

Korporativ elektron poçt sistemində təhlükəsizlik məsələləri

Rəşid Ələkbərov¹, Səməd Dursunov², Mürsəl Qurbanlı³

^{1,2,3}AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹t.direktor_muavini@iit.science.az, ²samed@iit.science.az, ³m.qurbanli@iit.science.az

Xülasə— Məqalədə e-poçt serverlər, onların tarixi, işləmə prinsipi araşdırılmışdır. Mail Exchange serverin işləmə prinsipi, xüsusiyyətləri, digər e-poçt serverlərdən üstün cəhətləri, spamlardan və zərərli viruslardan qorunması üçün lazım olan tədbirlər haqqında geniş məlumat verilmişdir.

Açar sözlər— Mail Exchange; Active Directory; e-poçt protokolları; spam; MX, TLS, OWA, virus

I. GİRİŞ

Elektron poçt (Electronic Mail və ya E-Mail) – hazırkı dövrdə insanlar arasında ən çox yayılmış ünsiyyət növüdür. Bu ünvan bir neçə saniyə ərzində İnternet şəbəkəsinin yerləşdiyi istənilən yerə nəinki mətn, veb-səhifə, hətta məktub halında olan istənilən faylı göndərməyə imkan verir. ABŞ və Avropadan başlayaraq bu rəbitənin adı "e-mail" və ya "email" formasında yazılır.

İlk elektron poçt bir çox texnoloji yeniliklərin başlanğıcı kimi, hərbi və təhlükəsizlik orqanlarının əməkdaşlarının istifadəsi üçün yaradılmışdı. 1960-cı illərin sonlarında hərbi sahə üçün sistemlər inkişaf etdirməyə çalışan Rels Tomlinson ilk olaraq 1971-ci il oktyabr ayında iki kompüter arasında fayl mübadiləsini həyata keçirmişdir.

Korporativ poçt - xüsusi olaraq şirkət üçün istifadə edilən e-poçtdur. Şəxsi poçtdan əsas fərqi ünvanın özüdür. Adətən, korporativ e-poçt ünvanları aşağıdakı formatda istifadə edilir: *yourname@companyname.com*.

Şirkət üçün korporativ poçtun təşkili üçün bir neçə əsas yol var. Bu və ya digər metodun seçimi həm işin həcmindən, həm də onun əsas xüsusiyyətlərindən və şirkətin poçt qutularına xidmət etmək üçün nə qədər xərcləmək istəyindən və bunun üçün bir büdcə ayırmağından asılıdır.

Gmail, Hotmail və s. e-poçt istifadəçiləri üçün ideal olan bir çox elektron poçt xidmətləri vardır və bu xidmətlər fərdi istifadəçilər tərəfindən pulsuz olaraq verilir. Pulsuz e-poçt xidmətlərindən çox güman ki, faydalanmışıq. Ancaq bir şirkət və ya bir müəssisə üçün, pulsuz xidmətlər göstərən e-poçtlar xoş qarşılanmaya bilər.

Bir nümunə ilə izah edək; şirkətin adının “adatum” olduğunu, domen adımızın “adatum.com” olduğunu fərz edək. Şirkətdən kənar heç kim bu kimi bir elektron poçt hesabından istifadə edə bilməyəcək. Çünki “adatum.com” adı altında

qeydə alınan bir domendir və heç kim tərəfindən istifadə edilə bilməz.

II. KORPORATİV ELEKTRON POÇT SİSTEMİNİN İŞLƏMƏ PRİNSİPİ

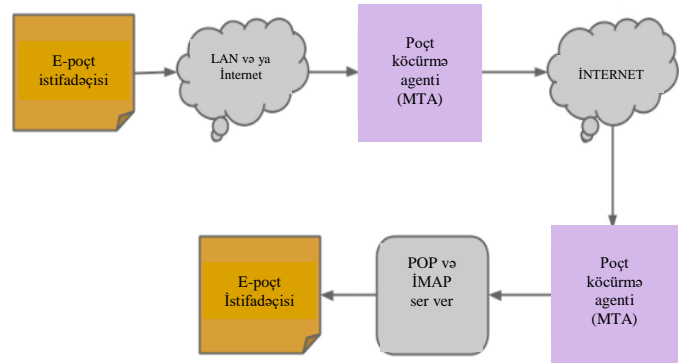
Korporativ poçt bir və ya bir qrup elektron poçt qutusudur. Məsələn, *company.com* üçün elektron poçt qutuları yaratmaq mümkündür; *info@company.com*, *sales@company.com* və ya *anna@company.com* və s.

