UOT 004.056

***Əliquliyev R.M.*[1]*, Abdullayeva F.C.*[2]**
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
[1]director@iit.ab.az, [2]farqana@iit.ab.az

BULUD TEXNOLOGİYALARININ TƏHLÜKƏSİZLİK PROBLEMLƏRİNİN TƏDQİQİ VƏ ANALİZİ

Məqalə bulud texnologiyalarının informasiya təhlükəsizliyi problemlərinin analizi məsələsinə həsr olunmuşdur. Tədqiqatın aparılması prosesində bulud texnologiyalarının yaranma səbəbləri, əsas anlayışları, xarakteristikaları, servis modelləri, tətbiq modelləri öyrənilmişdir. Bulud texnologiyalarının təhlükəsizliyi üçün aktual olan identifikasiyanın idarə edilməsi, veb-proqramlar, virtuallaşma, etimadın idarə edilməsi kimi müxtəlif təhlükəsizlik məsələləri araşdırılmış, bu sahədə əsas problemlər müəyyən olunmuş və onların həlli üçün bir sıra tövsiyələr verilmişdir.

Açar sözlər: *bulud texnologiyaları, virtuallaşma, identifikasiyanın idarə edilməsi, etimadın idarə edilməsi, vahid giriş, identifikasiyanın federativ modeli.*

Giriş

Bulud texnologiyalarının meydana gəlməsi son illər informasiya texnologiyaları sənayesinə böyük təsir göstərmişdir. Belə ki, Google, Amazon, Microsoft kimi nəhəng təşkilatlar öz diqqətlərini çox güclü, etibarlı və mənfəətli bulud platformalarının istehsalına yönəltmişlər, biznes təşkilatları isə bu yeni texnologiyadan mənfəət götürmək məqsədilə öz biznes modellərini yenidən qurmağa cəhd edirlər.

Bulud texnologiyaları geniş sahəni əhatə edən paylanmış resurslara vahid nöqtədən sorğu üzrə giriş imkanı verən yeni növ informasiya texnologiyalarıdır [1, 2]. Bu texnologiyaların xüsusiyyətləri sırasına istifadəçilərin bulud servislərlə sərbəst işləmək bacarığının olması, buluda girişin istənilən məkandan, istənilən vaxt, istənilən qurğu (smartfon, noutbuk, planşet, leptop və s.) vasitəsilə mümkünlüyüdür. Bundan əlavə, resurslar külliyatının istifadəçilərə servislər menyusu şəklində təqdim olunması, istifadəçiyə resursların həçmini sərbəst şəkildə artırıb-azaltmaq imkanının verilməsi bu texnologiyanın geniş tətbiqinə dəlalət edən amillərdəndir.

Lakin bu texnologiyaların təhlükəsizlik səviyyəsinin olduqca zəif olması onun geniş tətbiqinə böyük maneə yaradır. Bu səbəbdən bulud texnologiyalarının təhlükəsizlik problemlərinin müəyyənləşdirilməsi, onlara qarşı mübarizə üsullarının işlənməsi hazırda ən aktual məsələlərdən biridir.

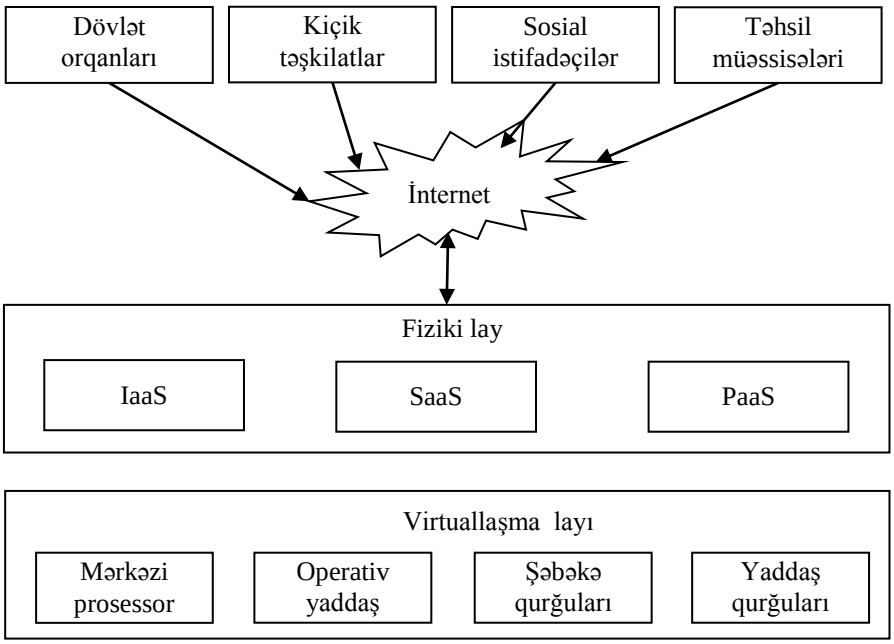
Bulud texnologiyalarının təhlükəsizlik problemlərinin həllinə həsr olunmuş çox sayda yanaşmalar irəli sürülmüşdür [3–11]. Lakin qoyulan əksər təhlükəsizlik məsələləri bulud texnologiyalarının xüsusiyyətlərini, xarakteristikalarını özündə əks etdirmir. Bu səbəbdən bulud infrastrukturunda müxtəlif təhlükəsizlik modelləri arasında interoperabelliyin təmin edilməsi kimi problemlər meydana çıxır.

Təqdim olunan işdə bulud texnologiyalarının *identifikasiyanın idarə edilməsi, veb-proqramlar, virtuallaşma, etimadın idarə edilməsi* kimi müxtəlif təhlükəsizlik problemlərinin analizi aparılır. İdentifikasiyanın federativ idarə edilməsini təmin etmək üçün etimad modelinin bulud texnologiyalarına xas olan elementlər əsasında qurulması tövsiyə olunur.

Bulud texnologiyalarının əsas anlayışları

Bulud texnologiyaları ─ ümumi kompüter resursları toplusunu (məsələn, şəbəkə, serverlər, məlumat anbarları, proqramlar və servislər) sorğu əsasında şəbəkə vasitəsilə əldə etməyə imkan verən modeldir [12]. Resurslar minimal istismar xərcləri sərf etməklə və ya servis provayderlərinə müraciət etməklə əldə edilir.

