktura, dövlətin fəaliyyətinə və milli təhlükəsizliyə təsir göstərə bilərlər. Təbiətlərinə görə, bu insidentlər çox zaman bir deyil, bir neçə təşkilata təsir edir.

V. US-CERT-İN EINSTEIN SİSTEMİ

US-CERT (United States Computer Emergency Readiness Team) gov domeninin fasiləsiz monitorinqini həyata keçirmək üçün EINSTEIN sistemindən istifadə edir. EINSTEIN sistemi gov domenini kibertəhdidlərdən qoruyur, müdaxilələrin siqnatur əsasında aşkarlanması sistemində (Intrusion Detection System IDS) istifadə etməklə dövlət agentliklərinin və departmentlərinin şəbəkə şlüzlərini icazəsiz trafik baxımından analiz edir [5].

EINSTEIN sistemi üç mərhələdə qurulur.

EINSTEIN 1 – 2004-cü ildən quraşdırılmağa başlamışdır və 2008-ci ilə kimi könüllü idi. EINSTEIN 1-in tərkibində potensial təhdidləri aşkarlayan vasitələr və şəbəkə axınların idarə edilməsi alətləri daxildir.

EINSTEIN 1 quraşdırılmağa başladıqda federal hökumət agentliklərinin İnternetə qoşulma nöqtələrinin sayı 4000-dən çox idi. Etibarlı İnternet-qoşulma (Trusted Internet Connection, TIC) təşəbbüsü çərçivəsində belə nöqtələrin sayını kəskin azaltmaq - bu sayı 50-yə salmaq planlaşdırılırdı. Təşəbbüs bütün federal agentlikləri əhatə edirdi, onların hər biri 2008-ci ilin iyununa kimi qoşulma nöqtələrinin sayının azaldılması planını təqdim etməli idi.

EINSTEIN 2 – müdaxilələrin aşkarlanması sistemidir, quraşdırılması 2011-ci ildə başa çatıb. 19 etibarlı İnternet servis provayderlərində (Tursted Internet Contection Access Provader TICAP) və 4 MTIPS-də (Managed Trusted IPS)-də qurulub. EINSTEIN 2-də aqreqasiya, avtomatlaşdırılmış korrelyasiya və vizuallaşdırma vasitələri istifadə edilir.

EINSTEIN 3 – bədniyyətli kiberaktivliyi avtomatik tapmaq və aradan qaldırmaq, departament və agentliklərlə avtomatlaşdırılmış informasiya paylaşımı imkanı olacaq.

EINSTEIN proqramı federal agentliklərdəki təhlükəsizlik süzgəclərini və İDS-ləri əvəzləmək üçün nəzərdə tutulmayıb. Onun funksiyası fasiləsiz monitorinqi təmin etməkdir. Eyni zamanda agentliklərə federal şəbəkənin digər hissələrində baş verən hadisələrdən, xüsusilə onların sistemlərinə təsir edən hadisələrdən xəbər tutmağa imkan verir. İştirakçı təşkilatların təhlükəsiz veb-portala çıxışları olur, burada onlar öz şəbəkə şlüzlərindəki trafik haqqında məlumatla tanış ola bilərlər.

Trafik məlumatlarını korrelyasiya etməklə və onu bir neçə sistem arasında paylaşmaqla EINSTEIN proqramı US-CERT analitiklərinə və federal agentliklərin informasiya təhlükəsizliyi mütəxəssislərinə federal şəbəkələrdə ziyankar aktivlik barədə geniş təsəvvür yaratmağa imkan verir.

EINSTEIN sistemi kompüter təhlükəsizliyi insidentləri üzrə kritik məlumatları toplamaq və paylaşmaq üçün federal hökumətin sərf etdiyi vaxtı əhəmiyyətli dərəcədə (5-7 gündən 4-5 saata) qısaltmışdır. Bundan başqa, EINSTEIN-in məlumat toplamaq və paylaşmaq üçün sərf olunan vaxtı 2 saatdan az etməyə potensialı var, bu hökumətin kiberinsidentlərə cavabını əsaslı təkmilləşdirməyə imkan verir. Əgər planda nəzərdə tutulduğu kimi düzgün həyata keçirilsə, bu proqram kibertəhdidləri analiz etmək və qarşısını almaq imkanlarını gücləndirəcək. Lakin EINSTEIN imkanları hələlik federal mühitdən kənarda reallaşdırılmayıb [6].

