AZƏRBAYCAN MİLLİ ELMLƏR AKADEMİYASI
İDARƏETMƏ SİSTEMLƏRİ İNSTİTUTU

Əlyazması hüququnda

VASİF İLKAN OĞLU HƏSƏNOV

AÇIQ KORPORATİV ŞƏBƏKƏ MÜHİTİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİ TƏMİN EDƏN İNTELLEKTUAL İNTEQRASİYA SİSTEMLƏRİNİN QURULMASI

3338.01 – «Sistemli analiz, idarəetmə və informasiyanın işlənməsi»

Texnika üzrə fəlsəfə doktoru elmi dərəcəsi almaq üçün təqdim edilmiş dissertasiyanın

A V T O R E F E R A T I

BAKI - 2018

Dissertasiya işi Azərbaycan Milli Elmlər Akademiyası
İdarəetmə Sistemləri İnstitutunda yerinə yetirilmişdir.

Elmi rəhbər:
texnika elmləri doktoru, professor **R.R.Rzayev**

Rəsmi opponentlər:
texnika elmləri doktoru, professor **Ə.Ə.Əliyev**

texnika elmləri doktoru, professor **V.Ə.Qasımov**

Aparıcı təşkilat: Azərbaycan Texniki Universitetinin "Kompüter sistemləri və şəbəkələri" kafedrası

Dissertasiyanın müdafiəsi "28" sentyabr 2018-ci ildə saat 14:00-da Azərbaycan Milli Elmlər Akademiyasının İdarəetmə Sistemləri İnstitutunun nəzdindəki **D 01.121** Dissertasiya Şurasının iclasında keçiriləcəkdir.

Ünvan: AZ1000, Bakı, B.Vahabzadə küç., 9

Dissertasiya işi ilə Azərbaycan Milli Elmlər Akademiyasının İdarəetmə Sistemləri İnstitutunun kitabxanasında tanış olmaq olar.

Avtoreferat "___" _____ 2018-ci il tarixdə paylanmışdır.

D 01.121 Dissertasiya Şurasının
elmi katibi, r.ü.f.d., dos. **Ə.B.Paşayev**

İŞİN ÜMUMİ XARAKTERİSTİKASI

Mövzunun aktuallığı. Dünyada və ölkəmizdə məlumat və ünsiyyət tenologiyalarında meydana gələn yeniliklərlə birlikdə maliyyə, səhiyyə, təhsil, əhali, iqtisadiyyat, nəqliyyat, xəbərləşmə, enerji, hərbi, mətbuat və s. kimi sahələrdə bir çox xidmətlərin İnternet mühitinə daşınması nəticəsində informasiya təhlükəsizliyi anlayışı günümüzün ən önəmli mövzularından biri halına gəlmişdir. Günümüzdə yeni texnologiyaların kəşf edildiyi, hər gün yeni kompüterlərin daxil olduğu kiber fəzada, bir yandan milli və beynəlxalq tənzimləmələrdəki əksikliklər, digər tərəfdən təhdidlərə bağlı fərqindəliyin yetərsizliyi və əsasən bu mühitdə istifadə olunan bir çox tətbiqin dizayn mərhələlərində təhlükəsizlik ölçüsünün düşünülməmiş olması, təhlükələrin təsir sahəsini genişləndirmişdir. Vəziyyət belə olduğu halda kiber təhlükələr iqtisadi, siyasi, hərbi və ictimai motivasiyalarla gündəmdəki yerini qorumağa davam edir. Bunları nəzərə alaraq, informasiya təhlükəsizliyini təmin etmək məqsədi ilə intelektual inteqrasiya sistemlərinin qurulması çox aktual məsələdir.

Müasir dövrdə informasiyanın emalı vasitələrinin evolusiyası öz-özünü təşkil edə bilən elementləri daxil edən informasiya texnologiyaları (İT) sistemlərinin yaradılması istiqamətində baş verir. Belə elementlərin nəzdində olan yaranma, uyğunlaşdırma və inkişaf prosesləri evolyusiya təcrübəsi və sellektiv seçmə ilə fərqlənən bioloji sistemlərin əsasını təşkil edir. Biosistemlərin arxitektura prinsiplərinin mənimsənilməsi süni intellektual sistemlərin əsasını təşkil edən neyron şəbəkələr və qeyri-səlis çoxluqlar nəzəriyyələrinin, evolyusiya üsullarının yaradılmasına gətirib çıxarmışdır.

Məlum olduğu kimi, biosistemlər informasiya bolluğunun, mühafizəsinin və immunitetinin mexanizmlər kompleksinin istifadəsilə realizə olunan çoxlaylı iyerarxiq həyat qabiliyyəti sisteminə malikdir. Müasir İT sistemlər öz informasiya təhlükəsizliyinin təminat mexanizmləri imkanlarına görə bioloji prototiplərindən hələlik olduqca uzaqdır. Məhz buna görə biosistemlərə analoji olan yaşama qabiliyyəti funksiyasını özünə cəlb edən intellektual inteqrasiya sistemlərinin qurulması aktual məsələdir.

Beləliklə, mövcud dissertasiyada neyron şəbəkələrin və qeyri-səlis məntiqin intellektual alətlərinin istifadəsilə biosistemli analogiya əsasında realizə olunan adaptiv informasiya mühafizəsinin modelləşdirilməsinə dair bir yanaşma tədqiq olunur.

Dissertasiya işinin məqsədi. İnformasiya baxımından təhlükəsiz İT sistemlər üçün ekspert qiymətləndirmələrin adaptiv toplularını (matrisləri) istifadə edən, neyroşəbəkəli modellərə və hesablamalara yönəldilmiş, İT sistemin həyat dövrlərində təhlükələrin dəyişməsini nəzərə alan adaptiv informasiya təhlükəsizliyi sisteminin (İTS) işlənməsidir.

Tədqiqatın obyekti. Korporativ şəbəkələrdə informasiya mühafizəsi sistemləri və informasiya mühafizəsi vasitələri.

