Bulud texnologiyalarında identifikasiya federasiyasının dinamik idarəetmə modeli

Fərqanə Abdullayeva
AMEA İnformasiya Texnologiyaları İnstitutu
farqana@iit.ab.az

***Xülasə*— İstifadəçilərin identifikasiya məlumatlarının federasiyasının dinamik idarə edilməsini təmin edən model təklif olunmuşdur. Tədqiqat prosesində vahid giriş texnologiyalarının və federativ idarəetmə mexanizminin iş prinsipi öyrənilmişdir, mövcud vəziyyəti araşdırılmışdır. Multiagent sistemləri və qərarların qəbulu yanaşmalarını tətbiq etməklə, identifikasiya məlumatlarının federasiyasının dinamikliyi təmin olunmuşdur.**

Açar sözlər— federativ idarəetmə; vahid giriş; provayder; bulud texnologiyaları;

I. GİRİŞ

Son zamanlar bulud texnologiyalarının meydana gəlməsi İnternet mühitində böyük inqilabi çevrilişə səbəb olmuşdur. Lakin bu texnologiyanın informasiya təhlükəsizliyinin təmin edilməsi problemləri onun geniş tətbiqinə ciddi maneə törədir.

Bulud texnologiyalarının təhlükəsizliyi sahəsində aparılan tədqiqatların və standartlaşdırma sənədlərinin əksəriyyətində mühüm məsələlər sırasına identifikasiya məlumatlarının idarə edilməsi, etibar münasibətlərinin qurulması və risklərin qiymətləndirilməsi aid edilir.

ENISA (European Network and Information Security Agency) təşkilatı tərəfindən dərc olunan təlimatda [1] bulud infrastrukturunda etibar münasibətinin qurulması mühüm elmi-tədqiqat istiqaməti kimi müəyyən olunur. NIST (National Institute of Standards and Technology) [2] və CSA (Cloud Security Alliance) təşkilatlarının [3] bulud texnologiyalarının təhlükəsizliyi sahəsində hazırladığı tövsiyələrdə identifikasiya məlumatlarının idarə edilməsi və etibar münasibətlərinin qurulması mühüm məsələ kimi vurğulanır. Bundan əlavə bir sıra digər standartlaşdırma təşkilatları və elmi-tədqiqat müəssisələri tərəfindən dərc olunan sənədlərdə də identifikasiya məlumatlarının federasiyasının təşkili əvəzolunmaz mexanizm kimi göstərilir [4, 5].

Bulud infrastrukturunda identifikasiya məlumatlarının federativ idarə edilməsi sahəsində aparılan elmi-tədqiqat işlərinin sayı az deyil. Bu işlər sırasında buludlar arasında federasiyanın təşkili [6], identifikasiya məlumatlarının idarə edilməsi proseslərinin inteqrasiyası [7] məsələlərinə həsr olunmuş yanaşmalar diqqəti daha çox cəlb edir. Bu yanaşmaların çatışmayan cəhəti odur ki, identifikasiya məlumatlarının idarə edilməsi modelləri provayderlər arasında əvvəlcədən mövcud olan etibar münasibətləri üzərində qurulur və yalnız rəqəmli sertifikatlar, Açıq Açarlı İnfrastruktur (Public Key Infrastructure, PKI) kimi statik texnologiyalara əsaslanır.

Hazırda identifikasiya məlumatlarının idarə edilməsinə xidmət edən bir sıra aparıcı təşkilatlar tərəfindən sistemlər yaradılmışdır. Bu sistemlərə misal olaraq McAfee Cloud Identity Manager, Microsoft Identity & Access, Novell Identity Manager, EmpowerID SSO Manager, Symplified Trust Cloud, OneLogin, IdM4Cloud və s. göstərmək olar. Bu sistemlərin çatışmazlığı onların müəyyən məhdudiyyətlər çərçivəsində işləməsidir. Bu sistemlərdə inteqrasiya vasitələrinin kifayət qədər effektiv qurulmaması, sistemlərin əhatə dairəsini ani genişləndirməyə imkan vermir. Yəni provayderlərin sayı artıqca göstərilən sistemlər inteqrasiya olunmaq funksiyasını itirir.