Bir e-poçtun göndərildiyi anda bir mesaj, müştəridən e-poçt alıcıları e-poçt serverinə gedənə qədər sadə bir poçt ötürülməsi protokolu vasitəsilə serverdən serverə ötürülür.

İlk məktubu göndərən bir e-poçt tətbiqi istifadə edərkən mesajla birlikdə alıcının e-poçt ünvanını daxil etməlidir. Bu yerli kompüterlərdə edilməlidir. Bitdikdən və "Göndər" düyməsini sıxdıqdan sonra, e-poçt MTA-ya (Mail Transfer Agent) göndəriləcəkdir. Bu əlaqə SMTP protokolu vasitəsilə həyata keçirilir.

Növbəti addım DNS axtarışıdır. Sistem, alıcının müvafiq MTA-nı tapmaq üçün sorğu göndərir. Bu MX qeydinin köməyi ilə ediləcəkdir. DNS zonasında, alıcının domen ünvanında MX (Mail Exchanger) yazısı olacaqdır. Bu bir domenin poçt serverini təyin edən DNS yazısıdır. Beləliklə, DNS axtarışından sonra tələb olunan poçt serverinə alıcının poçt serverinin IP ünvanı ilə cavab verilir.

Növbəti addım mesajı poçt serverləri arasında ötürməkdir. Bu rəbitə üçün SMTP protokolu istifadə olunur (şəkil 1).



Şəkil 1. E-poçt serverinin işləmə prinsipi

İndi bu mesaj MDA vasitəsilə (Mail Delivery Agent) alıcının kompüterinə ötürülür. Daha əvvəl gördüyümüz kimi, burada iki protokoldan istifadə edilə bilər. POP3 istifadə etsək, onda bütün e-poçt kompüterə yüklənir və serverdəki nüsxə silinir. İstifadə olunan protokol IMAP-dırsa, o zaman e-poçt mesajı poçt serverində saxlanılır, ancaq istifadəçi kompüterdəki kimi poçt serverindəki e-poçtları asanlıqla idarə edə bilər. Hər iki protokolu istifadə edərkən fərq budur və e-poçtunuzun çatdırılma qaydası belədir. E-poçtu göndərməkdə bir səhv varsa, e-poçtlar gecikəcəkdir. Hər bir poçt serverində poçt növbəsi var. Bu poçtlar poçt növbəsində gözləyir. Poçt serveri e-poçtu yenidən göndərməyə çalışacaq. E-poçt göndərmə uğurlu bir nəticə verməyincə, poçt serveri geri göndərilən e-poçt mesajını göndərənin e-poçt ünvanına göndərə bilər.

III. MICROSOFT EXCHANGE SERVER KORPORATİV ELEKTRON POÇT PROQRAM TƏMİNATININ ÜSTÜNLÜKLƏRİ

Bildiyimiz kimi, günümüzdə mail alış-verişi artıq o qədər ciddi bir həddə gəlib çatıb ki, dünyanın bir çox şirkətlərinin işləri tamamilə mail serverlərdən asılıdır. Çoxsaylı böyük şirkətlər şəbəkəsinin mail axışını təmin etmək üçün mail xidməti göstərən bir çox məhsuldan istifadə edirlər ki, bunların arasında geniş yayılmış mail serverlərdən biri də Microsoft Exchange Server-dir.