Tədqiqatın predmeti. Korporativ şəbəkələrdə informasiya təhlükəsizliyini təmin edən intelektual inteqrasiya sistemlərinin qurulması üçün qeyri-səlis məntiqin tətbiqi.

Tədqiqatın metodları. Dissertasiya işində tədqiqatın əsas metodları aşağıdakılardan ibarətdir:

Nəzəri metodlar qrupu: problemli-müqayisəli təhlil; milli və autentik xarici mənbələrin öyrənilməsi əsasında sistemləşdirmə və təsnifləşdirmə metodu; qeyri-səlis metodlar və vasitələr, o cümlədən qeyri-səlis riyazi elementlər və qeyri-səlis nəticə mexanizmi; ümumiləşdirmə və sintez; neyro-fuzzy təsnifat üsulları; universitetlərdə, müəssisə və təşkilatlarda mövcud intelektual vasitələr və informasiya mühafizəsi sistemlərinin modelləşməsinin təhlili; korporativ müəssisələrdə informasiyanın mühafizə sisteminin adaptiv modelinin təhlili; informasiya təhlükəsizliyinin hərtərəfli qiymətləndirilməsinin təhlili; şəbəkə trafiki ilə idarəetmə modelinin təhlili.

Empirik metodlar qrupu: Elektron idarəetmə sistemi mövcud olan korporativ müəssisələrdə, o cümlədən universitetlərdə informasiya təhlükəsizliyinin mövcud vəziyyəti ilə bağlı sorğu, söhbət, müsahibələrin aparılması, informasiya təhlükəsizliyinin təmin edilməsi məqsədi ilə görülmüş işlərin müşahidə edilməsi. Empirik məlumatların işlənməsi məqsədi ilə informasiya təhlükəsizliyinin hərtərəfli qiymətləndərilməsi və analizi üçün qeyri-səlis məntiq metodlarından istifadə edilmişdir: kompüter texnikası və İKT vasitələrindən istifadə dərəcəsinin səviyyəsi üzrə; emalın intensivliyi üzrə; məxfilik dərəcəsi üzrə; emal olunmuş məlumatların həcmi üzrə.

Tədqiqatın bazası. Azərbaycanda yerləşən elektron idarəetmə sisteminə malik olan bütün müəssisə və təşkilatlar və eyni zamanda təlim tədris prosesi ilə yanaşı bütün idarəetmə məsələlərini elektron mühitə keçirən universitetlər.

İşin elmi yenilikləri:

1. Korporativ İT şəbəkələrin informasiya mühafizə sistemlərinə biosistemlərə xas olan evolyusiya xüsusiyyətlərini və ilk növbədə inkişaf

və adaptivlik imkanlarının mənimsədilməsinin zəruriliyi müəyyən edilmişdir.

2. Adaptiv informasiya mühafizə sisteminin bioliji oxşarlıq prinsipinə əsaslanan iyerarxiq modeli və korporativ İT şəbəkəsinin mühafizə olunmasının qiymətləndirilməsi metodikasını daxil etməklə layihələndirilməsinin qeyri-səlis üsulları təklif edilmişdir.

3. Korporativ İT şəbəkələrin informasiya təhlükəsizliyinə təsir göstərən faktorların böyük bir qismini əhatə edən koqnitiv xəritə modeli işlənib hazırlanmışdır.

4. Korporativ İT şəbəkələrdə informasiya təhlükəsizliyi səviyyəsini qiymətləndirmək məqsədilə tipik qeyri-səlis koqnitiv model işlənilmiş və təsvir edilmişdir.

5. Qeyri-səlis qaydalarla idarə olunan koqnitiv xəritənin modelinin və dinamiki sıraların verilənlərinin qeyri-səlis təhlilinə əsaslanan şəbəkə trafikinin həcminin proqnozlaşdırma modelinin sintezi əsasında şəbəkə trafiki ilə effektiv idarəetmə modeli işlənilmişdir.

6. Şəbəkə trafiklərində IP-paketlərin həcmlərinin dəyişməsinin qeyri-səlis təhlilinə və orada volatilliyin mövcudluğuna əsaslanaraq şəbəkə trafiklərinin həcmlərinin dəyişməsinin proqnozlaşdırılması məsələsi həll olunmuşdur. Nəticədə şəbəkə trafikində mümkün ola bilən anomaliyaların aşkar edilməsi üçün yeni yanaşma təklif edilmişdir.

Müdafiəyə çıxarılan əsas məsələlər:

- Bioloji sistemlərin mühafizə mexanizmlərinə analoji olaraq informasiya mühafizəsinin neuro-fuzzy vasitələrin əsasında İT sistemlərin adaptiv informasiya mühafizəsinin medellərinin işlənməsi;
- Adaptiv informasiya mühafizəsi sisteminin iqtisadi və struktur göstəricilərini nəzərə alaraq İT sisteminin informasiya təhlükəsizliyinin qiymətləndirmə sisteminin işlənməsi;
- Təklif olunan qiymətləndirmələr və adaptiv İTS modeli əsasında adaptiv informasiya mühafizəsi sisteminin qurulmasına dair yeni metodikanın işlənməsi;
- NŞ təsvirinin detallaşdırmasını nəzərə alaraq informasiya cəhətdən mühafizə olunan qərargah bölməsinin arxitektura həllərinin işlənməsi;
- Adaptiv İTS qurulması metodikasının dəstəyi üçün instrumental vasitələrin işlənməsi.

İşin praktiki əhəmiyyəti. Dissertasiya işində alınmış elmi-nəzəri və praktiki nəticələrin e-dövlət çərçivəsində böyük informasiya axınının mühafizəsinin təmin olunmasında, müəssisələrin özlərinə məxsus olan

korporativ şəbəkələrində məlumatların qorunmasında, universitetlərin e-universitet layihəsi çərçivəsində öz informasiyalarını mühafizə edən zaman geniş tətbiqinin mümkünlüyü ilə müəyyən olunur.

Dissertasiya işinin nəticələrinin realizasiyası və onun tətbiqi. Gəncə Dövlət Universitetində təsərrüfat və dövlət büdcəli elmi işlər yerinə yetirilən zaman aparılan nəzəri tədqiqatların əsas göstəricilərindən və praktiki nəticələrdən istifadə edilmişdir. Dissertasiya işi aşağıdakı sahələrdə öz tətbiqini tapmışdır:

- Gəncə Dövlət Universitetinin "İnformatika" kafedrasının tədris proseslərində.