Tərifdən göründüyü kimi, bulud texnologiyaları müəyyən bir konstruksiyadır. Bu konstruksiya vasitəsilə kompüter resurslarının virtuallaşmış infrastrukturu ümumi İnternet şəbəkəsindən istifadə etməklə istifadəçilərə servis şəklində təqdim olunur [13]. Bu proses sxematik olaraq şəkil 1-də təsvir olunur.



Şəkil 1. Bulud texnologiyasının arxitekturu

Bulud texnologiyalarının arxitekturuna daxil olan dövlət orqanları, kiçik təşkilatlar və s. kimi aktivlər buludun istifadəçiləri hesab olunur.

İstifadəçilər bulud infrastrukturuna daxil olmaq üçün müxtəlif kliyent qurğularından istifadə edirlər [14]. Kliyent qurğularının aşağıdakı növləri var:

Mobil kliyentlər mobil qurğulardır, portativ hesablama qurğularından (Personal Digital Assistant, PDA) və ya Blackberry, Windows Mobile, Smartphone, iPhone tipli smart telefonlarından ibarətdir;

İncə kliyentlər (ing.,Thin Clients) daxili sərt diskləri olmayan kompüterlərdir.

Kobud kliyentlər (ing., Thick Clients) bulud sisteminə qoşulmaq üçün veb-brauzerlərdən istifadə edən adi kompüterlərdir.

Hazırda bulud texnologiyalarına əsaslanan sistemləri ənənəvi kompüter sistemlərindən fərqləndirmək üçün bir sıra aparıcı təşkilatlar tərəfindən bulud texnologiyaları üçün xarakteristikalar müəyyən olunmuşdur. Məsələn, NIST təşkilatı aşağıdakı xarakteristikaları ödəyən sistemi [12] bulud sistemi adlandırır:

Sorğuya görə özünə xidmət (ing., on-demand self-service) istifadəçinin bulud servisləri ilə sərbəst işləmək bacarığını göstərir. Bu xarakteristikaya görə, istifadəçi administratora, şəbəkə mütəxəssisinə müraciət etmədən ona lazım olan resursu, məsələn, yaddaş fəzasını, prosessor resurslarını və s. özü sərbəst əldə edir.

Şəbəkəyə geniş giriş imkanının olması (ing., broad network access). Bu xarakteristikaya görə, buluda girişin təşkili istənilən məkandan, istənilən vaxt, istənilən qurğu vasitəsilə mümkün olmalıdır. Yəni, buludun təqdim etdiyi xidmətləri istənilən qurğudan istifadə etməklə əldə etmək mümkündür. Bu növ qurğular, məsələn, smartfon, stolüstü kompüter, leptop, noutbuk, planşet və gələcəkdə meydana gələn yeni qurğular ola bilər.

Resurslar külliyyatı (ing., resource pooling). Resurslar külliyyatı dedikdə, yaddaş, prosessor, hesablama resursları, şəbəkə resursları toplusu başa düşülür. Burada sadalanan resursların abstrakt toplusu nəzərdə tutulur. Resursların abstrakt toplusunu virtuallaşma vasitələri formalaşdırır, istifadəçi bu toplunun sırasından ona lazım olan miqdarda resursu əldə etmək imkanına malik olur. Daha doğrusu, bu servislər menyusudur. Bu menyunun sırasından istifadəçi, məsələn, 6 Gb həcmli 6 ədəd server, 100 Gb Ethernet, 50 Gb disk fəzası və s. kimi resursların qarşısına işarə qoyaraq onları ani şəkildə əldə edir.

Ani elastiklik (ing., rapid elasticity) resursların miqdarını çevik şəkildə artırıb-azaltmaq imkanının olmasıdır.

Ölçülən servis (ing., measured service) istifadəçiyə göstərilən servisin pul şəklində qiymətləndirilməsidir.

Bulud texnologiyalarında istifadəçilərə müxtəlif servislərin təqdim olunması üç fundamental model (SaaS, PaaS, IaaS) və digər törəmə modellər əsasında həyata keçirilir. Fundamental modellər birlikdə SPI model adlanır, burada SPI – Software, Platform, Infrastructure (as a Service) modellərinin baş hərflərindən formalaşıb və aşağıdakı kimi müəyyən olunur [12, 15]:

Proqram təminatı servis kimi (ing., Software as a Service, SaaS) provayderin bulud infrastrukturunda icra olunan proqram əlavələrinin servis şəklində istifadəçiyə təqdim olunmasıdır. Bu model bulud texnologiyalarından əvvəl də dünya bazarında mövcud olub və hazırda da aktiv şəkildə istifadə olunur. Proqram əlavələrinə misal olaraq Google Docs, Microsoft Office Live, Salesforce Customer Relationship Management göstərmək olar.

Platforma servis kimi (ing., Platform as a Service, PaaS) müxtəlif platformaların istifadəçiyə servis şəklində təqdim olunmasıdır. Platformalara Google App Engine, Microsoft Azure, Salesforce Force.com misal göstərilə bilər.

İnfrastruktur servis kimi (ing., Infrastructure as a Service, IaaS) hesablama infrastrukturunun istifadəçiyə servis şəklində təqdim olunmasıdır. Hesablama infrastrukturuna hesablama resursları, yaddaş, şəbəkə və s. aiddir. İnfrastrukturu istifadəçiyə servis şəklində təqdim etdikdə, bu servisin istifadəçiyə hansı üsullarla təqdim olunması, fiziki resursların harada yerləşməsi, neçə serverin işlək vəziyyətdə olması, bu serverlərdə neçə prosessorun olması istifadəçi üçün heç bir əhəmiyyət kəsb etmir. İstifadəçi, sadəcə, əlyetən olan resurslar toplusunu görür və oradan ona lazım olan miqdarda resursu əldə edir. İnfrastruktura Amazon Simple Storage Service (S3), RackSpace Cloud Servers misal ola bilər.

Adətən, bulud texnologiyalarının istifadəçilərə təqdim etdiyi bütün növ servislər "*Hər şey servis kimi" (ing., Everything as a service, X as a Service, XaaS)* şəklində şərh olunur. Bu qısaltma İnternet şəbəkəsinin təqdim etdiyi servislərin sayının artan olduğunu göstərmək üçün istifadə edilir.

Bulud texnologiyalarının təqdim etdiyi servislərdən istifadə etmək üçün müəyyən bir infrastruktur olmalıdır. Bu infrastrukturu bulud texnologiyalarının tətbiq modelləri adlandırırlar. Bu modellər tətbiq olunan servis modellərinin tipindən (IaaS, SaaS, PaaS) asılı deyil. Hazırda tətbiq modellərinin müxtəlif məsələlər üçün spesifik olan çox sayda törəmələri mövcuddur [15]. Lakin əsas tətbiq modelləri kimi ümumi bulud, xüsusi bulud, qrup buludu və hibrid bulud növündən istifadə olunur.

