Sahəyə aid mətnlərin leksik səviyyədə statistik təhlilinin nəticələri göstərir ki, belə mətnlərdə terminlər daha çox işlənir. Ona görə də elmi-texniki tərcümələr zamanı terminoloji lüğətlərin aktivləşdirilməsi nəzərdə tutulur. Bu da əsas lüğətin ümumişlək sözlərdən ibarət lüğətin olmasından irəli gəlir. Elmi-texniki mətndə qeydə alınan sahə terminləri ümumişlək sözlərin avtomatik lüğətində olmadıqda, proqram təminatı leksik səviyyədə başqa bloka müraciət olunmasına imkan yaradır. Əlavə leksik blok terminoloji lüğətləri özündə birləşdirir.

Elektron lüğətlər mövcud lüğətlərin kompüterə daxil edilməsi, həmçinin kompüter bazasında yeni lüğətlərin formalaşdırılması əsasında yaradılır.

Azərbaycan dilindən türk dilinə və əksinə türk dilindən Azərbaycan dilinə tərcümə qohum dillərin ortaq leksik bazasını, eləcə də leksika üçün qrafik səviyyədə fərqləri aydınlaşdırmağı tələb edir.

ŞƏBƏKƏ TƏHLÜKƏSİZLİYİNİN MONİTORİNQİ SİSTEMLƏRİNİN VƏ VASİTƏLƏRİNİN ANALİZİ

Nəbiyev B.R.
AMEA İnformasiya Texnologiyaları İnstitutu

Monitorinq idarəetmənin nəzarət funksiyalarından biridir. Inforasiya təhlükəsizliyində monitorinqlə yanaşı audit, nüfuzetmə testləri, informasiya sisitemlərinin attestasiyası, informasiya təhlüəsizliyi vasitələrinin sertifikatlaşdırılması, və s. kimi nəzarət funksiyaları da istifadə edilir. Şəbəkə təhlükəsizliyinin monitorinqi (ŞTM) dedikdə: Şəbəkə təhlükəsizliyinə təhlükə yaradan və ya yarada bilcək hadisələrin aşkarlanması və qarşısının alınması üçün müntəzəm və ya vaxtaşırı nəzarətin aparılması başa düşülür. Adətən ŞTM sahəsində mövcud elmi-tədqiqat işləri və tətbiqi sistemlər [1-4] korporativ şəbəkə miqyası ilə kifayətlənir. Qeyd etmək lazımdır ki, hətta orta ölçülü korporativ şəbəkələr üçün də şəbəkə təhlükəsizliyinin monitorinqi problematikdir. Problem şəbəkənin, istifadə edilən sistemlərin heterogenliyi, şəbəkənin müxtəlif hissələrində sensorlar tərəfindən generasiya edilən hadisələrin sayının olduqca çox olmasından, onların məkan və zamana görə paylanmasından və s. qaynaqlanır.

Monitorinq, cavab vermənin təmini və analiz funksiyalarına yalnız kompyuter şəbəkələrinə edilən hücum və pozuntu faktlarının aşkarlanması deyil, həmçinin önləyici tədbirlər kompleksinin hazırlanması və təhdidlərin nəticələrinin aradan qaldırılması da daxildir.

ŞTM-in vəzifələrinə gəlincə, bu sahədə əsas standarlar müəyyən olunmalıdır. Bu standartlar istifadəçilərin global və lokal şəbəkədən istifadəsini etibarlı və təhlükəsiz etməklə yanaşı informasiyanın toplanaraq analiz edilməsi üçün vacibdir. Bu baş verecek hadisənin qarşısını alınması və ya baş vermiş hadisəni tətqiq edilməsi üçün olduqca əhəmiyyətlidir.

Bu məqalədə ŞTM sahəsində monitorinq sistemlərinin və vasitələrinin xüsusiyətləri analiz edilir. Monitorinq sistemlərinin və vasitələrinin konsepsiyası aşağıdakılardan ibarətdir: 24x7x365 rejimində şəbəkə trafikinin toplanması, toplanmış trafikin analizi və problemlərin aşkarlanması, insidentlər haqqında xəbərdarlıqların generasiyası, hesabatların yaradılması və s.

ISA server 2006 Standartı (Microsoft Internet Security and Acceleration Server) Microsoft şirkətinin məhsuludur. İSA Server Proxy Server funksiyasını yerinə yetirməklə bərabər şəbəkəni xaricdən gələ biləcək təhdidlərə qarşı qoruyur və şəbəkələr arası ekran funksiyasını yerini yetirir.