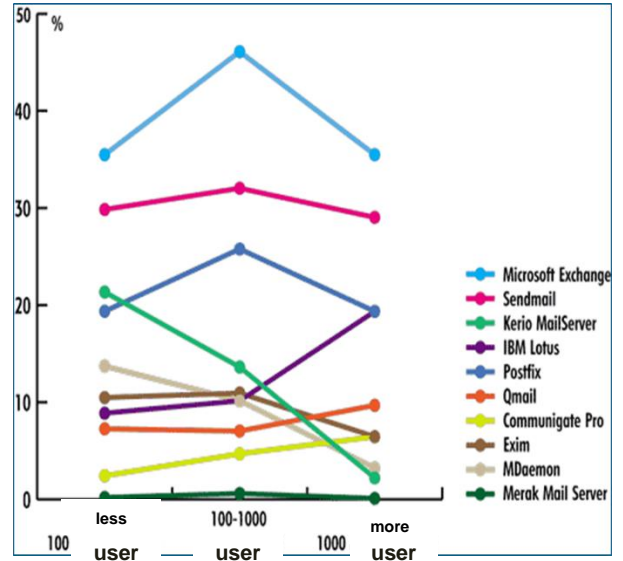
Microsoft Exchange Server – məlumat mübadiləsi və birgə iş üçün nəzərdə tutulmuş proqram təminatıdır. İlk versiyası 1993-cü ildə Microsoft şirkəti tərəfindən işlənilib hazırlanıb. Əsas funksiyaları poçt məlumatlarının emalı və göndərilməsi, mobil qurğuların dəstəklənməsi və səsli məlumat sistemləri ilə inteqrasiya (Exchange 2007 versiyasından başlayaraq), ani məlumat mübadiləsi sistemlərinin dəstəklənməsidir. Exchange server istər Microsoftun əvvəlki Exchange məhsullarından, istərsə də digər vendorların məhsulları ilə müqayisədə imkanlarına və funksionallığına görə çox fərqlənir. Microsoft şirkəti Exchange strukturu buluda daşıyaraq eyni zamanda Exchange Online xidməti də göstərməkdədir.

Microsoft Exchange Server istifadə edən şirkətlər, işçilərinə dünyanın istənilən yerindən elektron poçtlarına daxil olmağa icazə verə bilər. İşçinin ofisdə və ya yolda olmasından asılı olmayaraq, bütün vacib sənədlərini əldə edə və hər an vacib bir sorğuya bildirişlə cavab verə bilər. Microsoft Exchange Server tərəfindən istifadə olunan e-poçt platforması, e-poçt və əlaqə idarəçiliyini sadə və problemsiz etmək üçün hazırlanmış bir çox fərqli xüsusiyyətlərə malik Microsoft Office Outlook-dur. Microsoft Office Outlook və Microsoft Exchange Server ilə birlikdə istifadə edilə bilər bəzi xüsusiyyətlərə təqvim xüsusiyyətləri, planlaşdırma xüsusiyyətləri, səs poçtu saxlama və əlaqə idarəetmə proqramları daxildir.

Dünya üzrə istifadə olunan bir necə poçt serverləri mövcuddur (şəkil 2). Bunlara aşağıdakıları göstərmək olar:

- Microsoft Exchange Server;
- Sendmail;

- Kerio MailServer;
- IBM Lotus;
- Postfix;
- Qmail;
- CommuniGate Pro.



Şəkil 2. Müxtəlif ölçülü şirkətlərdə E-poçt serverlərinin istifadə diaqramı

Exchange Serverin yerinə yetirdiyi funksiyalar aşağıdakılardır:

- e-poçt və sənədlərin paylaşımı;
- mərkəzi əlaqə trafikinin yaradılması;
- təhlükəsiz məlumatların saxlanması və məlumatların ehtiyat sürətinin alınması;
- təqvim və kontaktların yaradılması, idarə edilməsi;
- qaydalar vasitəsilə əməliyyatların avtomatlaşdırılması.

Microsoft Exchange Serverin digər e-poçt serverlərindən üstün cəhətləri vardır:

1. Poçt hesabına istənilən yerdən Outlook Web Access (OWA) ilə daxilolma imkanı. İnternetin hər hansı bir yerindən elektron poçtlara daxil olmaq imkanı verir. Bundan əlavə, Microsoft Exchange ilə e-poçt, təqvim, ünvan kitabı, kimi digər xüsusiyyətlər serverdə saxlanılır. Bu şəkildə elektron poçtlarda və istifadəçinin bir mərkəzdən bütün poçtlarında məlumatların təhlükəsizliyi təmin edilir.

Yalnız kompüterlərlə deyil, portativ əl cihazları (PDA - Blackberry - iPhone - Android) ilə poçt qutusunda daxil olmaq imkanı əldə etmək mümkündür.

2. Fayl paylaşımı. Şirkətlər və ya şöbələr üçün İctimai qovluqlar yaratmaq, sənədləri və vacib mesajları bu ictimai qovluqlarda saxlamaq və istifadəçilər ilə paylaşmaq mümkündür. Ümumi bir qovluqda bir e-poçt ünvanı təyin etmək olar. Bu şəkildə, e-poçt ünvanına

təyin edilən elektron poçtlar birbaşa ictimai qovluğa düşəcək və bütün istifadəçilər bu e-poçt barədə məlumatlandırılacaqlar.