Ümumi bulud (ing., public cloud). Geniş ictimaiyyətin açıq istifadəsi üçün nəzərdə tutulmuş bulud infrastrukturudur. Bu növ buluda hər bir subyektin giriş əldə etmək hüququ olur. Məsələn, Microsoft, Amazon, Apple, IBM kimi nəhəng təşkilatların malik olduğu bulud

infrastrukturları ümumi bulud sinfinə aiddir, çünki bu təşkilatların hər biri öz resurslar külliyyatını istənilən subyektə təqdim edir.

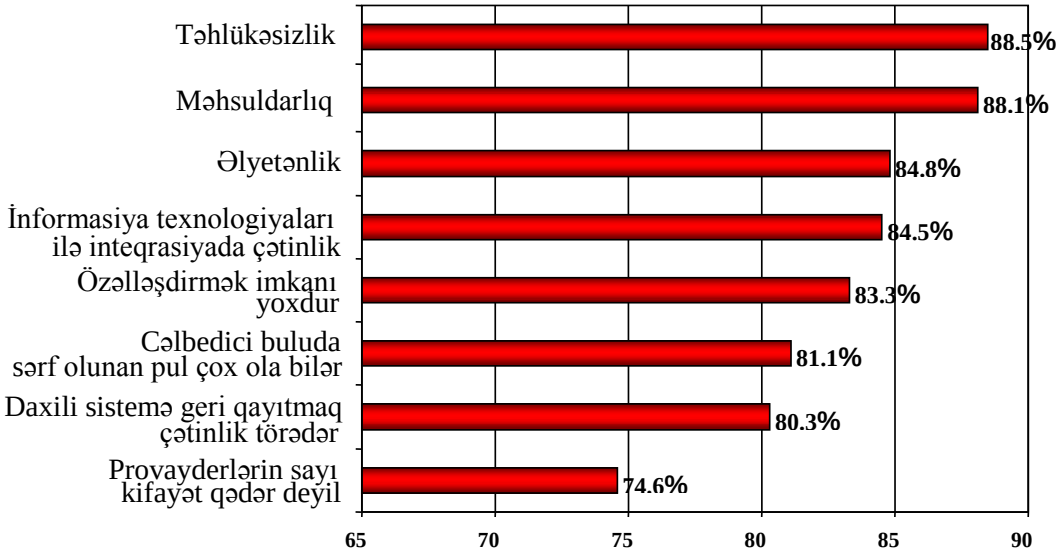
Xüsusi bulud (ing., private cloud) vahid təşkilat daxilində fəaliyyət göstərən bulud infrastrukturudur. Burada bütün resurslar toplusu yalnız bir təşkilata məxsus olur.

Hibrid bulud (ing., hybrid cloud) xüsusi və ümumi buludun kombinasiyasıdır. Yəni, burada xüsusi buludu dəstəkləyən təşkilat öz imkanlarını genişləndirərək resurslarını kənar təşkilatlara da təqdim edir və bununla da hibrid bulud formalaşmış olur.

Qrup buludu (ing., community cloud) maraqları eyni sahəni əhatə edən (məsələn, missiyaları, təhlükəsizlik tələbləri, siyasətləri, ümumi tələbləri) təşkilatlardan olan istifadəçilərin müəyyən qrupunun xüsusi istifadəsi üçün nəzərdə tutulmuş bulud infrastrukturudur. Qrup buludu xüsusi buluda oxşayır, lakin daha iri miqyaslıdır. Xüsusi buluddan fərqli olaraq, burada resurslardan missiyaları eyni olan müxtəlif təşkilatların istifadə etmək hüququ olur. Bu növ bulud dövlət strukturuna tətbiq oluna bilər.

Bulud texnologiyalarının təhlükəsizliyi

Bulud texnologiyalarının geniş tətbiqinə maneələr törədən bir sıra səbəblər vardır. Bu səbəbləri müəyyən etmək üçün International Data Corporation (IDC) təşkilatı tərəfindən bir sıra tədqiqatlar aparılmışdır və doqquz problem müəyyən olunmuşdur [16]. Bu problemlər arasında birinci yerə təhlükəsizlik problemləri qoyulmuşdur (şəkil 2). Digər tərəfdən, Cloud Security Alliance (CSA) təşkilatının da son zamanlar apardığı tədqiqatlardan görünür ki, istifadəçilərin bulud mühitinə keçidinə böyük maneə törədən səbəb informasiya təhlükəsizliyidir [15].



Şəkil 2. Bulud texnologiyalarının tətbiqinə manea törədən səbəblər [16]

Bulud texnologiyalarının aşağıdakı təhlükəsizlik tələbləri vardır [17]:

Effektivlik (ing., effectiveness) – boşluqların və hücumların qarşısının alınması və aşkarlanması prosesinin effektiv şəkildə həyata keçirilməsi.

Dəqiqlik (ing., precision) – sistemin dəqiqlik səviyyəsinin artırılması. Buna nail olmaq üçün hücumların aşkarlanması prosesində pozitiv və neqativ səhvlərin dərəcəsinin minimallaşdırılması məsələsinə baxılır.

Şəffaflıq (ing.,transparency) – servis provayderlərinin, proqram istehsalçılarının, istifadəçilərin və hücum edənlərin bulud sisteminin təhlükəsizlik modeli haqqında məlumatının minimal olmasına nail olmaq.

Qeydiyyatın aparılmasının mümkünlüyü (ing., accountability) – təhlükəsizlik sistemi buludun əsas funksional imkanlarına təsir etməməlidir, uçotun aparılmasını mümkün etmək üçün bulud sistemində baş verən hadisələrin qeydiyyatını aparmalıdır.

Bulud texnologiyalarının meydana gəlməsinin üstünlükləri çoxdur, lakin bu texnologiya informasiya təhlükəsizliyi ilə bağlı ciddi problemlərin də meydana gəlməsinə səbəb olmuşdur. Bulud texnologiyalarının beş əsas təhlükəsizlik problemi var [18]:

- autentifikasiya və identifikasiyanın idarə edilməsi;
- girişin idarə edilməsi;
- təhlükəsizlik siyasətlərinin inteqrasiyasının təşkili;
- servisin idarə edilməsi;
- etimadın idarə edilməsi.

