Qlobal Kibertəhlükəsizlik Sənayesinin Analizi

Yadigar İmamverdiyev[1], Günay Muradova[2]
[1,2]AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1] *yadigar@lan.ab.az*, [2]*gmuradova9@gmail.com*

***Xülasə*— Məqalədə qlobal kibertəhlükəsizlik sənayesinin formalaşması və inkişafı problemləri araşdırılır. Kibertəhlükəsizliyin müasir mənzərəsinə qısa nəzər salınır, kibertəhlükəsizlik sənayesinin seqmentləri müxtəlif meyarlara görə təsnif olunur, yaxın illər üçün bu seqmentlərin inkişaf proqnozları və əsas trendləri müəyyən edilir, sənayenin əsas oyunçuları arasında bazarın paylaşılması analiz edilir. Kibertəhlükəsizlik sənayesinin əsas trendləri kimi məhsullarda süni intellekt inqilabının baş verməsi, mürəkkəb, smart silahların yaradılmasında sistemli, layihə yanaşmalarının istifadə edilməsi göstərilir.**

Açar sözlər*— *kibertəhlükəsizlik, kibertəhlükəsizlik sənayesi, kiber-silah, kibercinayətkarlıq, kibermüharibə

I. GİRİŞ

Müasir cəmiyyətdə informasiya texnologiyaları böyük üstünlüklərlə yanaşı, böyük problemlər də yaradır. İnternetdən istifadənin sürətlə artdığı bu dövrdə kibertəhlükəsizlik ən böyük problemlərdən biridir [8]. Dünya əhalisinin 70 %-indən çoxu İnternet istifadəçisidir. Bu həm də, dünya əhalisinin 70 %-nin kibertəhlükəsizlik problemləri ilə üzləşə biləcəyi deməkdir. Bütün xəbərdarlıqlara, rəsmi və qeyri-rəsmi çalışmalara baxmayaraq, kibertəhlükəsizlik problemləri hələ də davam edir və getdikcə daha da kəskinləşir.

Kiber-təhdidlər dünya iqtisadiyyatı üçün də daimi təhlükə təşkil edir və vurulmuş ziyanın həcmi bir neçə trilyona çatır. Hazırda 4-cü sənaye inqilabı baş verir, bu inqilab – istehsal proseslərində kiber-fiziki sistemlərin, süni intellektin, qlobal kommunikasiyaların geniş tətbiqi ilə xarakterizə olunur. Texnologiyaların sürətli inkişafı ilə kiber-təhdidlər də durmadan artır və genişlənir, onların qarşısını almaq üçün bütün ölkələr əhəmiyyətli xərclər çəkirlər.

Beynəlxalq İqtisadi Forum 2014-cü ildən başlayaraq kibertəhlükəsizliyi qlobal risklərin sırasına daxil edir. 2017-ci ildə keçirilmiş Forum yaxın on ildə qlobal inkişafı müəyyən edəcək ən yüksək beş trend arasında cəmiyyət həyatının bütün sahələrində kiber-asılılığın artması tendensiyasını da göstərmişdir. Forumun hesabatında kiberhücumlar və fərdi məlumatların oğurlanması/verilənlərlə dələduzluq riskləri ən ehtimallı 10 risk arasında yüksək yerləri tutur [1].

Nəticədə qlobal kibertəhlükəsizlik sənayesi formalaşır və hazırda yüksək templə inkişaf edir. Bu sahənin özünəməxsus innovasiyaları, hərəkətverici qüvvələri, oyunçuları, inkişaf problemləri vardır. Təqdim olunan məqalənin məqsədi qlobal kiber-təhlükəsizlik sənayesinin formalaşması və inkişafını problemlərini analiz etməkdir.