EINSTEIN dövlət agentliklərinin və departamentlərinin şəbəkə şlüzlərinin trafikini analiz etmək üçün Deep Packet Inspection (DPI) texnologiyasından istifadə edir. DPI statistik verilənlərin toplanması, məzmuna görə şəbəkə paketlərinin yoxlanması və süzülməsi texnologiyasıdır. Şəbəkələrarası ekranlardan fərqli olaraq, DPI təkcə paketlərin başlığını yox, OSI modelində 2-ci və daha yuxarı səviyyələrdə trafikin tam məzmununu analiz edir. DPI virusları aşkarlaya və bloklaya, verilən meyarlara uyğun olmayan informasiyanı süzə bilər. DPI təkcə paketlərin məzmununa görə deyil, müəyyən şəbəkə proqramlarına və protokollarına xas dolayı əlamətlərə görə də qərar qəbul edə bilər. Bunun üçün statistik analiz yanaşması (məsələn, müəyyən simvolların rastgəlmə tezliyinin, paketlərin uzunluğunun statistik analizi) istifadə edilə bilər.

Qeyd edək ki, ITU-T təşkilatı DPI texnologiyasının tətbiqi üzrə Y.2770 standartını (tövsiyələri) qəbul etmişdir (2012-ci il, dekabr). Bəzi ölkələr bu standartın İnternet-provayderlərə məcburi tətbiq edilməsini təklif edirlər.

EINSTEIN proqramının xidmət etdiyi şəbəkədə istifadəçilərin konfidensiallığı məsələsi hələlik, açıq qalır. Lakin məsul şəxslər bildirirlər ki, bu məsələ ətraflı şəkildə öyrənilir: "konfidensialıq və vətəndaşların hüquqları bu təşəbbüsün əsas prioritetləridir" [7].

VI. İNSİDENTLƏRƏ HAZIRLIQ ÜZRƏ KİBERTƏLİMLƏR

İnformasiya təhlükəsizliyi insidentlərinin baş verməsi faktına ölkənin hazırlıq səviyyəsinin test edilməsi ən vacib tədbirlərdən biridir, mümkün insidentlərin emalında uğur bu

mərhələdən çox asılıdır. Hazırda bir sıra ölkələrdə irimiqyaslı kibertəhlükəsizlik təlimləri keçirilir.

Cyber Storm 2006-cı ildən başlayaraq ABŞ-da iki ildə bir dəfə geniş miqyasda və real vaxtda keçirilən kibertəlimlərdir. Bu kibertəlim iştirakçılara özlərinin kiberhücumlara hazırlıq, müdafiə və cavablandırma imkanlarını qiymətləndirməyə şərait yaradır.

Cyber Storm I 2006-cı ilin 6-10 fevralında milli kibermüdafiə sisteminin rəqəmsal casusluğa qarşı test edilməsi məqsədilə keçirilmişdi. Təlimlərdə rabitə, nəqliyyat və enerji istehsalı kimi kritik infrastrukturlara genişmiqyaslı hücumlar imitasiya edilmişdi. Təlimlər ABŞ təhlükəsizlik təşkilatlarını əhatə edirdi, eyni zamanda təlimlərdə Böyük Britaniya, Kanada, Avstraliya və Yeni Zelandiya mütəxəssisləri də iştirak edirdilər.

Cyber Storm II 2008-ci ildə keçirilmişdi. Bu təlimlərdə ABŞ-ın 18 federal agentliyi, 9 ştat və 40-dan çox özəl şirkət iştirak edirdi. Təlimlərə 5 ölkənin mütəxəsisləri də qoşulmuşdu. Təlimin məqsədlərindən biri kiberhücumlar zamanı kommersiya və dövlət strukturlarının qarşılıqlı əlaqə metodlarının sınaqdan çıxarılması idi. Təlim iştirakçıları fövqəladə hallarda: İnternetə çıxış tam bağlandıqda, dövlət, kommersiya və enerji strukturlarının əsas qovşaqlarına yönəlmiş lokal xaker hücumları zamanı sürətli məlumat mübadiləsini «məşq edirdilər». Bundan əlavə, rabitə şəbəkəsinin tam sıradan çıxması hallarında da hərəkətlər planı işlənib hazırlanmışdı.

Dördgünlük Cyber Storm III təlimlərində (2010-cu il) 8 federal nazirlik, 13 ştat, 60 özəl şirkət və 12 xarici ölkədən minlərlə mütəxəssis iştirak etmişdir. Xarici tərəfdaşlar Avstraliya, Böyük Britaniya, Kanada, Fransa, Yaponiya, Almaniya və digər dövlətlər idi.

Təlimlərin əsas məqsədi kiberfəzada insidentlərin cavablandırılması üzrə milli planın real şəraitə maksimum uyğunlaşdırılmış şərtlərdə yoxlanması və təlimin nəticələrinə görə onun təkmilləşdirilməsi idi. Təlimlər əvvəlkilərdən daha mürəkkəb ssenarilər üzrə aparılırdı. Cyber Storm III çərçivəsində düşmənin İnternet infrastrukturunun iki mühüm komponentinə – DNS-serverlərə və rəqəmsal sertifikatların həqiqiliyinə nəzarət edən serverlərə hücum ssenariləri sınaqdan çıxarılırdı.