Aşağıdakı bəndlərdə sadalanan problemlərin bəzilərinin ətraflı şərhi verilir.

İdentifikasiyanın idarə edilməsi

İdentifikasiyanın idarə edilməsi (ing., identity management) – istifadəçinin identifikasiya məlumatlarının yaradılmasını, idarə edilməsini, istifadə olunmasını təmin edən infrastrukturdur.

Subyektin unikal xarakteristikaları çoxluğu *identifikasiya məlumatları* adlanır. Subyekti identifikasiya etmək məqsədilə istifadə olunan identifikasiya məlumatları *identifikator* adlanır [19]. Subyektin identifikatorları servis provayderinin (SP) infrastrukturunda autentifikasiya olunmaq üçün istifadə olunur. İdentifikatorlar subyektin kimliyinin təsdiqlənməsinə xidmət edir. Bu isə subyektə servisdən istifadə etmək hüququnun verilməsi haqqında qərar qəbul etməkdə SP-yə böyük dəstək verir. Müəyyən subyektə xas olan rəqəmsal identifikatorların sayı bir neçə ola bilər. Bu rəqəmsal identifikatorların idarə edilməsini təmin edən sistemi identifikatorların idarə edilməsi (İİE) sistemi adlandırırlar. İİE sistemi aşağıdakı funksiyaları yerinə yetirir:

- *Kimliyi müəyyən edir.* Bu fərdi məlumatları identifikasiya məlumatları ilə əlaqələndirməklə təmin edilir.
- *Kimliyi təsvir edir.* Subyekti identifikasiya edən atributlar daxil edir.
- *İdentifikasiya verilənlərinin istifadə hallarını qeydə alır.* Sistemdə baş verən identifikasiya fəaliyyətini loq-jurnallara daxil edir və ya loq-fayllara girişi təmin edir.
- *İdentifikasiya məlumatlarını ləğv edir.* Fərdi məlumatlara son istifadə tarixi daxil edir. Fərdi məlumatlar istifadə tarixi bitdikdən sonra istifadəyə yararsız olur.

İİE sistemi vasitəsilə subyektin müəyyən olunması prosesində bir neçə tərəf iştirak edir:

- *İdentifikator provayderi.* Rəqəmsal identifikatorların hazırlanmasını təmin edir.
- *Servis provayderi.* İdentifikasiya iddiası ilə müraciət edən subyektləri servislərlə təmin edir.
- *Subyekt.* İdentifikasiya məlumatları hazırlanan subyektdir.
- *İdentifikator verifikatoru.* SP-dən sorğu qəbul edərək xüsusi subyektin kimlik məlumatlarını yoxlayır.

İdentifikasiya məlumatlarının idarə edilməsini təmin edən bir sıra infrastruktur modelləri mövcuddur. Bu modellər sırasına Silo, mərkəzləşmiş, federativ və istifadəçi-yönümlü modellər daxildir [20].

Silo modelində provayderin resurslardan istifadə etmək üçün yaratdığı identifikatoru yalnız onun servis domeni çərçivəsində etibarlı olur. Bu səbəbdən istifadəçi hər bir servis provayderinin resursundan istifadə etmək üçün ayrıca identifikator əldə edir.

Mərkəzləşmiş model əsasında istifadəçi vahid identifikatordan istifadə edərək müxtəlif veb-servislərə giriş imkanı əldə edir. Lakin bu model çoxsaylı təhlükəsizlik boşluqlarına malikdir. Məsələn, əgər hücumçu istifadəçinin vahid identifikatorunu təşkil edən autentifikasiya məlumatlarını əldə edərsə, özünü asanlıqla həqiqi istifadəçi qismində qələmə verərək domenin bütün servislərinə giriş imkanı əldə edir.

Federativ model servis provayderlərindən ibarət etimad çevrəsinin yaradılması ideyasına əsaslanır. Burada identifikator provayderinin hasil etdiyi istifadəçi identifikatorunun etimad çevrəsinə daxil olan servis provayderləri arasında paylanması həyata keçirilir.

İstifadəçi-yönümlü model. Bu modeldə hər bir subyektin müəyyən servisə edilən sorğusu onun identifikasiya məlumatlarına bağlanır.

Ümumilikdə bulud-yönümlü identifikasiya sistemləri açıq standartlar üzərində qurulur. Bu isə identifikasiya sistemlərinə müxtəlif təyinatlı sistemlərlə asanlıqla əlaqə qurmaq imkanı verir. Bu növ idarəetmə mexanizmlərindən biri federativ idarəetmədir. Federativ idarəetmə – identifikasiya məlumatlarının müxtəlif təhlükəsizlik domenləri arasında daşınmasına imkan verən texnologiyadır, yəni, vahid identifikatordan bir neçə sistemdə istifadə olunması ideyasına əsaslanır.

Access Manager, *Identity Manager*, *Identity Directory* identifikasiyanın idarə edilməsi sahəsində məşhur proqram vasitələridir [21]. *Access Manager* sistemlərə olan veb-girişlərin federativ idarəetmə mexanizmi (Security Assertion Markup Language) əsasında idarə edilməsinə xidmət edir. *Identity manager* istifadəçi hesablarının, rolların, avtorizasiya qruplarının yaradılmasını təmin edir.

İdentifikasiyanın idarə edilməsini təmin edən standartlar sırasına SAML, WS Federation, OAUTH, OpenID, SPML aid edilir [22]. SAML və WS Federation – İnternet mühitində identifikatorların əlaqələnməsini təmin edən XML-yönümlü sənaye standartlarıdır. OAUTH – veb-proqramlar və mobil qurğular üçün nəzərdə tutulmuş xüsusi avtorizasiya standartıdır. OpenID – identifikatorların federativ və istifadəçi-yönümlü idarə edilməsini təmin edən standartdır. SPML (Service Provisioning Markup Language) – istifadəçilər haqqında identifikasiya məlumatlarının qarşılıqlı əlaqədə olan təşkilatlar arasında mübadiləsini təmin edən açıq standartdır.

İdentifikasiyanın idarə edilməsi üzrə məhsul istehsalçıları sırasında Novell, IBM, CA, Oracle, Microsoft kimi nəhəng təşkilatlar üstünlük qazanmışdır [21]. Bu təşkilatlara məxsus Novell E-Directory, IBM Tivoli, CA SiteMinder, Oracle Identity Manager, Microsoft Federated İdentity Manager məhsulları hazırda identifikasiyanın idarə edilməsi sahəsində geniş tətbiqini tapmışdır.