Təqdim olunan işdə bulud infrastrukturunun dinamiklik xüsusiyyətlərini (məsələn, buludun miqyasını asanlıqla artırıb azaltmağın mümkünlüyü) nəzərə alan federativ idarəetmə modeli verilir. Model, multiagent sistemlərinin hesabına subyekt haqqında lazımi məlumatlar toplayaraq, bu məlumatlar əsasında real vaxt rejimində dinamik qərar qəbul etmək imkanına malikdir. Bulud kimi qeyri-müəyyən mühitdə qərar qəbulu prosesinin reallaşdırılması üçün mühüm vasitə subyektin etibar dərəcəsinin qiymətləndirilməsidir. Etibar dərəcəsinin müəyyən metrikalar əsasında hesablanmış ədədi qiyməti vasitəsilə bulud provayderləri arasında dinamik etibar münasibətini quraraq federasiyanı təmin etmək mümkündür.

II. VAHİD GİRİŞ TEXNOLOGİYALARI VƏ FEDERATİV İDARƏETMƏ

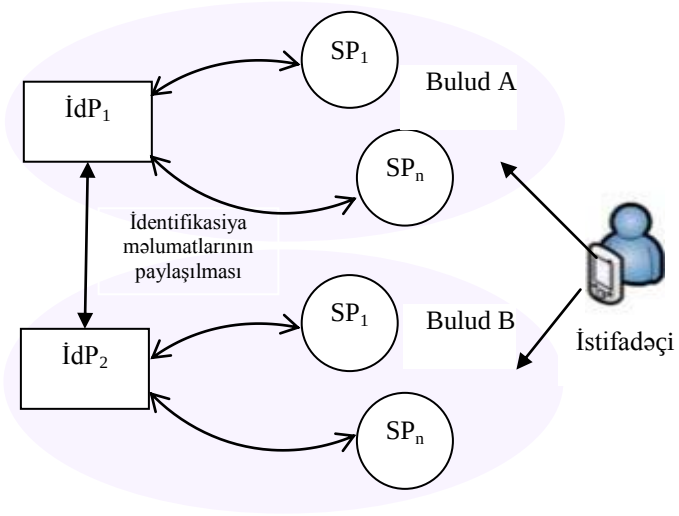
İnternet mühitində istifadəçilər müxtəlif xidmətlərdən istifadə edərək ayrı-ayrı servis provayderinin resurslarına giriş əldə edir. Bu xidmətləri istifadə üçün yaradılan parollar və istifadəçi adları bir-birindən fərqli olur. Bu səbəbdən şəbəkə istifadəçilərinin böyük əksəriyyəti eyni bir paroldan mümkün olan yerdə istifadə etməyə cəhd edir. Bu isə ciddi təhlükəsizlik risklərinin meydana gəlməsinə səbəb olur. İstifadəçilərin təkrar-təkrar autentifikasiya olunması, onlarda narahatçılıq yaratmaqla yanaşı, bir sıra administrativ xərclərin miqdarını da kəskin artırır. Hazırda dünya təşkilatlarının əksəriyyəti parollara qarşı mübarizə aparmaq məqsədilə vahid giriş (Single Sign On, SSO) texnologiyalarından istifadə etməyə cəhd edir. Çünki bu texnologiyalar çoxsaylı şəbəkə parollarını vahid parolla əvəz etməyə imkan verir.

Vahid giriş texnologiyaları – bir İdP-də autentifikasiyadan keçmiş istifadəçinin, əlavə autentifikasiya prosesi keçmədən, İdP ilə federativ münasibətdə olan bütün SP-i çoxluğuna giriş imkanı verən texnologiyadır.

Federasiya − identifikasiya məlumatlarının idarə edilməsini təmin edən konsepsiyalardan biridir. Bu konsepsiyanın əsas məqsədi istifadəçi atributlarının və identifikasiya məlumatlarının müəyyən siyasət əsasında müxtəlif domenlər arasında paylanmasıdır.

Federativ modeli aşağıdakı üç aktor təşkil edir (Şəkil 1):

- *Servis provayderi (SP).* İstifadəçinin identifikasiya məlumatlarından istifadə edən aktordur. SP istifadəçinin etibarlı olduğunu, üçüncü tərəf aktorun (İP) autentifikasiya məlumatlarına əsasən yoxlayır. SP-ni adətən etibar edən tərəf də (Relying Parties, RP) adlandırırlar.
- *İdentifikasiya Provayderi (İdP).* Subyekt haqqında məlumatı təsdiqləyən aktordur. İdP-ni adətən təsdiqləyici tərəf də (Asserting Parties, APs) adlandırırlar. İdP-i istifadəçilərin autentifikasiyasını həyata keçirir və identifikasiya məlumatlarını idarə edir.
- *İstifadəçilər.* İstifadəçi agentlərinin (məsələn, veb brauzerlər) köməyi ilə SP-i ilə qarşılıqlı əlaqə yaradan aktorlardır.