GFİ Webmonitor - İSA serverdən istifadə ederek yeni imkanlar yaradır. Şəbəkələr arası ekran funksiyalarını genişləndirir - konkret fayl tipinin yuklənməsinə və online istifadəsinə qadağa qoyur, proksi serverdən keçən trafikin təhdidlərə qarşı 3 antivirus (Kaspersky, Norman, BitDefender) tərəfindən yoxlanmasına şərait yaradır, həmçinin HTTP trafikə qulaq asıraq online monitorinq üçün imkan yaradır. Bu proqram vasitəsi ilə

istifadəçilərin hansı veb səhifələrə və nə zaman daxil olduqlarını, nə qədər informasiya göturduklərini və s. kimi məlumatları almaq mümkündür.

Bandwidth splitter - istifadəçilərin məlumatı qəbul etmə və ötürmə sürətlərinə limit qoymaq üçün istifadə olunur.

Internet Access Monitor – Əməliyyat sistemində toplanan log failların avtonom analizi üçün istifadə olunur.

CACTİ proqram təminatı - statistik informasiyanı müəyyən vaxt intervalında SNMP vasitəsilə toplayaraq qrafiklər yaradır

SpamTitan - e-poçt xidmətinin anti spam və monitorinq sistemi. Monitorinq xidməti üçün gündəlik, həftəlik, aylıq və illik avtomatik hesabarlar (e-poçt və ya PDF formatında) yarada bilir. E-məktublar iki antiviru sistemi (ClamAV və Kaspersky) tərəfindən yoxlanır və antivirus bazası isə periodik yenilənir.

WebSpy Vantage – Ümumi şəbəkənin və istifadəçilərin tək və ya qrup halında monitorinqini həyata keşirir. Bu proqram vasitəsi ilə proksi serverdə toplanan log-faylları avtonom analiz etmək mümkündür. Bu proqram 200-dən çox log-fayl və hadisə jurnalı tipini dəstəkləyir, beləliklə zəruri olduqda digər tip log-fayl və hadisə jurnalı tiplərinidə analiz etmək imkanını yaradır.

Nagios – açıq kodlu proqram təminatı olub, kompyuter şəbəkəsinin, hesablama nöqtələrinin vəziyyətinin və servislərin monitorinqini təmin edərək administrator heyyətini xəbərdar edir. Nagios proqram təminatının imkanlarına şəbəkə servislərinə nəzarət (paralel monitorinqdə mümkündür), SSH və ya SSL şifrələmə tunelləri vasitəsi ilə kənardan monitorinqin təşkili, plaqinlər vasitəsilə modulların sadə genişlənmə arxitekturası, hostların ierarxiyasının müəyyən olunması da daxildir.

Cisco ASA – yüksək hesablama gücünə malik avadanlıqdır, trafikin süzgəclənməsini, viruslardan, soxulcan və müxtəlif tipli İnternet hücumlarından müdafiəni, korparativ şəbəkənin perimetrinin təhlükəsizliyini, VPN-lə qoşulma zamanı İPSec şifrələmə pratakolunu dəstəkləyir.

Beləliklə koporativ şəbəkələrın hər birində ŞTM müstəqil şəkildə həyata keçirilə bilər, lakin belə yanaşma səmərəli deyil, çünki qarşılıqlı asılı sistemlərın birində reallaşan təhlükə kaskad effekti ilə digər sistəmlərə də keçərək, bütün infrostrukturun işinin iflic edilməsinə səbəb ola bilər.

ƏDƏBİYYAT

1. Мельников М.И. Автоматизированная система мониторинга по сетям TCP/IP // Доклад Томский государственный университет систем управления и радио-электроники, 2008, № 2 (18), с.98-100.
2. Андрианов Г.А., Самуйлов К.Е., Гайдамака Ю.В. Анализ модели трафика ОКС-7 по результатам обработки статистики измерений // Журнал «Вестник связи» , 2007, №11, с. 17-23.
3. Булахов П.Г., Методы обнаружения компьютерных вирусов и сетевых червей / Научная сессия ТУСУР. Томск : В-Спектр, 2008, с. 39-41.
4. Миков А., Замятина Е., Панов М. Мультиагентная система защиты распределенной имитационной модели с удаленным доступом / 7th International Conference on Information Research and Applications –i.Tech, 2009, с. 199-204.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ИКТ ОБРАЗОВАНИЯ В РАЗВИТЫХ СТРАНАХ МИРА

Агаев Ф.Т., Мамедова Г.А.

Институт Информационных Технологий Национальной Академии Наук

В настоящее время область информационных технологий стала обширным полем практической деятельности людей, характеризующейся постоянно расширяющейся сферой применений и, все возрастающим спросом на высокопрофессиональное кадровое обеспечение. Долгосрочные прогнозы экспертов подтверждают тенденцию роста