Müasir dövrdə əksər təşkilatların veb-proqramlarının, servislərinin, tətbiqi proqram interfeyslərinin tətbiq dairəsinin sürətlə artımı müşahidə olunur. Bu isə təşkilatlar arasında identifikasiya məlumatlarının idarə edilməsi məsələsini olduqca çətinləşdirir. Hazırda veb-proqramların, servislərin və tətbiqi proqram interfeyslərinin təhlükəsizliyini təmin etmək üçün identifikasiya məlumatlarının idarə edilməsinə əsaslanan bir sıra açıq kodlu sistemlər yaradılmışdır. Bu sistemlərə Forgerock (Open AM, Open İDM, Open DJ) stekini, WSO2 Identity Server sistemini və Open IAM sistemini göstərmək olar [21].

Bir sıra standartlaşdırma təşkilatları tərəfindən identifikasiyanın idarə edilməsinə xidmət edən standart sənədlər də hazırlanmışdır [23, 24].

Aparılan tədqiqatlar nəticəsində məlum olmuşdur ki, hazırda identifikasiyanın idarə edilməsi sistemlərinin aşağıdakı problemləri vardır: məxfiliyin təmin edilməsi, istifadəçi hesablarına müraciət zamanı istifadəçinin kimliyinin müəyyən olunması prosesində konfliktin meydana gəlməsi, fərdi məlumatların qorunması, identifikasiyanın əminlik səviyyəsinin idarə edilməsi, istifadəçinin kimliyinin təsdiq edilməsi, səlahiyyətin ötürülməsi, identifikasiyanın federativ idarə edilməsi (vahid identifikatordan bir neçə sistemdə istifadə olunması).

Hazırda bu problemlərin həlli istiqamətində əsaslı tədqiqat işləri aparılır. Bəzi yanaşmalarda identifikatorların federativ idarə edilməsi modelinin qurulması üçün IaaS, PaaS, and SaaS laylarının inteqrasiyası məsələsinə baxılır [5].

Digər yanaşmada idarəetmə subyekt-yönümlü modelin qurulması ilə təmin olunur [3]. Bu modelə əsasən, subyekt identifikasiya məlumatlarının yaradılmasını və idarə edilməsini özü həyata keçirir. Bu zaman subyekt autentifikasiya olunduqda. onun identifikasiya məlumatları

servis provayderlərindən gizli saxlanır. Bu isə fərdi məlumatlara edilən avtorizasiyasız giriş cəhdlərinin qarşısını alır.

Bu modelin üstünlüyü odur ki, burada fərdi məlumatların görünən olması provayderin arzusu ilə deyil, fərdi məlumatların sahibinin arzusu ilə mümkün olur. İdentifikasiyanın və girişin idarə edilməsini təmin etmək üçün təhlükəsizlik siyasəti qərarının qəbul edilməsi məsələləri üzərində qurulmuş modellər də vardır [4]. Burada prediktiv modelləşdirmə və simulyasiya metodlarından istifadə olunur. Model əsasən müəssisənin infrastrukturuna aid proqramlar və servislər üçün istifadəçi hesabının yaradılması ideyasına əsaslanır. Digər tərəfdən, növbəti yanaşmada identifikasiyanın idarə edilməsində risklərin qiymətləndirilməsinin vacibliyi göstərilir [21].

Virtuallaşma mexanizmlərinin təhlükəsizliyi

Bulud infrastrukturunda kompüter resurslarının dinamik paylanması, yerləşdirilməsi və həcminin artırıb-azaldılması virtuallaşma vasitələrinin köməyi ilə təmin olunur. *Virtuallaşma* – ayrı-ayrı resursların virtual versiyasının yaradılmasını təmin edən müxtəlif vasitələri, üsulları və yanaşmaları ifadə edən termindir. Virtual maşınlar müəyyən proqram təminatıdır. Bu proqram təminatı müxtəlif əməliyyat sistemlərinin və proqram əlavələrinin fiziki qurğu şəklində işləməsini təmin edir. Adətən, virtual maşına quraşdırılmış əməliyyat sistemini kliyent əməliyyat sistemi (*ing., guest OS*) adlandırırlar.

Virtual maşınların yaradılmasını və idarə edilməsini virtual maşın monitorları (hipervizorlar) həyata keçirir. Bulud texnologiyalarında virtual maşınlar, virtual maşın monitorları, hipervizorlar kimi vasitələrdən geniş istifadə olunur. Lakin istifadə olunan hipervizorlar bir sıra üstünlükləri ilə yanaşı çatışmazlıqlara da malikdir. Hipervizorların çatışmazlıqlarından biri odur ki, əgər hücumçu hipervizor üzərində idarəetməni ələ keçirərsə, o dərhal virtual maşınlara giriş əldə edər.

Hazırda bulud texnologiyalarının virtuallaşma əsasında mühafizəsini təmin edən bir sıra modellər işlənmişdir. IaaS-da virtual infrastrukturun idarə edilməsinə xidmət edən etibarlı virtual verilənlər mərkəzi (*Trusted Private Virtual Data center, TVPDc*) adlı model təklif olunmuşdur [25]. Model IaaS layı üzrə müxtəlif məkanlara və fiziki maşınlara paylanmış hesablama və yaddaş resurslarının mərkəzdən idarə edilməsi ideologiyasına əsaslanır. Təhlükəsizlik təhdidlərinin qarşısını alan və virtuallaşma üzərində bütün idarəetməni öz üzərinə götürən iyerarxik təhlükəsiz virtuallaşma modeli təklif olunmuşdur [26]. Model provayderin İaaS üzərində idarəetmə funksiyalarını yüksəltməklə yanaşı, IaaS, PaaS, dSaaS, and SaaS kimi müxtəlif servis modellərinin də mühafizəsini təmin edir. Model bulud texnologiyalarını DDoS hücumlarından, avtorizasiyasız giriş cəhdlərindən, verilənlərin itkisi hallarından mühafizə etmək xüsusiyyətlərinə malikdir. Virtuallaşmanın təhlükəsiz idarə edilməsi və virtual sistemin təhlükəsizliyi kimi iki mexanizmin kombinasiyasından ibarət model də təklif edilmişdir [27]. Təklif edilən model bulud texnologiyalarında mövcud boşluqlarla mübarizə aparmağa imkan verir, keyfiyyətli idarəetməni və virtual təhlükəsizliyi təmin edir.