Şəkil 1. Federativ idarəetmə prosesi

Şəkildən göründüyü kimi, identifikasiya məlumatlarının iki provayder arasında paylaşılması istifadəçiyə imkan verir ki, o bir domenə daxil olaraq digər domenin də resurslarından istifadə etsin. SAML, Liberty Alliance (LA), Shibboleth, OpenID, WS-Federation kimi standart İnternet texnologiyaları identifikasiya provayderləri arasında federasiyanı təmin edən texnologiyalardır.

SAML (Security Assertion Markup Language). Subyektlər arasında təhlükəsizlik bəyannamələrinin mübadiləsini təmin edən XML-yönümlü protokoldur. Bu modeldə SP ilə İdP-i arasında etibar münasibətləri əvvəlcədən müəyyən olunur. Etibar münasibətlərinin qurulması PKİ [8] texnologiyasına əsaslanır. 2005-ci ildə yaradılıb OASIS təşkilatına məxsusdur.

Shibboleth. "Internet2 Middleware Initiative" konsorsiumunun layihəsidir, SAML texnologiyası üzərində qurulmuşdur. Dünyada ən geniş tətbiq olunan federativ idarəetmə mexanizmidir, istifadəçilərin resurslarla həm təşkilatdaxili və həm də təşkilatlararası əlaqələnməsini təmin edir. Burada provayderlər arasında federasiya prosesi provayderlərin adlarının daxil edildiyi böyük siyahıya əsasən aparılır. Bu siyahı provayderlər arasında ümumi qaydalardan istifadə etməyə imkan verir. Burada provayderlər siyahısının idarə edilməsinin mürəkkəbliyi bu modelin çatışmayan cəhətlərindən biridir.

OpenID. İstifadəçi-yönümlü protokoldur. Bu o deməkdir ki, burada istifadəçi autentifikasiya olunmaq üçün İdP-ni özü seçir. Burada etibar modelindən istifadə olunmur.

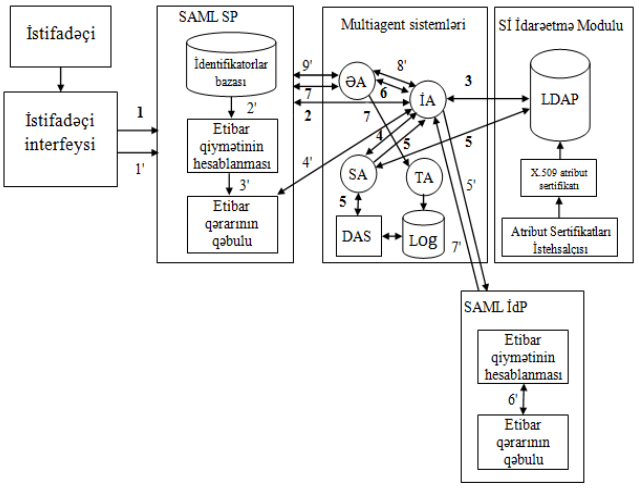
Identity Federation Framework (ID-FF). Liberty Alliance təşkilatına məxsus layihədir. Bu modeldə subyektlər arasında federasiyanın təmin edilməsi "Etibar çevrəsi" (Circle of Trust, CoT) konsepsiyasına əsaslanır.

WS-Federation. Bu modeldə subyektlər arasında federasiyanın təmin edilməsi WS-Trust (Web servise) konsepsiyası əsasında təmin edilir.

Aparılan tədqiqatlar göstərir ki, provayderlər arasında federasiyanın mövcud texnologiyalar əsasında təmin edilməsi əvvəlcədən məlum olan statik etibar münasibətləri üzərində qurulur. Bu isə bulud kimi dinamik infrastrukturda əlverişli hesab olunmur. Bu səbəbdən bulud texnologiyalarının xüsusiyyətlərini nəzərə alan, yeni növ dinamik federativ idarəetmə modelinin işlənməsi zərurəti meydana çıxır.

III. BULUD TEXNOLOGİYALARINDA İDENTİFİKASİYA MƏLUMATLARINI FEDERATİV İDARƏETMƏ MODELİ

Şəkil 2-də təqdim olunan model istifadəçilərin identifikasiya məlumatlarının federasiyasının dinamik idarə edilməsini təmin edir və autentifikasiya, avtorizasiya prosesinə əsaslanır.