II. KİBERTƏHLÜKƏSİZLİYİN MÜASİR MƏNZƏRƏSİ

Kiber-hücumların arxasında duran əsas motivasiyalar kibercinayətkarlıq, haktivizm, kibermüharibə və kiber-casusluqdur. Bu hücumların əsas hədəfləri isə IT-sənaye, dövlət orqanları, fərdlər, onlayn-servislər, maliyyə institutlarıdır. IT-sənayedə proqram təminatı, veb-hostinq, əyləncə və avtomobil sektorları əsas hədəflərdir [2].

Kibercinayətkarlıq hazırda qlobal problemdir, əhəmiyyətli dərəcədə inkişaf etmişdir və artıq təkcə insanları və sənayeni təhdid etmir, birbaşa milli təhlükəsizliyə qarşı yönəlmişdir. Kibercinayətkarlıq olduqca gəlirli sahədir. Kibercinayətkarlığın dünya miqyasında əldə etdiyi gəliri dəqiq söyləmək çətindir, bir sıra mütəxəssislər güman edirlər ki, gəlirlərinə görə kibercinayətkarlıq narkotik ticarətindən sonra ikinci yeri tutur.

Haktivizm (hacker və activism sözlərindən yaranmışdır) – elektron mühitdə vətəndaş itaətsizliyinin formasıdır, siyasi ideyaların yayılması, sosial etirazlar üçün kompüterlərdən və kompüter şəbəkələrindən istifadə edilməsidir [3]. Yəqin ki, ən məşhur haktivist qruplar Anonymous, WikiLeaks, LulzSec-dir [4].

Kibermüharibə – siyasi məqsədlərə nail olmaq üçün ölkələr tərəfindən kiberhücumların istifadəsidir, kiberfəzada hərbi əməliyyatlardır. Bura həm hərbiçilərin dövlətin silahlı qüvvələrinə qarşı döyüş hücumları (məsələn, düşmənin kritik vacib rabitə kanallarının sıradan çıxarılması), həm də mülki əhaliyə qarşı olan hücumlar daxildir.

Kibercasusluq – hərbi, siyasi və iqtisadi üstünlüklər əldə etmək məqsədilə qiymətli konfidensial informasiyanın oğurlanmasıdır. Korporativ sistemlərə icazəsiz girişlər bir çox halda kibercasusluq məqsədləri daşıyır. Kibercasusluğun obyekti kimi çox zaman kommersiya sirri təşkil edən məlumatlar, intellektual mülkiyyət – istehsalat sirləri (“nou-hau”lar), marketinq planları, təqdiqatlar, məhsul nümunələri və hətta proqram təminatının ilkin kodları çıxış edir.

Kiberhücumların həyata keçirilməsi üçün müxtəlif kibersilahlardan istifadə edilir – DDoS (Distributed Denial of Service), SQL inyeksiya, ənənəvi zərərli proqramlar, smart-silahlar (məsələn, Stuxnet).

Son illər təşkilatların informasiya infrastrukturuna kiber-hücumların təşkilində mühüm dəyişikliklər baş vermişdir. Bu paradiqma dəyişikliyi məqsədyönlü və davamlı hücumlar (Advanced Persistent Threat, APT) adı ilə xarakterizə olunur. APT-nin kiber-hücumların ənənəvi növlərindən fərqi yaxşı təşkil olunmuş layihə yanaşması, planlaşdırma, yaxşı

DOI: 10.25045/NCSoftEng.2017.22

maliyyələşdirmə və davamlı yerinə yetirilməsidir. Bu növ hücumlar icraçıların qarşısında qoyulmuş məsələlərdən asılı olaraq, aylarla və hətta illərlə davam edə bilər. Bir çox hallarda hədəf olaraq şəbəkəni dağıtmaq və ya ona sarsıdıcı zərbə endirmək məsələsi qoyulmur, informasiyanın uzun müddət əldə edilməsi və analizi, sonra isə məqsədyönlü istifadəsi nəzərdə tutulur [5].