Şəxsi töhvələri. Dissertasiyada bütün elmi məsələlərin nəticələri və tövsiyələri şəxsən dissertant tərəfindən işlənib hazırlanmış, əsas elmi nəticələrin tətbiqi müəllifin iştirakı ilə olmuşdur.

Dissertasiya işinin aprobasiyası. Dissertasiya işinin əsas nəticələri Respublika və Beynəlxalq konfranslarda, seminarlarda, simpoziumlarda məruzə və müzakirə olunmuşdur, o cümlədən:

1. Fırat Universiteti (Türkiyə), Gazi Universiteti (Türkiyə), Sam Houston Dövlət Universiteti (ABŞ), Polis Akademiyası (Türkiyə) və TUBİTAK (Türkiyə) birgə təşkil etdiyi "1st İnternational Symposium on digital forensics and security" mövzusunda keçirilmiş beynəlxalq konfransda (Elazığ/Türkiyə, 20-21 may 2013)
2. Gəncə Dövlət Universitetində Milli Qurtuluş Gününə həsr edilmiş "Riyaziyyat və İKT-nin tətbiq sahələri. Yeni tədris texnologiyaları" mövzusunda keçirilmiş Beynəlxalq konfransda (Gəncə, 05-06 iyun 2014)
3. Gəncə Dövlət Universitetində keçirilmiş "Gənc alimlərin I beynəlxalq elmi konfransı" mövzusunda keçirilmiş Beynəlxalq konfransda (Gəncə, 17-18 oktyabr 2016)
4. "9th International Conference on Theory and Application of Soft Computing, Computing with Words and Perception, ICSCCW 2017" mövzusunda keçirilmiş beynəlxalq konfransda (24-25 August 2017, Budapest, Hungary)
5. "Автоматизация и приборостроение: проблемы, решения." mövzusunda keçirilmiş beynəlxalq konfransda (11-15 сентября 2017 года, г. Севастополь, Россия)

Nəşrlər. Tədqiqatlar və elmi işlərin nəticələri üzrə 17 elmi məqalə dərc edilmişdir. Onlardan 7-si AAK-ın tövsiyə etdiyi nəşrlərə aiddir.

İşin həcmi və strukturu. Dissertasiya işi girişdən, 4 fəsildən, nəticədən, 106 adda istifadə edilmiş ədəbiyyat siyahısından ibarətdir. İşin əsas məzmunu 128 səhifə, 26 şəkil və 21 cədvəldən ibarətdir.

İŞİN QISA MƏZMUNU

Girişdə müəllif tərəfindən müdafiəyə çıxarılan müddəalarda aparılan tədqiqatın aktuallığı, işin əsas məqsədi və qarşıya qoyulan əsas məsələlərin həll yolları göstərilmişdir. Eyni zamanda qoyulan məsələnin elmi yenilikləri, praktiki dəyəri, nəşrlər haqqında məlumatlar və dissertasiyanın strukturu göstərilmişdir.

Dissertasiya işinin I bölməsində korporativ şəbəkələr: əsas anlayışlara, xususiyyətlərə və mövcud topologiyalara baxılır. Korporativ şəbəkələrin təhlili aparılmışdır. Sonra korporativ şəbəkələrin xüsusiyyətlərinə və korporativ şəbəkələrdə mövcud olan topologiyalar araşdırılmışdır.

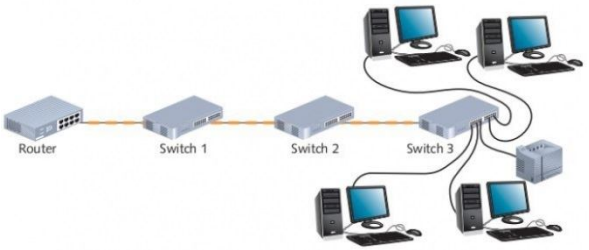
Korporativ şəbəkənin ən mühüm xüsusiyyətləri araşdırılmışdır. Belə ki,

- *geniş miqyaslı olması*;
- *qeyri-bircinsliyi*;
- *qlobal əlaqənin istifadə olunması*;
- *interqrasiyalığı*;
- *etibarlığa yüksək tələb*;
- *şəbəkənin idarə olunmasına yüksək tələb*;
- *həll olunan məsələlərin universal xarakterli olması*;
- *əhatə olunan texniki problemlərin genişliyi*.

Bu fəsildə daha böyük şəbəkələr (korporativ şəbəkələr) təşkil etməyin bəzi məşhur metodları təsvir edilmişdir. Bunlar:

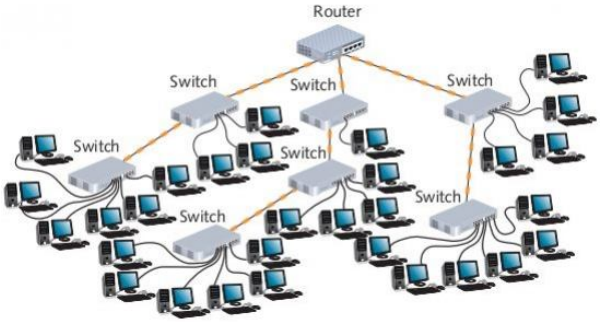
Onurğa şəbəkələri (Backbone networks).

Ardıcıl onurğa (serial backbone).

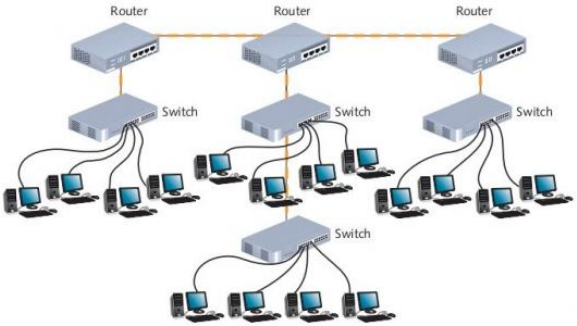


Şəkil 1.1. Ardıcıl onurğa topologiyası

Yayılan onurğa (distributed backbone).