Şəkil 2. İdentifikasiya məlumatlarının federasiyasının dinamik idarə edilməsi arxitekturu

Burada istifadəçilərin bulud infrastrukturuna vahid girişini təmin etmək üçün SAML protokolundan istifadə olunur. İstifadəçilərin identifikasiya məlumatlarının federasiyasının dinamik idarə edilməsi prosesi PKİ texnologiyasına və etibar

qiymətinin hesablanması yanaşmasına əsaslanır. Burada istifadəçilərin bulud infrastrukturuna girişi onların atribut sertifikatları əsasında təmin olunur və onlara müvafiq icazələr rollarla idarəetmə mexanizminə əsasən müəyyən olunur. Bulud kimi dinamik bir mühitdə rolların yalnız sertifikatlara əsasən statik müəyyən olunması məsələsi öz aktuallığını itirmiş olur və rolların dinamik idarə olunmasının təmin edilməsi zərurəti meydana çıxır. Bu səbəbdən arxitekturada multiagent sistemlərinin tətbiqi rolların dinamik müəyyən olunmasına imkan yaradır və istifadəşinin davranış xüsusiyyətlərini özündə cəmləşdirir.

Arxitekturanın müəyyən bir sistem şəklində fəaliyyətini təmin etmək məqsədilə aşağıdakı komponentlərdən istifadə olunmuşdur:

Multi-agent sistemi (MAS). Bulud texnologiyaları çərçivəsində autentifikasiya, avtorizasiya və audit əməliyyatlarını yerinə yetirir. MAS modulunun etibarlılıq dərəcəsi PKİ (Public Key İnfrastructure) tərəfindən müəyyən olunur. MAS aşağıdakı agentlərdən ibarətdir:

- *İstifadəçi agenti (İA).* İstifadəçi sertifikatlarının təsdiqlənməsi, istifadəçi sorğularının yoxlanması, Siyasət Agentindən (SA) avtorizasiya məlumatlarının əldə olunması, istifadəçiyə imtiyazlar siyahısının təqdim olunması funksiyalarını yerinə yetirir.
- *Toplayıcı agent (TA).* Loq serverlə interfeys yaradan agentdir. Sistemə daxil olan bütün subyektlərin fəaliyyəti ilə bağlı loq-yazılar bu agentə göndərilir və bu interfeys vasitəsilə loq-serverə əlavə olunur.
- *Siyasət agenti (SA).* İstifadəçinin atribut sertifikatlarındakı rollarını və DAS-də yaradılmış DİS-nı birləşdirərək, istifadəçi üçün vahid imtiyazlar siyahısı (VİS) yaradır.
- *Əlaqə Agenti (ƏA).* SP ilə əlaqə yaratmaq üçün təyin edilmişdir.

Davranışı Analiz edən Server (DAS). İki funksiyanı yerinə yetirir: loq faylları analiz edir və istifadəçi üçün Dinamik İmtiyazlar Siyahısı (DİS) formalaşdırır. Bu siyahı istifadəçinin davranışı ilə bağlı məlumatlardan ibarət olduğu üçün DİS adlanır.

Loq-server. Hər bir subyektin sistemdə fəaliyyəti ilə bağlı loq yazıları toplayır.

Sertifikat İstehsalçısının (Sİ) İdarəetmə Modulu. X.509 tipli atribut sertifikatı istehsal edən komponentdir. Bu sertifikat fiziki olaraq LDAP (Lightweight Directory Access Protocol) kataloqunda saxlanır. Atribut Sertifikat (AS) – Buluda daxil olmaq istəyən istifadəçinin imtiyazları AS-da göstərilən rollara əsasən idarə olunur. Atribut sertifikatının strukturunu aşağıdakı xanalar təşkil edir: sertifikatın versiyası, sertifikatın sahibi, istehsalçı təşkilatın adı, imzası, seriya nömrəsi, qüvvədə olma müddəti, istifadəçinin atributları. Atributlar xanasına istifadəçinin rolları daxil edilə bilər.

IV. FEDERATİV İDARƏETMƏ MODELİNDƏ İNFORMASİYA AXINI

İdentifikasiya məlumatlarının federasiyasının dinamik idarə edilməsi modelində informasiya axını iki mərhələdə həyata keçirilir (şəkil 2): etibar çevrəsi məlum olan və etibar çevrəsi məlum olmayan federativ idarəetmə mərhələləri.