III. KİBERTƏHLÜKƏSİZLİK SƏNAYESİNİN SEQMENTLƏRİ

Həm kiberhücumları həyata keçirmək, həm də onlardan müdafiə olunmaq üçün müvafiq alətlərdən, sistemlərdən, yanaşma və metodlardan istifadə edilməlidir. Müasir kibertəhlükəsizlik sənayesi belə alətlərin geniş spektrini təqdim edir.

Kibertəhlükəsizlik sənayesini müxtəlif meyarlara görə seqmentlərə bölmək mümkündür. Geniş yayılmış yanaşma aparat təminatı, proqram təminatı və xidmətlərə görə təsnifatdır [6]. Daha detallı analizdə *həllərə* (antivirus, identifikasiya, avtorizasiya, müdaxilələrin aşkarlanması, kiber-hücumlardan müdafiə, şəbəkə ekranları, veb filtrasiya və s.), *təhlükəsizliyin sahələrinə* (tətbiqi proqramlar, bulud, kontent, şəbəkə, naqilsiz şəbəkə, sənaye idarəetmə sistemləri), *tətbiq sahələrinə* (dövlət, müdafiə, sənaye, telekommunikasiya, bank-maliyyə, topdansatış, səhiyyə, aero-kosmos, kəşfiyyat), *xidmətlərə* (təhsil, təlim, məsləhət, risk menecmenti, autsorsinq, inteqrasiya), *təşkilat ölçülərinə* (böyük, orta və kiçik müəssisələr), *regionlara* və *ölkələrə* görə seqmentlərə bölmək, təhlil etmək olar.

[7]-də kibertəhlükəsizlik sənayesi üçün qarışıq meyarlar əsasında müəyyən edilmiş seqmentləri cədvəl 1-də verilmişdir.

Təhlükəsizlik analitikası Big Data texnologiyalarının tətbiqi ilə formalaşır və sürətlə yeni startaplar meydana çıxır.

Mobil telefonların və digər mobil qurğuların, mobil tətbiqlərin artması ilə kibertəhlükəsizliyin bu seqmenti də öz yerini möhkəmlədir.

Buludların tətbiq edilməsinin qarşısını alan əsas məsələ onlara inam və onların təhlükəsizliyidir. Buna görə bulud texnologiyaları sahəsində təhlükəsizlik həlləri inkişaf etməkdədir.

Əşyaların İnternetinin inkişafı özü ilə kibercinayətkarlığın yeni dalğasını gətirir. Buna görə Əşyaların İnternetində təhlükəsizlik seqmentinin inkişafı üçün də böyük tələbat vardır.

Avtomobillərin kibertəhlükəsizliyi sahəsində böyük bazar seqmenti hazırda formalaşmaqdadır. Hazırda istehsalçıların diqqəti maşınların, sürücülərin və sərnişinlərin fiziki təhlükəsizliyindən kiberhücumlardan müdafiə məsələlərinə keçir. ABI analitika şirkətinin hesabatına görə 2020-ci ilə kimi 20 milyon avtomobildə proqram təhlükəsizlik sistemləri olacaq, aparat təhlükəsizlik modullarının satışı isə 2020-ci ildə 2,3 milyard qurğuya çatacaq.

Kibertəhlükəsizlik sənayesinin daha bir seqmenti təhsil treninqləridir, əməkdaşların kibertəhlükəsizlik sahəsində məlumatlılıq səviyyəsinin artırılmasına yönəlir.