3. Vahid ünvan kitabçası. Həmkarlarınız haqqında bütün məlumatları telefon və poçt kontaktlarının sinxronlaşması sayəsində smartfonda saxlamaq mümkündür.
4. Exchange səsli mesaj (Unified Messaging).
İstifadəçilərə səs mesajları və mətn e-poçtlarını birləşdirmək və onları bir-birinə çevirmək imkanı verir.
5. Mobillik. Məkan və zamandan asılı olmayaraq istifadəçilərə daha çox mobil giriş imkanı verir.
6. Arxivləşdirmə xüsusiyyəti. Şəxsi arxivləşdirmə və PST (Personal Storage Table) xidmətinin istifadəçi ilə əlaqəli olması.
7. Active Directory ilə sinxronlaşma. E-poçtun Active Directory ilə sinxronlaşdırılaraq 5 dəqiqə ərzində 1000 poçt qutusu yaradılması imkanı var.
8. Kommunikasiyanın qorunması. Microsoft Exchange-də quraşdırılmış təhlükəsizlik xüsusiyyətləri işgüzar yazışmaların təhlükəsizliyini və mübadilə zamanı məlumatların məxfiliyini təmin edir. Məlumat itkisindən qorunma xüsusiyyətləri, məzmunu ətraflı təhlil etməklə məxfi məlumatları tanımağa və qorumağa imkan verir.
9. Təhlükəsizlik. Spam və viruslardan yüksək keyfiyyətli qorunması (Microsoft Forefront Security).

Microsoft Exchange Server üçün bir neçə anti-spam proqram təminatı vardır:

1. GravityZone Enterprise Security for Exchange antispam və antivirus proqram təminatlarını özündə birləşdirən poçt serverləri üçün olan bir proqram təminatıdır. Məktublarnın təhlükəsiz şəkildə mübadiləsini təmin edir.
2. Exclaimer Anti spam dünyanın hər yerinə göndərilən spam məktubları təhlil edir və poçt qutularındakı elektron poçtlarla müqayisə edir.

IV. MICROSOFT EXCHANGE SERVER SİSTEMİNDƏ E-POÇTLARIN TƏHLÜKƏSİZLİK MƏSƏLƏLƏRİ

E-poçt təhlükəsizliyi bir elektron poçt hesabı və ya xidmətin girişi və kontentini təmin etmək üçün istifadə olunan kollektiv tədbirlərə aiddir. Bir şəxsə və ya bir təşkilata bir və ya bir neçə e-poçt ünvanına, hesablarına ümumi girişi qorumağa imkan verir.

E-poçt təhlükəsizliyi, bir e-poçt xidmətini təmin etmək üçün istifadə olunan, bir çox üsulu əhatə edən geniş bir termindir. Fərdi istifadəçi nöqtəyi-nəzərindən e-poçt təhlükəsizlik tədbirlərinə daxildir:

- Mürəkkəb şifr;
- Spam filtrləri;

- Anti-virus və anti-spam tətbiqləri.

Analoji olaraq, xidmət provayderi e-poçt serverində mürəkkəb şifr və girişə nəzarət mexanizmlərindən istifadə edərək e-poçt təhlükəsizliyini təmin edir. O, həmçinin istifadəsiz, etibarsız və zərərli e-poçt mesajlarını istifadəçinin poçt qutusuna çatdırılmasını məhdudlaşdırmaq üçün şəbəkə ekranı və proqram əsaslı spam filtrləmə tətbiqlərini də tətbiq edir.

Bir çox kiçik müəssisələr işçilərinin elektron poçtlarını, təqvimlərini və ünvan kitablarını idarə etmək üçün Microsoft Exchange serveri işə salırlar. Exchange sisteminin administratorunun fərqli server parametrlərini konfigurasiya etmək və Exchange tətbiqetmənin təhlükəsizliyinə nəzarət etmək imkanı var. Exchange serverin təhlükəsizliyini artırmaq üçün SMTP protokoluna giriş idarəetməsini məhdudlaşdırmalı və hesab məlumatları üçün TLS (Transport Layer Security) şifrələməsini tələb edilməlidir.