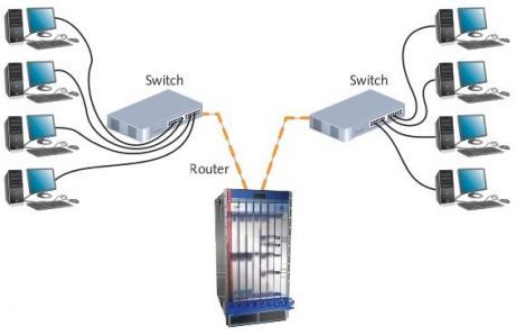


Şəkil 1.2. Sadə yayılan onurğa (distributed backbone)



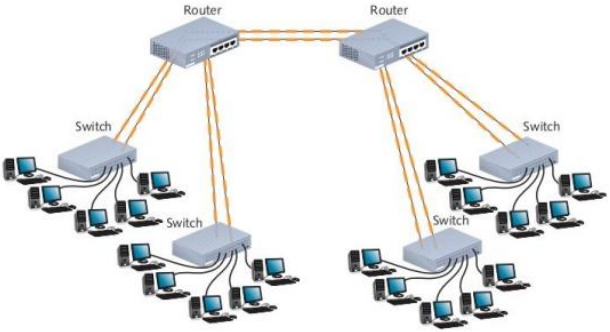
Şəkil 1.3. Çoxsaylı LAN-ları birləşdirən yayılan onurğa (distributed backbone)

Dağıdılmış onurğa (Collapsed backbone).



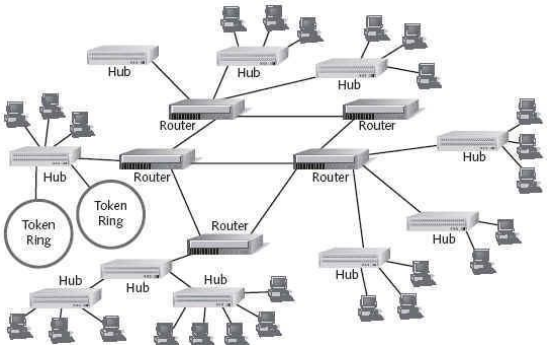
Şəkil 1.4. Dağıdılmış onurğa

Paralel onurğa (Parallel backbone).



Şəkil 1.5. Paralel onurğa

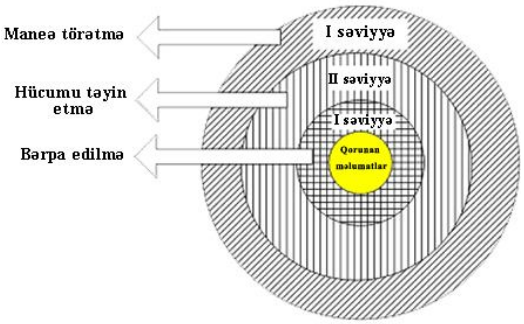
Tor şəbəkələri (Mesh networks).



Şəkil 1.6. Tor şəbəkələri

Dissertasiya işinin II bölməsində korporativ şəbəkələrin təhlükəsizliyini təmin edən üsullar və vasitələr araşdırılmışdır. Araşdırma zamanı korporativ şəbəkələrin təhlükəsizliyinə dair ilkin anlayışlar müəyyən edilmişdir.

Çox laylı təhlükəsizlik sistemlərindən söz edilmişdir. Lay quruluşunu qurulacaq təhlükəsizlik sistemlərinin xüsusiyyətinə görə fərqliləşdirmək və hər layda alt laylar istifadə etmək mümkündür. Ümumiyyətlə üç laydan ibarət olan bir quruluşdan söz etmək mümkündür. Bu ümumi model aşağıdakı şək. 2.2-də göstərilmişdir. Laylar aşağıdakı kimidir:



Şəbəkə təhlükəsizliyinin təmin edilməsi üçün lazımlı olan əsas siyasətlər sıralanmışdır:

1. Qəbul edilə bilər istifadə (acceptable use) siyasəti,
2. Müraciət siyasəti.
3. Şəbəkə təhlükəsizlik divarı (firewall) siyasəti. Təhlükəsizlik divarı sadlanan xidmətlərlə birlikdə işləyərək şəbəkə təhlükəsizliyini təmin edir: Proxy, Anti-Virus həlləri, Məzmun Süzmə (content filtering), Xüsusi Virtual Şəbəkələr (Virtual Private Network-VPN), Kimlik Təyinetmə Sistemləri (Intrusion Detection Systems-IDS),
4. İnternet siyasəti. Təşkilat daxilində hər bir istifadəçinin xarici qaynaqlara, yəni İnternetə qoşulmasına ehtiyac yoxdur. İnternetə qoşulmanın yol açа biləcəyi problemlər bunlardır: Zərərli kodlar, Təsirli Kodlar, Məqsəddən kənar istifadə, Zaman itkisi.
5. Şifrə rəhbərliyi siyasəti. Təşkilatlar təhlükəsizlik siyasətlərində şifrə seçkisi ilə əlaqədar sadalanan məhdudiyyətləri təyin edə bilərlər: Şifrənin ölçüsü və məzmunu, Müddət dolması (köhnəlmə) siyasəti, Tək qeyd ilə hər yerə müraciət (Single Sign on-SSO) siyasəti.
6. Fiziki təhlükəsizlik siyasəti.
7. İctimai mühəndislik siyasəti.

Cihazlarda alına biləcək ilkin tədbirlər müəyyən edilmişdir: Bunlar: Təhlükəsizlik əlavələrinin davamlı olaraq tətbiq olunması, Əlavə rəhbərliyi, Antivirus, İnternet skaneri seçimi, Fərdi Təhlükəsizlik Divarı.

Şəbəkədə alına biləcək tədbirlər aşağıdakı Cədvəl 2.1-də göstərilmişdir. Cihazların OSI modelinin hansı səviyyəsində iş qabiliyyətinə sahib olduğuna görə L2 və L3 cihazlar olaraq təyin olunmuşdur.