CƏDVƏL I. KİBERTƏHLÜKƏSİZLİK BAZARININ PROQNOZU

	Bazarın seqmentləri	**İllik artım, %**
1	SİEM (Security İnformation and Event Management)	10
2	Təhlükəsizlik analitikası	10
3	Mobil təhlükəsizlik	18
4	Buludların təhlükəsizliyi	50
5	İdarə edilən təhlükəsizlik servisləri	15.8
6	İdarəetmə, risk və tələblərə uyğunluq	14.6
7	Əşyaların İnternetinin təhlükəsizliyi	55
8	Avtomobillərin təhlükəsizliyi	
9	Kibertəhlükəsizlik sahəsində sığorta	
10	Təhsil treninqləri	13

IV. KİBERTƏHLÜKƏSİZLİK SƏNAYESİNİN ƏSAS OYUNÇULARI

Kibertəhlükəsizlik sənayesinin əsas oyunçuları Intel, IBM, Cisco Systems, Check Point Software Technologies, Fortinet, CA Technologies, McAfee və Symantec-dir. (Ən böyük oyunçular Symantec, Intel və IBM şirkətləridir). Kibertəhlükəsizlik sahəsində 10-dan çox vendora malik ölkələrin siyahısı cədvəl 2-də göstərilir. Cədvəldən göründüyü kimi, dünya üzrə bu sahədə şirkətlərin yarıdan çoxu ABŞ-da yerləşir.

CƏDVƏL II. BƏZİ ÖLKƏLƏRDƏ KİBERTƏHLÜKƏ-SİZLİK VENDORLARININ SAYI

Ölkə	**Vendorların sayı**	**Ölkə**	**Vendorların sayı**
ABŞ	827	Almaniya	33
İsrail	228	Fransa	25
Birləşmiş Krallıq	76	Avstraliya	15
Kanada	49	İsveç	12
Hindistan	41	İrlandiya	10

İsrail kibertəhlükəsizlik məhsullarının və xidmətlərinin ixracı həcminə görə ABŞ-dan sonra 2-ci yerdədir. "2015-ci ildə İsrail şirkətləri 6 milyard dollarlıq kibertəhlükəsizlik məhsulları və xidmətləri ixrac etmişlər, bu dünya bazarının 10%-nu təşkil edir - bu rekord hətta İsrail sənayesinin vizit kartı olan adi silah ixracını da üstələyir. Xüsusi qeyd etmək lazımdır ki, 2014-cü ildə ixrac 3 milyard olmuşdu və növbəti ildə 2 dəfə artıb.

2012-ci ildə 3 illik müddətə KIDMA 1.0 proqramı işə salınmışdı (bu qısaltma ivrit dilində "kibertəhlükəsizlik sahəsində tədqiqatların inkişafı" mənasını verir). 2016-cı ilin əvvəlində proqramın ikinci mərhələsi KIDMA 2.0 işə salınıb. Bu proqramla İsrail kibertəhlükəsizlik sənayesi yeni mərhələyə keçir: uzunmüddətli layihələr, şirkətlərin müştərilərlə əlaqələri, İsrail və xarici şirkətlərlə əlaqələrin qurulması və büdcənin effektiv paylaşılması".

Əhalinin sayına görə dünyada ikinci ölkə olan Hindistanda kibertəhlükəsizlik sənayesi böyük deyil. Lakin sənayenin inkişaf sürəti böyükdür – cəmisi bir ildə, 2014-2015-ci illərdə Hindistan kibertəhlükəsizlik sənayesi 500 milyondan 1 milyard dollara artmışdı.

DOI: 10.25045/NCSoftEng.2017.22

V. KİBERTƏHLÜKƏSİZLİK SƏNAYESİNİN İNKİŞAFI

Forbes-in qiymətləndirmələrinə görə, qlobal kibertəhlükəsizlik bazarı 2015-ci ildəki 75 milyard dollardan 2020-ci ildə 170 milyard dollara artacaq. Bazarın illik artımı 2015-2020-ci illərdə 9.8% təşkil edəcək [7].