Virtuallaşmanın aşağıdakı xarakteristikaları var [28]:

- *Bölünmə*. Vahid fiziki sistemdə müxtəlif proqram əlavələrinin və əməliyyat sistemlərinin icra olunması resursların bölünməsi və paylanması hesabına mümkündür.
- *İzolyasiya*. Hər bir virtual maşın onu dəstəkləyən əsas fiziki sistemdən və digər virtual maşından izolyasiya olunur. Digər tərəfdən, bir virtual maşının zədələnməsi digər virtual maşına heç bir təsir göstərmir.

İzolyasiya vahid hostda icra olunan virtual maşınların bir nüsxəsinin digərinə təsir etməməsini təmin edir. Virtual maşınlar arasında izolyasiyanın pozulmasına xidmət edən hücumlar vardır [6]. Lakin qeyd edək ki, hazırda bu hücumların bulud infrastrukturunda

özünü aparmasını xarakterizə edən tədqiqatlara çox az hallarda rast gəlmək olur. Belə tədqiqatlardan birində [29] virtuallaşma hücumlarının bulud servislərinə müxtəlif təsir formalarının analizi verilir.

Digər bir tədqiqatda bulud texnologiyalarının virtuallaşma layına xas boşluqlarının analizi aparılır [17]. Müdaxilələrin aşkarlanması sistemləri (MAS) vasitəsilə aşkarlanmış hücumlara qarşı müvafiq tədbirlərin görülməsini təmin etməyə xidmət edən təhlükəsizlik arxitekturu verilir.

Virtuallaşmanın təhlükəsizlik problemlərindən biri də buludun proqram əlavələrini özündə əks etdirən virtual maşın təsvirlərini təhlükəsiz idarə etməkdir. Növbəti tədqiqat işində bulud infrastrukturunun təsvirlər bazasında meydana çıxa bilən yeni növ risklərin müəyyən olunması məsələlərinə baxılır [7]. Bu riskləri əsas götürərək təsvirlərin idarə edilməsi üçün bir model verilir, model təsvirlər bazasına girişin idarə edilməsinə əsaslanır.

Veb-proqramların təhlükəsizliyi

Bulud texnologiyaları *veb-proqramlar, veb-servislər, virtuallaşma, kriptoqrafiya* kimi bir sıra mühüm texnologiyalar üzərində qurulmuşdur [30]. Bu səbəbdən bulud infrastrukturu üçün mühüm olan məsələlərdən biri *veb-proqramların* təhlükəsizliyidir.

Veb-proqramların təhlükəsizliyi informasiya təhlükəsizliyinin vacib bir sahəsidir. Əsasən v*eb-saytların*, *veb-proqramların* və *veb-servislərin* təhlükəsizliyini təmin edir.

Veb-sayt – müxtəlif kontent məlumatlarından ibarət, bir-biri ilə əlaqəli veb-səhifələrdən ibarət topludur. *Veb-proqramlar* – şəbəkə vasitəsilə əldə olunması mümkün olan proqramlardır. *Veb-servis* – İnternet mühitində iki elektron qurğunu əlaqələndirən proqram sistemidir [31].

SANS (SysAdmin, Audit, Network, Security) institutunun tədqiqatları göstərir ki, onlayn boşluqların istismarına yönəlmiş ümumi hücumların 60%-dən çoxunu veb-proqramlara edilən hücumlar təşkil edir [32].

OWASP (Open Web Application Security Project) təşkilatının tərtib etdiyi "OWASP Top Ten Project" adlı hesabatda [33] inyeksiya qüsurları və saytlararası skript hücumları veb-proqramlarda mövcud olan əsas boşluq kimi qiymətləndirilir. Baxmayaraq ki, bu iki hücum müxtəlif adlar altında klassifikasiya olunur, onların mahiyyəti, demək olar ki, eynidir.

Veb-proqramlarda və veb-proqramları dəstəkləyən infrastrukturda yol verilmiş zəiflikləri aşkarlamaq üçün IBM, Acunetix, Qualys, Veracode, Siberas və s. kimi aparıcı təşkilatlar tərəfindən veb-proqramların təhlükəsizlik skaneri funksiyalarını yerinə yetirən çox sayda məhsullar və açıq kodlu proqramlar hazırlanmışdır [34].

Veb-proqramların təhlükəsizliyinin təmin edilməsi sahəsində aparılan elmi-tədqiqat işlərinin əksəriyyəti bu mühit üçün aktual olan risklərin, təhdidlərin, boşluqların qiymətləndirilməsi məsələlərinə həsr olunur. Bəzi tədqiqatlarda veb-proqramlarda aktivlərin qiymətləndirilməsi məsələsnin həllini risklərin qiymətləndirilməsi texnologiyası əsasında həyata keçirirlər [8].

Digər tədqiqat işində veb-proqramlar üçün təhlükəsizlik siyasəti modeli verilir [35]. Bu model qeyri-səlis qiymətləndirmə və qraflar nəzəriyyəsi əsasında təhlükəsizlik səviyyəsinin ölçülməsinə əsaslanır. Bundan əlavə, S-vektor (scoring vector) əsasında veb-proqramların təhlükəsizliyinin qiymətləndirilməsi üsulu da işlənmişdir [9]. Veb-proqramların layihələndirmə mərhələsində mövcud risklərin kəmiyyətcə qiymətləndirilməsi məsələsinə baxılmışdır [36]. Qiymətləndirmə prosesi aktivlərin, təhdidlərin və boşluqların əmələ gətirdiyi təhlükəsizlik vektorları əsasında aparılır.

Etimadın idarə edilməsi

Etimadın idarə edilməsi (ing., trust management) – fərdlər arasındakı sosial etimad münasibətlərini simvolik şərh edən abstrakt sistemdir. Adətən, qərarların qəbulu prosesini avtomatlaşdırmağa xidmət edir.

Müxtəlif təyinatlı servis şəbəkələrində səmərəli qərar qəbul etməyə imkan verən çoxsaylı sistemlər yaradılmışdır. Bu sistemlər etimad və reputasiya sistemləri (Trust and Reputation systems) adlanır. Bu nov sistemlərin sırasında eBay, Unitec, FuzzyTrust, REGRET, NICE, Managing the Dynamic Nature of Trust (MDNT), PeerTrust, Managing Trust, Maximum Likelihood Estimation of Peers' Performance (MLE), EigenTrust və Travos kimi sistemlərin adlarını çəkmək olar.