Cədvəl 2.1

Şəbəkədə alına biləcək tədbirlərin təsnifatı

Şəbəkədə alına biləcək ilkin tədbirlər	Birinci Lay	İkinci Lay	Üçüncü Lay
	Yoluxmasına manea törətmə	Yoluxmuş sistemi təyin etmə	Qurtarma və təsirləri azaltma
L2 Cihazları ilə alına biləcək tədbirlər			
MAC ünvanı əsasında təhlükəsizlik		x	x
802.1x əsaslı kimlik təsdiqləmə	x	x	
Broadcast/Multicast məhdudlaşdırması		x	x
L3 Cihazları ilə alına biləcək tədbirlər			
VLAN əsaslı təhlükəsizlik tədbirləri	x		x
Müraciət siyahıları ilə alınabiləcək tədbirlər	x	x	x
QoS ilə diapazon genişlik məhdudlaşdırma			x
Yeni nəsil təhlükəsizlik tədbirləri		x	x
Təhlükəsizlik Cihazları ilə alına biləcək tədbirlər			
Firewall (təhlükəsizlik divarı)	x	x	x
Antivirus keçidləri	x	x	x
IDS/IPS sistemləri	x	x	x
Digər Sistemlər ilə alına biləcək tədbirlər			
Saldırğan tələsi şəbəkəsi (Honeynet)		x	
Mərkəzi LOG idarəsi		x	
Trafik analizi		x	
DNS server			x
Arp hücumlarını təyin edəbilən tətbiqlər		x	

Şəbəkədə alına biləcək tədbirlər dörd əsas başlıqda təsnif edilmişdir:

- L2 Cihazları ilə alına biləcək tədbirlər;
- L3 Cihazları ilə alına biləcək tədbirlər;
- Təhlükəsizlik Cihazları ilə alına biləcək tədbirlər;
- Digər Sistemlər ilə alına biləcək tədbirlər.

OSI modelinin ikinci layında işləyən yerli şəbəkə cihazlarında alına biləcək tədbirlər: MAC ünvanı əsasında təhlükəsizlik, 802.1x əsaslı kimlik təsdiqləmə, Broadcast/Multicast məhdudlaşdırması araşdırılmışdır.

OSI modelinin 3-cü layında işləyən cihazlarda alına biləcək tədbirlər: WLAN əsaslı təhlükəsizlik tədbirləri, Müraciət siyahıları ilə alınabiləcək

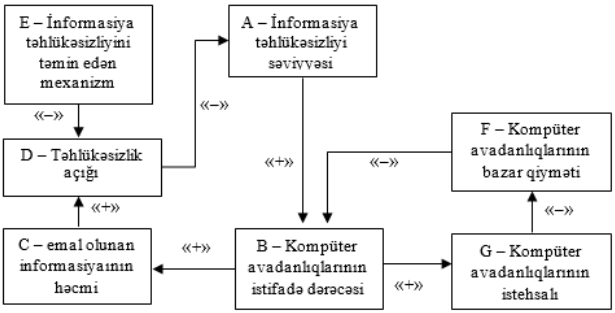
tədbirlər, QoS ilə diapazon genişliyi məhdudlaşdırması, Yeni nəsil təhlükəsizlik tədbirləri araşdırılmışdır.

Şəbəkə üzərində təhlükəsizlik məqsədli qurulacaq sistemlərlə alına biləcək tədbirlər: Təhlükəsizlik Divarları (Firewall), Antivirus keçidləri, IDS/IPS Sistemləri araşdırılmışdır.

Daha sonra isə digər sistemlərlə alına biləcək tədbirlər: Saldırğan tələsi şəbəkəsi (Honeynet), Mərkəzi LOG idarəsi, Trafik hərəkət analizi serverləri, DNS Server, Arp hücumlarını təyin edəbilən tətbiqlər araşdırılmışdır.

Dissertasiya işinin III bölməsində informasiyanın təhlükəsizliyinin hərtərəfli qiymətləndirilməsi üçün qeyri-səlis koqnitiv model işlənib hazırlanmışdır. Zəif strukturlaşdırılmış sistemlərin qeyri-səlis koqnitiv modelinin ümumi prinsipləri verilmişdir.

İnformasiya təhlükəsizliyi probleminin analizi üçün koqnitiv xəritə işlənmişdir.



İnformasiya təhlükəsizliyinin qiymətləndirilməsi üçün tipik qeyri-səlis koqnitiv model hazırlamaq üçün informasiya təhlükəsizliyi səviyyəsinə təsir edən amillər cədvəl şəklində təqdim edilmişdir. Bu amillər əsas götürülərək informasiya təhlükəsizliyinin analizi üçün qeyri-səlis koqnitiv xəritə hazırlanmışdır.

Qeyri-səlis koqnitiv xəritə əsasında kompüter texnikası və İKT vasitələrindən istifadə dərəcəsinin səviyyəsi müəyyən edilmişdir. Bəzi əvəzləmələr və linqvistik dəyişənlərin giriş şərtlərini nəzərə alaraq qeyri-səlis implikativ (dolayı) qaydalar əldə edilmişdir:

a_1: «Əgər B_1=BÖYÜK DEYILSƏ və B_7=ISTIFADƏ EDILMIRSƏ və B_8=ISTIFADƏ EDILMIRSƏ, onda B=TS»;

a_2: «Əgər B_1=BÖYÜK DEYILSƏ və B_5=ISTIFADƏ EDILIRSƏ və B_6=ISTIFADƏ EDILIRSƏ və B_7=ISTIFADƏ EDILMIRSƏ və B_8=ISTIFADƏ EDILMIRSƏ, onda B=*VS*»;

a_3: «Əgər B_1=BÖYÜK DEYILSƏ və B_7=ISTIFADƏ EDILIRSƏ və B_8=ISTIFADƏ EDILIRSƏ və B_9=ISTIFADƏ EDILIRSƏ və B_{10}=MÖVCUDDURSA və B_{13}=MƏQBULDURSA, onda B=*MS*»;