Ən böyük artım SIEM sektorunda – 10 %; təhlükəsizlik analitikasında – 10 %+; mobil təhlükəsizlikdə – 18%; buludların təhlükəsizliyində – 50% olması proqnozlaşdırılır. İdarə edilən təhlükəsizlik servisləri seqmentində illik artım 15,8 % olacaq və 2020-ci ildə təxminən 30 milyard dollara çatacaq. İdarəetmə, risk və tələblərə uyğunluq sahəsinin 2014-cü ildə 5,8 milyarddan 2019-cu ildə 11,5 milyard dollara yüksəlməsi gözlənilir (illik artım 14,6 %). Əşyaların İnternetinin təhlükəsizlik bazarı isə 2014-2019-cu illərdə illik 55 % artımla inkişaf edəcək.

Kibertəhlükəsizlik sahəsində sığorta ümumi sığorta bazarının ən sürətlə artan istiqamətlərindən biridir, əsasən ABŞ-da yayılıb. PwC hesabatı 2020-ci ildə qlobal kibertəhlükəsizlik sığorta bazarında illik satışların 7,5 milyard dollara çatacağını proqnozlaşdırır, bu 2015-ci səviyyədən üç dəfə çox olacaq.

Qlobal kibertəhlükəsizlik bazarının əsas alıcıları dövlətlər və böyük şirkətlərdir. Məsələn, ABŞ hökuməti son 10 ildə kibertəhlükəsizliyə 100 milyard dollardan çox xərcləmişdir. 2016-cı ildə xərclər 16 milyard dollar olmuşdur, 2017-ci il büdcəsində kibertəhlükəsizlik üçün ayrılan investisiya 19 milyard dollardır.

2004-cü ildə qlobal kibertəhlükəsizlik sənayesi xərcləri 3.5 milyard dollar idi və 2017-ci ildə isə bu rəqəm 120 milyard dollardır. Deməli, kibertəhlükəsizlik xərcləri son 13 ildə 35 dəfə artmışdır. Cybersecurity Ventures hesabatında qlobal kibertəhlükəsizlik xərclərinin 2017-ci ildən 2021-ci ilə qədər 1 trilyon dollardan daha artıq olacağı proqnozlaşdırılır.

Kibertəhlükəsizlik xərclərinin hərəkətverici faktorları qanunvericilik tələblərinə uyğunluğun təmin edilməsi, biznesin fasiləsizliyi, təşkilatın nüfuzu, korporativ siyasətə uyğunluq, dəyişiklik və biznesin transformasiyasıdır.

TechSci Research tərəfindən hazırlanan hesabata görə Şimali Amerika və Avropa kibertəhlükəsizlik məsələləri üçün ən çox investisiya yatıranlardır.

Kibertəhlükəsizlik sənayesinin trendlərindən biri məhsullarda süni intellekt inqilabının baş verməsidir. Kibertəhlükəsizlik sahəsinə Machine Learning və Big Data texnologiyalarının tətbiqi yeni nəsil kiber-təhlükəsizlik alətlərinin meydana çıxmasına və nəticədə analitika texnologiyalarına çəkilən xərclərin artmasına səbəb olacaq [8].

Digər trendlərdən biri mürəkkəb, smart silahların yaradılmasında sistemli, layihə yanaşmalarının istifadə edilməsidir. Stuxnet virusunun və onun ardıcıllarının (Flame, Gauss, Duqu) analizi göstərir ki, bu zərərli proqramları hansısa haker qrupu deyil, dövlət dəstəkli təşkilat(lar) yaradıb. Belə virusların hazırlanmasına on milyonlarla dollar vəsait sərf edildiyi güman edilir. Bundan başqa, bu viruslar o qədər mürəkkəbdirlər ki, onları mütəxəssislərin böyük qrupu bir neçə il (məsələn, Gauss – 5 il) ərzində hazırlaya bilərdi. "Elderwood layihəsi" kibersilahların sənaye üsulu ilə hazırlanmasını və eyni zamanda, kiberfəzada kəşfiyyat və kiberhücumların avtomatlaşdırılmasını təsdiq edir [5].