Təlimlərin digər məqsədi irimiqyaslı xaker hücumlarından mərkəzləşdirilmiş müdafiə sistemi olan Milli kibertəhlükəsizlik və kommunikasiyaların inteqrasiyası mərkəzinin (National Cybersecurity and Communications Integration Center, NCCIC) iş qabiliyyətini yoxlamaq idi. Təlimlər bu mərkəzdə qərarların nə dərəcədə tez və operativ qəbul edildiyini aydınlaşdırmalı idi.

Oxşar təlimlər Avropada 2010-cu ildə keçirilməyə başladı (Cyber Europe 2010). Bu təlimlərin gedişində Avropa Birliyi (AB) ölkələrində yerləşmiş e-idarəetmə infrastrukturunun kritik vacib elementlərinə qlobal DDoS-hücum imitasiya edilmişdi. Təlimlərin məqsədi AB dövlətlərində rəqəmsal infrastrukturun kritik obyektləri arasında rabitənin sıradan çıxmasına hazırlıq səviyyəsinin yoxlanması idi. Cəmi 320 hücum imitasiya edilmişdi.

NATO-nun nümunəvi birgə kibermüdafiə mərkəzində (NATO Cooperative Cyber Defence Centre of Excellence – CCDCOE, mərkəz Tallində yerləşir) informasiya texnologiyaları sahəsində illik kibertəlimlər 2008-ci ildən keçirilir. 2013-cü ildə «Bağlı qalxanlar 2013» (Locked Shields 2013) adlı kibertəlimlər kiberhücumlara qarşı müdafiənin effektivliyi yoxlanırdı və təlimdə Avropanın 9 ölkəsindən 250 mütəxəssis iştirak edirdi.

2011-ci ildə AB və ABŞ arasında Cyber Atlantic 2011 adlı ilk kibertəhlükəsizlik təlimi keçirilib. Təlimlərdə AB-nin 20 ölkəsindən və ABŞ-dan yüzə yaxın mütəxəssis iştirak edirdi. İki ssenari istifadə edilirdi: 1) AB-üzv ölkələrindən məxfi informasiyanın əldə edilməsinə və nəşr edilməsinə yönəlmiş APT-hücum (Advanced Persistent Threat); 2) Avropa enerji təchizatı obyektlərində istifadə edilən sənaye SCADA-sistemlərinin kütləvi sıradan çıxması. Təlimlər çərçivəsində AB və ABŞ arasında qarşılıqlı əlaqə metodları da məşq edilirdi.

NƏTİCƏ

Bu işdə e-dövlətdə CERT-komandaların qurulması və onların fəaliyyətinin əlaqələndirilməsi məsələləri analiz edilir. E-dövlətin informasiya infrastrukturu mürəkkəbləşir və informasiya təhlükəsizliyi insidentlərinin xarakterində keyfiyyət dəyişiklikləri baş verir. Qarşılıqlı asılılığı və qarşılıqlı əlaqəliliyi artan informasiya sistemlərinin birində baş verən insidentin kaskad effekti ilə digər sistemlərə yayılması ehtimalı yüksəlir. Belə insidentlərin qarşısının alınması, vaxtında aşkarlanması və qısa müddətdə nəticələrin aradan qaldırılması məqsədi ilə e-dövlətdə CERT-komandalarının vahid iyerarxik idarəetmə infrastrukturunda birləşdirilməsi, informasiya fəzasının fasiləsiz monitorinqinin həyata keçirilməsi, insidentlərin emalı fəaliyyətinin effektiv koordinasiya edilməsi, insidentlərə hazırlıq səviyyəsinin kibertəhlükəsizlik təlimləri yolu ilə yoxlanılması zəruridir.

ƏDƏBİYYAT

[1] İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında Azərbaycan Respublikası Prezidentinin Fərmanı, 26 sentyabr 2012-ci il.

[2] R.M. Əliquliyev, Y.N. İmamverdiyev, "İnformasiya təhlükəsizliyi insidentləri," Bakı: İnformasiya Texnologiyaları, 2012, 219 səh.

[3] Y.N. İmamverdiyev, R.F.Həmzəyev, "AzScienceNet elm kompyuter şəbəkəsi üçün CERT-komandasının nın yaradılması (rus)," İnformasiya cəmiyyəti problemləri, 2011, № 1, səh. 15-26.

[4] Y.N. İmamverdiyev, "Milli CERT yaradılmasına mərhələli yanaşma modeli," Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları. Respublika elmi konfransının materialları. – Sumqayıt, 26-27 noyabr, 2007, səh. 252-254.

[5] L.M. Surhone, M.T. Tennoe, S.F. Henssonow, "Einstein (US-CERT program)", 2010, 176 p.

[6] S.M. Bellovin, S.O. Bradner, W. Diffie, S. Landau, and J. Rexford, "Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure," *Harvard National Security Journal*, Vol. 3, 2011, pp.1-38.

[7] U.S. Department of Homeland Security: "Privacy Impact Assessment for EINSTEIN 2," May , 2008, 23 p.