a_4: «Əgər B_7=ISTIFADƏ EDILIRSƏ və B_8=ISTIFADƏ EDILIRSƏ və B_9=ISTIFADƏ EDILIRSƏ və B_{10}=MÖVCUDDURSA və B_{13}=MƏQBULDURSA, onda B=*S*»;

a_5: «Əgər B_6=ISTIFADƏ EDILIRSƏ və B_7=ISTIFADƏ EDILIRSƏ və B_8=ISTIFADƏ EDILIRSƏ və B_9=ISTIFADƏ EDILIRSƏ və B_{10}=MÖVCUDDURSA və B_{11}=ƏSASDIRSA və B_{12}=ƏHƏMIYYƏTLIDIRSƏ və B_{13}=MƏQBULDURSA, onda B=*L*»;

a_6: «Əgər B_5=ISTIFADƏ EDILIRSƏ və B_6=ISTIFADƏ EDILIRSƏ və B_7=ISTIFADƏ EDILIRSƏ və B_8=ISTIFADƏ EDILIRSƏ və B_9=ISTIFADƏ EDILIRSƏ və B_{10}=MÖVCUDDURSA və B_{11}=ƏSASDIRSA və B_{12}=ƏHƏMIYYƏTLIDIRSƏ və B_{13}=MƏQBULDURSA, onda B=*ML*»;

a_7: «Əgər B_3=TAMDIRSA və B_4=ISTIFADƏ EDILIRSƏ və B_5=ISTIFADƏ EDILIRSƏ və B_6=ISTIFADƏ EDILIRSƏ və B_7=ISTIFADƏ EDILIRSƏ və B_8=ISTIFADƏ EDILIRSƏ və B_9=ISTIFADƏ EDILIRSƏ və B_{10}=MÖVCUDDURSA və B_{11}=ƏSASDIRSA və B_{12}=ƏHƏMIYYƏTLIDIRSƏ və B_{13}=MƏQBULDURSA, onda B=*VL*»;

a_8: «Əgər B_1=BÖYÜKDÜRSƏ və B_4=BÖYÜKDÜRSƏ və B_3=TAMDIRSA və B_4=ISTIFADƏ EDILIRSƏ və B_5=ISTIFADƏ EDILIRSƏ və B_6=ISTIFADƏ EDILIRSƏ və B_7=ISTIFADƏ EDILIRSƏ və B_8=ISTIFADƏ EDILIRSƏ və B_9=ISTIFADƏ EDILIRSƏ və B_{10}=MÖVCUDDURSA və B_{11}=ƏSASDIRSA və B_{12}=ƏHƏMIYYƏTLIDIRSƏ və B_{13}=MƏQBULDURSA, onda B=*TL*».

Qeyri-səlis koqnitiv xəritə əsasında emalın intensivliyi müəyyən edilmişdir. Bəzi əvəzləmələr və linqvistik dəyişənlərin giriş şərtlərini nəzərə alaraq qeyri-səlis implikativ (dolayı) qaydalar əldə edilmişdir:

b_1: «Əgər B=BÖYÜKDÜRSƏ, onda C=YÜKSƏKDIR»;

b_2: «Əgər B=BÖYÜKDÜRSƏ və C_1=UYĞUNDURSA, onda C=BIRAZ YÜKSƏKDIR»;

b_3: «Əgər B=BÖYÜKDÜRSƏ və C_1=UYĞUNDURSA və C_2=KOMPAKTDIRSA, onda C=ÇOX YÜKSƏKDIR»;

b_4: «Əgər B=BÖYÜKDÜRSƏ və C_1=UYĞUNDURSA və C_2=KOMPAKTDIRSA və C_3=YAXŞIDIRSA, onda C=HƏDSIZ YÜKSƏKDIR»;

b_5: «Əgər B=BÖYÜK DEYILSƏ və C_1=UYĞUNDURSA və C_2=KOMPAKTDIRSA və C_3=YAXŞIDIRSA, onda C=YÜKSƏKDIR»;

b_6: «Əgər B=BÖYÜK DEYILSƏ və C_3=PISDIRSƏ, onda C=YÜKSƏK DEYIL».

Qeyri-səlis koqnitiv xəritə əsasında məxfilik dərəcəsi müəyyən edilmişdir. Bəzi əvəzləmələr və linqvistik dəyişənlərin giriş şərtlərini nəzərə alaraq qeyri-səlis implikativ (dolayı) qaydalar əldə edilmişdir:

c_1: «Əgər D_1=YÜKSƏKDIRSƏ və D_2=YAXŞIDIRSA, onda D=YÜKSƏK olar»;

c_2: «Əgər D_1=YÜKSƏKDIRSƏ və D_2=YAXŞIDIRSA və D_3=TAMDIRSA, onda D=BIRAZ YÜKSƏK olar»;

c_3: «Əgər B=BÖYÜK DEYILSƏ və D_1=YÜKSƏKDIRSƏ və D_2=YAXŞIDIRSA və D_3=TAMDIRSA, onda D=ÇOX YÜKSƏK olar»;

c_4: «Əgər B=BÖYÜK DEYILSƏ və D_1=YÜKSƏKDIRSƏ və D_2=YAXŞIDIRSA və D_3=TAMDIRSA və D_4=YÜKSƏKDIRSƏ, onda D=HƏDSIZ YÜKSƏK olar»;

c_5: «Əgər B=BÖYÜKDÜRSƏ və D_1=YÜKSƏKDIRSƏ və D_2=YAXŞIDIRSA və D_4=YÜKSƏKDIRSƏ, onda D=YÜKSƏK olar»;

c_6: «Əgər B=BÖYÜKDÜRSƏ və D_2=PISDIRSƏ və D_4=ALÇAQDIRSA, onda D=YÜKSƏK DEYIL».