Kibersilahların istehsal xərcləri əsasən cəlb edilən insan resursları ilə əlaqəlidir. Elmi tədqiqatlara və layihə-konstruktor işlərinə ilkin investisiyalar zəruridir, lakin təkbaşına hakerlərin və kiçik qrupların (məsələn, Anonymous, Lulzsec) uğurları göstərir ki, məhdud resurslarla da çox şeyə nail olmaq olar. Müasir adi silahların yaradılması ilə müqayisədə kibersilahların yaradılması dövlətlər üçün kiçik xərclərdir. Kibersilahlar insan biliyi və nisbətən ucuz kompüter avadanlığı əsasında yaradılır. Proqram mühəndisliyi, eksployt mühəndisliyi və nüfuzetmə testləri sahəsində biliklər (və bacarıqlar) kiberhücumların əsasıdır. Düzgün seçilmiş mütəxəssislərin cəlb edilməsi, onların biliyinin artırılması kibersilah arsenalını saxlamaq və genişləndirmək üçün zəruri sərmayədir.

Lakin kibertəhlükəsizlik sənayesinin problemlərindən biri multi-dissiplinar hazırlığa malik kadrların çatışmazlığıdır. Məsələn, 2016-cı ilin 3-cü kvartalında İsrailin kibertəhlükəsizlik mütəxəssislərinə tələbatı 5000, İrlandiyanın tələbatı təxminən 3000, Birləşmiş Krallıqda isə 2500-ə yaxın idi. Cisco şirkətinin hesabatına görə, ümumilikdə dünyada kiber-təhlükəsizlik sahəsində bir milyon yarım mütəxəssisə tələbat vardır [9].

NƏTİCƏ

Məqalədə kibertəhlükəsizlik sənayesinin formalaşması və inkişafı problemləri təhlil edilir, onların ənənəvi sənaye ilə ümumi və fərqli cəhətləri müəyyən edilir. Qlobal kibertəhlükəsizlik bazarının həcmi və yaxın illər üçün inkişaf proqnozları və əsas trendləri, sənayenin əsas oyunçuları arasında bazar paylaşımı analiz edilir. Gələcək tədqiqatlarda qlobal kibertəhlükəsizlik bazarının rəqabət mühitinin, imkanlarının və məhdudiyyətlərinin, investisiya imkanlarının qiymətləndirilməsi, detallı strategiyaları və son məhsulları daxil olmaqla bəzi şirkətlərin profillərinin işlənməsi, bazara yeni daxil olanlar üçün tövsiyələrin hazırlanması nəzərdə tutulur.

ƏDƏBİYYAT

[1] World Economic Forum. Insight Report. Global Risks 2017, 12th Edition. http://www3.weforum.org/docs/GRR17_Report_web.pdf

[2] ENISA: Cooperation between CERTs and Law Enforcement Agencies in the fight against cybercrime – A first collection. 2012.

[3] S. Baldi, E. Gelbstein, J. Kurbalija, Hacktivism, cyber-terrorism and cyberwar: the activities of the uncivil society in cyberspace." 2003.

[4] G. Potter, "Anonymous: A Political Ontology of Hope," Theory in Action, Vol. 8, No. 1, pp. 2–3.

[5] Y.N. İmamverdiyev, "Kiberqoşunlar: funksiyaları, silahları və kadr potensialı," İnformasiya cəmiyyəti problemləri, 2015, №2, səh. 15-25.

[6] IDC EMEA. The European Network and Information Security Market – Scenario, Trends and Challenges, April 2009. http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=2153.

[7] S. Morgan, "Cybersecurity market reaches $75 billion in 2015; Expected to reach $170 billion by 2020." Forbes, December 2015.

[8] C. M. Sempere, "The European security industry. A research agenda," Defence and Peace Economics, Vol. 22, No. 2, pp. 245-264, 2011.

[9] Cisco: "Mitigating the Cybersecurity Skills Shortage." 6 p., 2015. http://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-talent.pdf

DOI: 10.25045/NCSoftEng.2017.22