TLS bir-biri ilə əlaqə quran tətbiqlər arasında təhlükəsiz məlumat ötürülməsini təmin etmək üçün istifadə olunur. TLS təhlükəsizliyə böyük önəm verən etibarlı veb sayt bağlantılarında, sürətli mesajlaşma proqramında, fayl köçürmələrində, müxtəlif proqramlarda, internet tətbiqlərində, VPN (Virtual Private Network) əlaqələrində və hətta VOIP (Voice Over Internet Protocol) bağlantılarında geniş istifadə olunur. TLS həm şifrələmə, həm də avtorizasiya protokolidir. Bu protokollar serverdən serverə və ya serverdən müştəriyə təhlükəsiz məlumat ötürülməsini təmin edir.

V. AZSCİENCENET ŞƏBƏKƏSİNDƏ KORPORATİV E-POÇT SİSTEMİNİN YARADILMASI VƏ TƏHLÜKƏSİZLİYİ.

AMEA-nın institut və təşkilatların əməkdaşları müxtəlif ölkələrin domen sistemlərində yerləşən e-poçt sistemlərindən geniş istifadə edirdilər. Bu e-poçtlar aşağıdakı problemlərə səbəb olurdu:

- Qeyri-rəsmi e-poçt ünvanları vizual identifikasiya oluna bilmir;
- Rəsmi e-sənədlər yayılarkən digər e-poçt serverləri tərəfindən onlar spam kimi tanındığından ünvanlara yetişmir;
- Qeyri-rəsmi e-poçt ünvanları üzrə məsuliyyətin kimin üzərində olmasını müəyyən etmək çətinləşir;
- Qeyri-rəsmi e-poçt ünvanları AzScienceNet şəbəkəsindən kənarında olduğu üçün İnternet trafikdən istifadənin səmərəsini azaldır;
- AzScienceNet şəbəkəsi mühitində spamlar və viruslarla mübarizə siyasətini həyata keçirmək mümkün olmur;
- Qeyri-rəsmi e-poçt ünvanlarına mənsub olan elmi müəssisə və təşkilatların sənədlərinin kənardan izlənilməsi və analizinə imkan verir;
- AMEA üzrə informasiya təhlükəsizliyi siyasətinin həyata keçirilməsinə müəyyən təhlükələr yaranır.

AMEA Rəyasət Heyətinin 27 fevral 2014-cü il tarixli qərarında aşağıdakılar tələb olunur:

- AMEA üzrə bütün qurumlar və məsul şəxslər rəsmi e-poçt ünvanlarından istifadə etməlidirlər
- Rəsmi e-poçt ünvanları üzrə məsul şəxslər təyin olunmalıdır.
- AMEA üzrə e-sənədlərin mübadiləsi və yayılması rəsmi e-poçt ünvanları vasitəsi ilə həyata keçirilməlidir.
- İnformasiya təhlükəsizliyi siyasətinin tələblərinə müvafiq AzScienceNet şəbəkəsinin e-poçt xidmətinin fəaliyyəti gücləndirilməlidir.
- Rəsmi e-poçt ünvanları üzrə məsul şəxslərlə müvafiq təlimatlandırma işləri aparılmalıdır.

Yuxarıda göstərilən qərara əsasən AzScienceNet şəbəkəsinin verilənləri emal mərkəzinin e-poçt xidməti üçün Microsoft Exchange Server quraşdırılmış və işə salınmışdır.

AMEA üzrə rəsmi elektron poçt ünvanları sisteminin yaradılması məqsədilə AzScienceNet şəbəkəsinin verilənləri emal mərkəzində e-poçt xidməti üçün Mail-server quraşdırılmış və işə salınmışdır. Mail-server AzScienceNet şəbəkəsinin istifadəçilərinə xidmət edir. Mail-serverdə istifadəçilərə poçt qutuları yaratmaq, dəyişikliklər etmək üçün CommuniGate Pro proqram təminatı quraşdırılmışdır. 2017-ci ilin əvvəllərində isə Mail-serverdə təkmilləşdirmə işləri aparılmışdır və @ab.az domen adı @science.az domeni ilə əvəz olunmuşdur. AzScienceNet şəbəkəsinin xidmətlərindən istifadə edən AMEA-nın institut və təşkilatlarının sayı 46-dir. 6500-dən çox fərdi kompüter AzScienceNet şəbəkəsinə qoşulub. Hazırda e-poçt xidmətindən yararlanan istifadəçilərin sayı isə 1830-dür. Onların hər birinə Mail-serverdən 1Gbayt həcmdə yaddaş poçt qutusu yeri ayrılmışdır.