Etimad məsələlərinin həlli bulud texnologiyalarında girişin idarə edilməsi üçün ən əlverişli üsul kimi qiymətləndirilir. Şəbəkə qovşaqları arasında etimad əlaqəsinin qurulmasını, adətən, *Web of Trust* texnologiyası əsasında həyata keçirirlər. Belə ki, bu məqsədlə *Web of Trust* texnologiyası əsasında P2P tipli sistemlərdə girişin idarə edilməsi modeli verilmişdir [10]. Model kliyent qovşaq üçün qlobal etimad qiymətinin hesablanması ideyasına əsaslanır. Nəticədə hesablanmış qlobal etimad qiymətinə uyğun olaraq istifadəçiyə sistemə giriş hüququ verilir və ya imtina olunur.

Bulud texnologiyalarında etimad məsələsinin vacib amili bulud provayderinin istifadəçi verilənlərindən sui-istifadə etmək cəhdlərinin qarşısını almaqdır. Bu problemin həlli üçün verilənlərin anonimləşdirilməsi yanaşması təklif edilmişdir [11].

Bundan əlavə, virtual klasterlərin, təhlükəsiz qurulmuş verilənlər mərkəzlərinin və etibarlı girişlərin reputasiya sistemləri əsasında inteqrasiyası məsələsinə baxılır [37]. Burada qurulmuş reputasiya sistemi buludları və verilənlər mərkəzlərini sayt səviyyəsində mühafizə etməyə imkan verir.

Bulud texnologiyalarında etimad məsələsinin həlli üçün ilk öncə etimad elementləri (buludun təhlükəsizliyi, məxfiliyi, verilənlərin yerləşmə məkanının qeyri-müəyyənliyi, verilənlərin çeşidlənməsi problemləri, provayderin fəaliyyət dövrünün uzunmüddətli olması, normativ aktlara riayət olunması, imtiyazlı girişin təşkili və s.) müəyyən olunmalıdır. Etimad elementlərinin müəyyən olunması istiqamətində çoxsaylı tədqiqatlar aparılmışdır [38, 39].

Nəticə

Bulud texnologiyalarına keçid zamanı istifadəçilərin identifikasiyası və onlara resurslardan istifadə etmək üçün giriş hüquqlarının verilməsi sahəsində ciddi problemlər meydana çıxır. Bu problemlərdən biri bulud istifadəçiləri ilə bulud provayderlərinin mövcud avtorizasiya və giriş modellərinin bulud mühitində inteqrasiyasını təşkil etməkdir. Bu problemin həllinə asanlıqla nail olmaq, yəni bulud sisteminə ayrıca identifikasiya məlumatları saxlancı əlavə etmək həm əlverişli deyil, həm də sistemdə çox sayda təhlükəsizlik boşluqlarının yaranmasına səbəb olur.

Bulud texnologiyalarında identifikasiya məlumatlarının və girişin idarə edilməsi üçün çox sayda yanaşmalar irəli sürülmüşdür. Bu yanaşmalardan biri identifikasiya məlumatlarının federativ idarə edilməsi sistemlərinin qurulmasına əsaslanır. Digər yanaşma bulud sisteminin həm daxili, həm də xarici infrastrukturunda identifikasiya məlumatlarının inteqrasiyasını təşkil etmək üçün etimad məsələsinin həllinə əsasanır. Lakin bu sistemlərdə bulud texnologiyalarının əsas xüsusiyyətləri nəzərə alınmır. Bu səbəbdən, bulud texnologiyalarına xas olan elementlər əsasında etimad modeli qurmaqla identifikasiyanın federativ idarə edilməsini yüksək etibarlılıqla təmin etmək olar.

Ədəbiyyat

1. Abdullayeva F.C. Bulud hesablamaları sistemlərinin informasiya təhlükəsizliyi problemləri / Beynəlxalq İnformasiya Təhlükəsizliyi gününə həsr olunmuş Elmi-Praktiki seminarın materialları, Bakı, 2012, s. 23–24.
2. Abdullayeva F.C. Kloud Kompyutinq mühitində təhlükəsizlik problemlərinin analizi / Riyaziyyatın tətbiqi məsələləri və yeni informasiya texnologiyaları, II Respublika elmi konfransının materialları, 2012, s. 100–102.
3. Angin P., Bhargava B., Ranchal R., Singh N., Linderman M. An Entity-centric Approach for Privacy and Identity Management in Cloud Computing / Proc. of the IEEE 29th International Symposium on Reliable Distributed Systems, 2010, pp. 177–183.
4. Baldwin A., Mont M.C., Shiu S. Using Modelling and Simulation for Policy Decision Support in Identity Management / Proc. of the IEEE International Symposium on Policies for Distributed Systems and Networks, 2009, pp. 17–24.
5. Stihler M., Santin A.O., Arlindo L.M., Fraga J.S. Integral Federated Identity Management for Cloud Computing / Proc. of the IEEE 5th International Conference on New Technologies, Mobility and Security (NTMS), 2012, pp. 1–5.
6. Vaidya V. Virtualization Vulnerabilities and Threats: A Solution White Paper. RedCannon Security, 2009, http://www.redcannon.com/vDefense/VM_security_wp.pdf.
7. Wei J., Zhang X., Ammons G., Bala V., Ning P. Managing security of virtual machine images in a cloud environment / Proc. of the ACM workshop on Cloud computing security, 2009, http://users.cis.fiu.edu/~weijp/Jinpeng_Homepage_files/ccsw09.pdf.
8. Romero M., Bolivar S., Haddad H.M. Asset Assessment in Web Applications / Proc. of the IEEE 7th International Conference on Information Technology: New Generations (ITNG), 2010, pp. 762–767.
9. Barton R.R., Hery W.J., Liu P. An S-vector for Web Application Security Management / Proc. of the 1st ACM Workshop on Business Driven Security Engineering (BIZSEC), 2004, http://www.smeal.psu.edu/cdt/ebrcpubs/res_papers /2004_01.pdf.
10. Chen D., Le J., Wei J. A Peer-to-Peer Access Control Management Based on Web of Trust / İEEE International Conference on Future Computer and Communication (ICFCC), 2009, pp. 192–194.
11. Jensen M., Schage S., Schwenk J. Towards an Anonymous Access Control and Accountability Scheme for Cloud Computing / Proc. of the IEEE 3rd International Conference on Cloud Computing, 2010, pp. 540–541.
12. SP 800-145. The NIST Definition of Cloud Computing. National Institute of Standards and Technology Special Publication, 2011, 7 p.
13. Alhamad M., Dillon T., Chang E. A Trust-Evaluation Metric for Cloud applications // International Journal of Machine Learning and Computing, 2011, V.1, No4, pp. 416–421.
14. Sosinsky B. Cloud Computing Bible. İndiana: Wiley Publishing, 2011, 532 p.
15. Security Guidance for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance, 2011, 176 p.
16. IDC SaaS Summit Spring, The Israeli Association of Grid, 2009, http://www.grid.org.il/_Uploads/dbsAttachedFiles/IDC_Cloud_Computing_IGT_final.ppt.
17. Manavi S., Mohammadalian S., Udzir N.I., Abdullah A. Secure Model for Virtualization Layer in Cloud Infrastructure // IEEE International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2012, No1, pp. 32–40.
18. Takabi H., Joshi D., Ahn G. SecureCloud: Towards a comprehensive security framework for cloud computing environment / Proc. of the IEEE 34th Annual Computer Software and Applications Conference Workshops, 2010, pp. 393–398.
19. Josang A., Pope S. User Centric Identity Management / AusCERT Conference, 2005, pp. 1–13.