Qeyri-səlis koqnitiv xəritə əsasında emal olunmuş məlumatların həcmi müəyyən edilmişdir. Bəzi əvəzləmələr və linqvistik dəyişənlərin giriş şərtlərini nəzərə alaraq qeyri-səlis implikativ (dolayı) qaydalar əldə edilmişdir:

d_1: «Əgər B=BÖYÜKDÜRSƏ və E_2=TAMDIRSA, onda E=YÜKSƏK olar»;

d_2: «Əgər B=BÖYÜKDÜRSƏ və E_2=TAMDIRSA və E_4=TAMDIRSA, onda E=BIRAZ YÜKSƏK olar»;

d_3: «Əgər B=BÖYÜKDÜRSƏ və E_2=TAMDIRSA və E_3=DAVAMLIDIRSA və E_4=TAMDIRSA, onda E=ÇOX YÜKSƏK olar»;

d_4: «Əgər B=BÖYÜKDÜRSƏ və E_1=BÖYÜKDÜRSƏ və E_2=TAMDIRSA və E_3=DAVAMLIDIRSA və E_4=TAMDIRSA, onda E=HƏDSIZ YÜKSƏK olar»;

d_5: «Əgər B=BÖYÜKDÜRSƏ və E_1=BÖYÜKDÜRSƏ və E_2=TAMDIRSA və E_3=IŞTIRAK ETMIRSƏ, onda E=YÜKSƏK olar»;

d_6: «Əgər B=BÖYÜKDÜRSƏ və E_2=ƏHƏMIYYƏTLI MƏHDUDDURSA, onda E=YÜKSƏK olmaz».

Beləliklə, sistemin təhlükəsizlik açığının mənbələrini qiymətləndirmək üçün standart qeyri-səlis modeli formasına nisbətən daha

asan qeyri-səlis nəticəçıxarma sisteminin qurulması üçün linqvistik dəyişənlər və qaydalar dəstini yaratmaqla sistemin təhlükəsizlik açığının səviyyəsini qiymətləndirmək mümkün olmuşdur. Asan olması üçün bütün dəyişənlər cədvəl şəklində verilmiş və simvolik formada qaydalar sistemi qeyd edilmişdir. Nəticədə aşağıdakı qaydalar əldə edilmişdir:

Əgər x_1=YÜKSƏK OLMAYAN və x_2=HƏDSIZ YÜKSƏK və x_3=YÜKSƏK OLMAYAN, onda y=ALÇAQ olar;

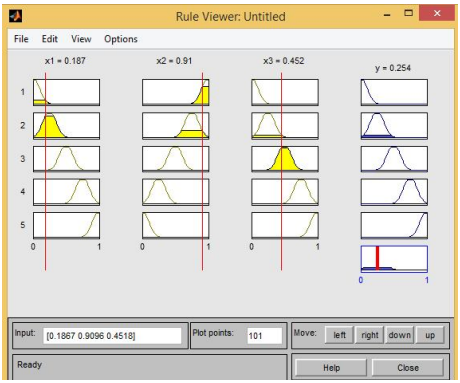
Əgər x_1=YÜKSƏK və x_2=ÇOX YÜKSƏK və x_3=YÜKSƏK, onda y=ENDIRIMLI olar;

Əgər x_1=BIRAZ YÜKSƏK və x_2=BIRAZ YÜKSƏK və x_3=BIRAZ YÜKSƏK, onda y=ORTA olar;

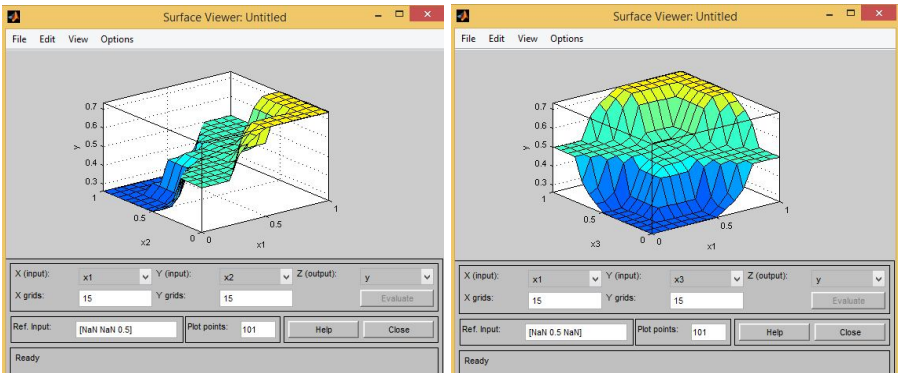
Əgər x_1=ÇOX YÜKSƏK və x_2=YÜKSƏK və x_3=ÇOX YÜKSƏK, onda y=ARTIMLI olar;

Əgər x_1=HƏDSIZ YÜKSƏK və x_2=YÜKSƏK OLMAYAN və x_3=HƏDSIZ YÜKSƏK, onda y=YÜKSƏK olar.

Bu qaydalar asanlıqla MATLAB proqramında göstərilə bilər, misal olaraq “hiperboloid” (kilisə zəngi) mənsubiyyət funksiyasının linqvistik dəyişənlərinin giriş və çıxış şərtlərini təsvir etmək üçün istifadə edilmiş və MATLAB proqramında sistemin təhlükəsizlik açıqları üçün uyğulama qaydaları verilmişdir.

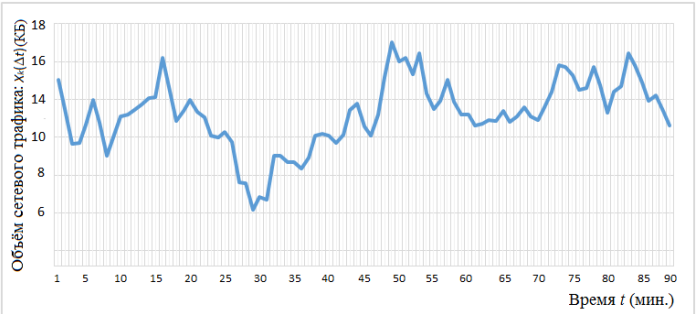


Daha sonra MATLAB proqramından istifadə etməklə amillərin təsiri ilə sistemin təhlükəsizlik açığının asıllıq dərəcəsi verilmişdir.