AzScienceNet-ə qoşulan hər bir abonent işlədiyi institut və təşkilatın adına uyğun domenlərlə indentifikasiya olunmuşdur. Məsələn, *depart1@iit.science.az* -İnformasiya Texnologiyaları institutunun 1-ci şöbəsi, *depart2@physics.science.az* – Fizika İnstitutunun 2-ci şöbəsi, *depart3@economy.science.az* – İqtisadiyyat İnstitutunun 3 sayılı şöbəsi və s. Bu cür indentifikasiya olunmuş domen adlar AMEA institut və təşkilatlarının arzu və təklifləri əsasında yaradılmışdır.

AzScienceNet-in Mail-serverində hər bir istifadəçinin poçt qutusunda məktublara 30 Mbayt həcmli müxtəlif tipli fayllar (mətnlər, şəkillər, audio və videolar) qoşaraq göndərmək olur. Hazırda AzScienceNet şəbəkəsində Milli Elmlər Akademiyasının hər bir istifadəçisi üçün ödənişsiz poçt xidməti göstərilir. 2017-ci ildə poçt serverdə təhlükəsizliyi təmin edilməsi və keyfiyyət göstəricisinin yüksəldilməsi üçün Windows Server 2016 və Microsoft Exchange Server 2016 Standart UsrCAL lisenziyalı proqram təminatı quraşdırılmışdır.

NƏTİCƏ

Məqalədə elektron poçt serverlərinin işləmə prinsipi haqqında geniş məlumat verilmişdir. E-poçt serverlərinin təhlükəsizliyi qeyd edilmişdir. TLS protokolu və onun işləmə prinsipi göstərilmişdir. Microsoft şirkətinin məhsulu olan Microsoft Exchange Server proqram təminatının üstünlükləri və əsas funksiyaları göstərilmişdir. Eyni zamanda qeyd edilən proqram təminatının e-poçt sistemində istifadəçilərin məlumatlarının təhlükəsizliyinin qorunması məsələləri analiz edilmişdir. Qeyd edilən proqram təminatı əsasında AzscienceNet şəbəkəsində korporativ e-poçt sistemi yaradılmış və istifadəyə verilmişdir.

İSTİNADLAR

- [1] P. Craig "The Technical Development of Internet Email" IEEE Annals of the History of Computing, 2008, 250 p.
- [2] R.W. Stanek, Exchange Server Pocket Consultant: Configuration & Clients, Microsoft Press; 1 editon, 378 p, 2013.
- [3] R. Morimoto, M. Noel, G. Yardeni, C. Amaris, A. Abbate, Microsoft Exchange Server 2013, Sams Publishing; 1 edition, 936 p, 2012.
- [4] G. Blokdyk, Anti-spam and Email Security A Complete Guide, SSTARCOoks Publishing, 288 p, 2018.
- [5] D. Cassens. "Law Firm's Automatic Deletion of Spam Emails Is Blamed for Failure to File Timely Appeal." ABA Journal, 325 p, 2017.
- [6] P. Craig, BBN Technologies, "The Technical Development of Internet Email", pp 3-29, 2008.
- [7] W. Shmied, K. Miller Microsoft Exchange Server 2007, John Wiley & Sons Ltd Publishing, 696 p, 2007
- [8] M. Tracy, W. Jansen, K. Scarfone, J. Butterfield Guidelines on Electronic Mail Security 154 p, 2007.
- [9] S. Furnell, P. Dowland E-mail Security ITGP Publishing; 1 edition, 350 p, 2010.
- [10] D.Elfassy Mastering Exchange Server, 818p, 2013

SECURITY ISSUES IN CORPORATE EMAIL SYSTEM

Rashid Alekberov¹, Samad Dursunov², Mursal Gurbanli³

^{1, 2, 3}Institute of Information Technology of ANAS, Baku, Azerbaijan

¹*t.direktor_muavini@iit.science.az* ²*samed@iit.science.az*,
³*m.qurbanli@iit.science.az*

Abstract— The article explores email servers, their history, and how they work. There is detailed information about the principles of Mail Exchange server operation, features, advantages of other e-mail servers, and necessary measures for protection against spam and malware.

Keywords— *Mail Exchange, Active Directory, email protocols, MX, TLS, OWA, virus*