20. Lee H., Jeun I., Jung H. Criteria for evaluating the privacy protection level of Identity Management Services / Proc. of the IEEE Third International Conference on Emerging Security Information, Systems and Technologies, 2009, pp. 155–160.
21. Woda A. Identity Management in the Cloud / Proc. of the North America Information Security and Risk Management (ISRM) and IT Governance Risk and Compliance Conference (IT GRC), 2012, http://www.isaca.org/Education/ Conferences/Documents/NAISRM-ITGRC-Presentations/211.pdf.
22. Leslie P.A. Manager's Guide to Identity Management and Federated Identity // Information Systems Control Journal, 2005, V.4, pp. 4–7.
23. SP 800-63-1. Electronic Authentication Guide. National Institute of Standards and Technology (NIST), 2011, 110 p.
24. Liberty Identity Assurance Framework. Liberty Alliance Project, 2008, V.1.1, 128 p.
25. Wan X. TVPDc: A Model for Secure Managing Virtual Infrastructure in IaaS Cloud / Proc. of the IEEE Eighth International Conference on Computational Intelligence and Security (CIS), 2012, pp. 136–141.
26. Manavi S. Hierarchical secure virtualization model for cloud / Proc. of the IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012, pp. 219–224.
27. Luo S., Lin Z., Chen X., Yang Z., Chen J. Virtualization security for cloud computing service / Proc. of the IEEE International Conference on Cloud and Service Computing (CSC), 2011, pp. 174–179.
28. Sharma P., Sood S.K., Kaur S. Security Issues in Cloud Computing // High Performance Architecture and Grid Computing Communications in Computer and Information Science, 2011, V.169, pp. 36–45.
29. Tsai H., Siebenhaar M., Miede A., Huang Y., Steinmetz R. Threat as a Service?: Virtualization's Impact on Cloud Security // IT Professional, 2012, pp. 32–37.
30. Grobauer B., Walloschek T. Stocker E., Understanding Cloud Computing Vulnerabilities // IEEE Security & Privacy, 2011, Vol. 9, pp. 50–57.
31. SP 800-95. Guide to Secure Web Services. Recommendations of the National Institute of Standards and Technology, 2007, 128 p.
32. SANS Report: 60% Of All Attacks Hit Web Applications, Dark Reading's special September issue on Web Applications security, 2009, http://www.darkreading.com.
33. OWASP Top 10 Project. The Open Web Application Security Project, 2010, http://www.owasp.org/index.php/Top_10_2010.
34. Web Application Security Scanners, http://projects.webappsec.org/w/page/13246988 /Web%20Application%20Security%20Scanner%20List
35. Xie W., Ma H. A policy-based security model for Web system / Proc. of the International Conference on Communication Technology Proc. (ICCT), 2003, Vol. 1, pp. 187–191.
36. Guan H., Chen W., Liu L., Yang H. Estimating Security Risk for Web Applications using Security Vectors // Journal of Computers, 2012, Vol. 23, No 1, pp. 1–5.
37. Hwang K., Kulkarni S., Hu Y. Cloud Security with Virtualized Defense and Reputation-based Trust Management / Proc. of the IEEE 8th International Conference on Dependable, Autonomic and Secure Computing, 2009, pp. 717–722.
38. Rashidi A., Movahhedinia N.A. Model for User Trust in Cloud Computing // IEEE International Journal on Cloud Computing: Services and Architecture (IJCCSA), 2012, Vol. 2, No 2, pp. 1–8.
39. Cabarcos P.A., Mendoza F.A., Lo´pez A.M., Sa´nchez D.D., Guerrero R.S. A Metric-Based Approach to Assess Risk for ''On Cloud'' Federated Identity Management // Journal of Network and System Management, 2012, Vol. 20, No 4, pp. 513–533.

УДК 004.056

Алгулиев Расим М.[1], Абдуллаева Фаргана Д.[2]
Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]director@iit.ab.az, [2]farqana@iit.ab.az

Исследование и анализ проблем информационной безопасности облачных технологий

Статья посвящена анализу проблем обеспечения информационной безопасности облачных технологий. В процессе проведения исследования были изучены причины создания, основные понятия, характеристики, сервисные модели и модели развертывания облачных технологий. Исследованы актуальные задачи информационной безопасности облачных технологий, такие, как управление идентификацией, безопасность веб-программ, виртуализация и управление доверием. Выявлены существующие проблемы облачных технологий, предложены ряд рекомендаций в направлении устранения этих проблем.

Ключевые слова: *облачные технологии, виртуализация, управление идентификацией, управление доверием, единый вход, федеративное управление идентификацией.*

Rasim M. Alguliev[1], Fargana C. Abdullayeva[2]
Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]director@iit.ab.az, [2]farqana@iit.ab.az

An investigation and analysis of security problems of the Cloud Computing

In this paper the security problems of cloud computing technologies have been investigated. At the investigation stage the motives underlying the establishment of cloud computing technologies, main concepts, characteristics, service models and deployment models were studied. Also current security problems of cloud computing technologies, especially in the area of identity management, web applications, virtualization, trust management have been analyzed. At the result the article had identified existing problems of main tasks of cloud computing technologies and offered a number of recommendations towards to solving of these problems.

Keywords: *Cloud computing, virtualization, identity management, trust management, single sign-on, federated identity management.*