Etibar çevrəsi məlum olan federativ idarəetmə mərhələsi

1. *İki-faktorlu autentifikasiya.* İstifadəçi smartkartlarda və ya tokenlərdə saxlanan sertifikatlar əsasında iki-faktorlu autentifikasiya prosesini həyata keçirmək üçün SP-nə sorğu göndərir.
2. *MAS-ın yaradılması.* Əgər istifadəçi SP-nin identifikatorlar bazasında qeydiyyatdadırsa, SP MAS moduluna sorğu göndərir, bu sorğunun əsasında istifadəçi üçün İA yaradılır. İA komponentinin təyinatı istifadəçinin bütün sorğularını idarə etməkdir. MAS yalnız SP tərəfindən təsdiqlənmiş istifadəçilər üçün İA yaradır və bu yeni yaradılmış İA avtomatik olaraq etibarlı subyekt kimi qəbul olunur.
3. *İstifadəçi sertifikatının yoxlanması.* İA LDAP kataloqunu axtarır, istifadəçi sertifikatının həqiqiliyini təsdiqləyir və onun sistemdə əvvəlcədən müəyyən olunmuş təhlükəsizlik siyasətinə uyğunluğunu yoxlayır.
4. *İstifadəçinin imtiyazlarının müəyyən olunması. B*urada istifadəçi üçün imtiyazlar siyahısının yaradılması həyata keçirilir. Bu imtiyazlar əsasında istifadəçi bulud infrastrukturunda bu və ya digər əməliyyatı həyata keçirmək imkanı əldə edir. Bunun üçün İA SA-ya sorğu göndərərək sertifikatı yoxlanmış istifadəçiyə imtiyazlar siyahısı yaradır.
5. *Dinamik imtiyazlar siyahısının istifadəçi rolları ilə birləşdirilməsi.* SA LDAP kataloquna müraciət edərək müxtəlif sertifikatlardan istifadəçinin statik rollarını əldə edir və onu DAS blokunda yaradılmış dinamik imtiyazlar siyahısı ilə birləşdirib İA blokuna göndərir. DAS blokunda yaradılmış imtiyazlar siyahısı istifadəçinin fəaliyyəti ilə bağlı məlumat-lardan ibarət olduğu üçün onun strukturu dinamik dəyişkəndir.
6. *Avtorizasiyanın verilməsi.* İstifadəçinin İA blokuna göndərilən sorğusu istifadəçinin imtiyazlar siyahısı ilə müqayisə olunur. Əgər istifadəçi avtorizasiya olunmuş istifadəçidirsə, onda İA istifadəçi üçün yeni sessiyanın başlanmasını təmin etmək üçün ƏA blokuna sorğu göndərir.
7. *Sessiyanın başlanması.* ƏA sorğunu imzalayıb SP-nə göndərir. SP sorğunu qəbul edir, və əvvəlki mərhələdə ƏA-nın imzaladığı imzanı yoxlayaraq, sorğunun etibarlılıq dərəcəsini müəyyən edir və sessiyanın başlanmasına icazə verir. ƏA-da baş verən hadisələr eyni zamanda TA blokuna göndərilir.

Yuxarıda göstərilən prosesdə SP ilə İdP arasında müəyyən müqavilələr əsasında əvvəlcədən müəyyən olunmuş etibar münasibəti vardır və burada istifadəçinin İdP-də qeydiyyatda

olması ona imkan verir ki, heç bir əlavə qeydiyyat prosesi keçmədən SP-nin infrastrukturuna daxil olsun.

Fərz edək ki, istifadəçinin SP-nin infrastrukturunda qeydiyyatı yoxdur, və o autentifikasiya prosesini SP-də deyil yalnız özünün hesab məlumatı olan İdP-də həyata keçirərərk SP-nin resurslarından istifadə etmək istəyir. Və bu provayderlər (SP ilə İdP) bir-birinə qarşı qeyri-müəyyən subyektlərdir, yəni bu provayderlər arasında əvvəlcədən müəyyən olunmuş statik etibar münasibətləri qurulmamışdır və onların etibar çevrəsi fərqlidir. Bu halda federativ idarəetmənin təmin edilməsi zəruri hesab olunur və aşağıdakı kimidir.

Etibar çevrəsi məlum olmayan federativ idarəetmə mərhələsi

1. İstifadəçi SP-nin resurslarından istifadə etmək üçün SP-ə sorğu göndərir.
2. İdentifikatorlar bazasında istifadəçinin qeydiyyatda olmadığı aşkarlanır və etibar qiymətinin hesablanması blokuna sorğu göndərilir. Burada müəyyən metrikalar əsasında (məsələn, İdP-nin reputasiya məlumatları, Servis səviyyəsi haqqında müqavilədəki məlumatlar və s.) istifadəçinin qeydiyyatda olduğu İdP-nin etibar qiyməti hesablanır.
3. Etibar qiyməti qərar qəbulu blokuna göndərilir və əgər alınmış etibar qiyməti SP-nin qəbul etdiyi sərhəd (threshold) qiymətindən böyük olmazsa, onda SP-i İdP-ni etibarlı subyekt kimi qiymətləndirir.
4. Qərar qəbulu bloku federasiya yaratmaq üçün MAS moduluna sorğu göndərir, bu sorğunun əsasında istifadəçi üçün İA yaradılır.
5. İA bloku vasitəsilə sorğu İdP-nə göndərilir.
6. Subyektlərin etibar qiyməti hər iki tərəfə məlum olmalıdır ki, onlar arasında federasiya prosesi başlasın. Bu səbəbdən SP ilə etibar münasibəti qurmaq və federasiyaya başlamaq qərarı qəbul etmək üçün İdP də öz növbəsində SP-nin etibar qiymətini hesablayır və onu göndərir Etibar Qərarının Qəbulu blokuna.
7. Əgər alınmış etibar qiyməti İdP-nin qəbul etdiyi sərhəd qiymətindən böyük olmazsa, onda İdP-i SP-ni etibarlı subyekt kimi qiymətləndirir və federasiya yaratmaq üçün İA blokuna sorğu göndərir.
8. İA bu məlumatlar əsasında ƏA blokuna sorğu göndərir.
9. ƏA sorğunu imzalayıb SP-nə göndərir. SP ƏA-nın imzasını yoxlayaraq, sorğunun etibarlı olduğuna əmin olur və istifadəçi üçün yeni sessiyanın başlanması təmin olunur.

NƏTİCƏ

Ənənəvi idarəetmə mexanizmlərində istifadəçilərin autentifikasiyası adətən sistemdə müəyyən olunmuş idarəetmə siyahısına əsasən həyata keçirilir. Lakin istifadəçilərin sayı artdıqca bu siyahını idarə etmək mürəkkəb məsələyə çevrilir. İstifadəçilərinin sayı çox olan bulud kimi bir mühitdə identifikasiya məlumatlarının idarə edilməsini təmin edən effektiv vasitə dinamik idarəetmə mexanizminin yaradılmasıdır. Bu məqsədlə arxitekturada multiagent sistemləri tətbiq olunur. Multiagent sistemləri dinamikliyi, istifadəçinin davranış xüsusiyyətlərini özündə cəmləşdirən rolların müəyyən olunması hesabına təmin edir. Digər tərəfdən, burada tərəflər arasında etibar dərəcəsinin qiymətləndirilməsi yanaşmasının tətbiqi, idarəetmə sisteminin dinamikliyini təmin etməyə xidmət edir.

Hazırda etibar dərəcəsinin qiymətləndirilməsi istiqamətində effektiv alqoritmin yaradılması istiqamətində biz tərəfimizdən tədqiqat işləri aparılır.

ƏDƏBİYYAT

[1] D. Catteddu, G. Hogben, "Cloud computing: benefits, risks and recommendations for Information security," European Network and Information Security Agency Technical Report, 2009, 125 p.
[2] SP 800-144. "Guidelines on Security and Privacy in Public Cloud Computing," National Institute of Standards and Technology Special Publication, 2011, 70 p.
[3] "Security Guidance for Critical Areas of Focus in Cloud Computing," Cloud Security Alliance, 2011, 176 p.
[4] "Identity in the Cloud−Use Cases," Organization for the Advancement of Structured Information Standards, 2012, 111 p.
[5] "Moving to the Cloud," Cloud Computing Use Case Discussion Group, 2011, 11 p.
[6] V. Casola, M. Rak, U. Villano, "Identity federation in cloud computing," In Proc. of the IEEE 6th International Conference on Information Assurance and Security, 2010, pp. 253–259.
[7] A. Celesti, F. Tusa, F.M. Villari, A. Puliafito, "Security and cloud computing: Intercloud identity management infrastructure," In proc. of the 19th IEEE International Workshop on Enabling Technologies: Infrastructures for Collaborative Enterprises, 2010, pp. 263–265.
[8] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL)," RFC 5280, 2008, 151 pp.