Dissertasiya işinin IV bölməsində qeyri-səlis qaydalara əsaslanan koqnitiv xəritə modeli əsasında şəbəkə trafiki ilə idarəetmə məsələsi işlənmişdir. İlk növbədə şəbəkə trafiki ilə idarəetmə modelinin strukturu verilmiş və şəbəkə trafiki ilə idarəetmə sisteminin modelləşdirilməsi prosesi göstərilmiş və şəkillərlə təsvir edilmişdir.

IP paketlərin həcminin dəyişməsinin qeyri-səlis təhlili əsasında şəbəkə trafiki proqnozlaşdırılmış və şəbəkə trafiki həcminin dəyişməsinin dinamik sırası verilmişdir.



Qeyri-səlis modelləşdirmə əsasında şəbəkə trafiki həcmi proqnozlaşdırılmışdır. Trafik həcminin dəyişikliklərini açıqlayan nizamlı məlumat sırası cədvəl şəklində təqdim edilmişdir.

Daha sonra $X_k(\Delta t)$ sırasının qeyri-səlis modelinin qurulması prosedurasına addım-addım baxılmışdır.

Addım 1-də Universumun müəyyən edilməsi və onun bərabər intervallara bölünməsi aparılmışdır.

Addım 2-də verilənlərin fazzifikasiyası aparılmış və $X_k(\Delta t)$ sırasının qeyri-səlis modelinin giriş xarakteristikaları cədvəl şəklində verilmişdir.

Addım 3-də daxili qeyri-səlis əlaqələrin müəyyən edilməsi və onların qruplar üzrə toplanması məsələsinə baxılmışdır. 1-ci tərtib qeyri-səlis əlaqələr, 1-ci tərtib qeyri-səlis əlaqələrin qrupları və 2-ci tərtib qeyri-səlis əlaqələrin qrupları müəyyən edilmişdir.

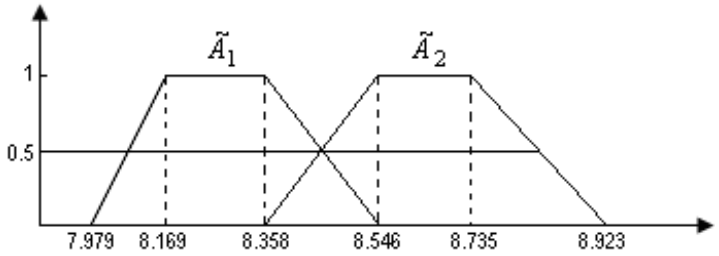
Addım 4-də isə qeyri-səlis proqnozların müəyyən edilməsi və onların defazzifikasiyası aparılmışdır. Bunun üçün dünyada daha çox istifadə edilən iki modelə baxılmışdır: S.Çen modeli; K.Sonq və B.Çissom modeli.

S.Çenin üsulu ilə şəbəkə trafikinin modelləşdirilməsinə baxılmış və müvafiq hesablamalar əsasında 1-ci və 2-ci tərtib əlaqələr üçün S.Çen modelinin defazzifikasiya olunmuş çıxışları müəyyən edilmiş və cədvəl formasında təqdim edilmişdir.

Sonra Sonq-Çissom üsulu ilə şəbəkə trafikinin modelləşdirilməsinə baxılmışdır. Uyğun hesablamalar aparıldıqdan sonra kompozisiya qaydasına əsasən şəbəkə trafikinin modelləşdirilməsi cədvəl şəklində təqdim edilmişdir.

Daha sonra isə Poulsenin alqoritmi ilə şəbəkə trafikinin modelləşdirilməsi aparılmışdır. Bu zaman bir neçə addımların yerinə yetirilməsi proseduru nəzərdə tutulmuşdur.

Addım 1-də dinamiki sıranın verilənlər diapazonu örtüyü şəklində universumun təyin edilməsi məsələsinə baxılmışdır. Addım 2-də U universumunun qeyri-səlis altçoxluqlarının qurulması məsələsinə baxılmış və trapesiodal mənsubiyyət funksiyaları qrafik şəklində təqdim edilmişdir.



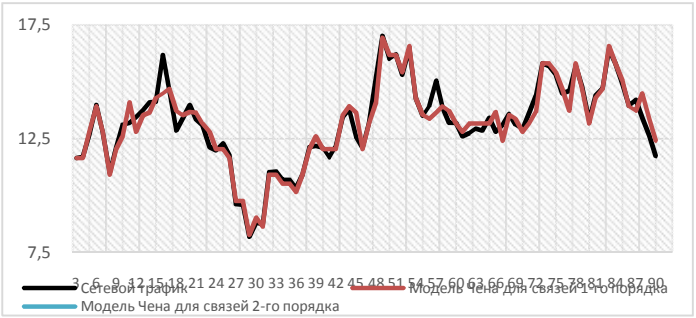
Addım 3-də şəbəkə trafikinin həcm verilənlərinin fazzifikasiyası məsələsinə baxılmış və şəbəkə trafikinin verilənlərinin fazzifikasiyasının nəticələri cədvəl şəklində təqdim edilmişdir.

Addım 4-də daxili qeyri-səlis əlaqələrin təyini və onların qruplara bölünməsi məsələsinə baxılmış, 1-ci və 2-ci tərtib qeyri-səlis əlaqələr

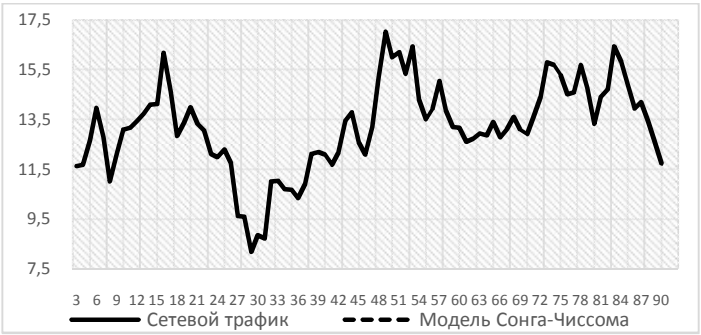
müəyyən edilmişdir. Daha sonra 1-ci və 2-ci tərtib qeyri-səlis əlaqələrin qrupları müəyyən edilmişdir.

Addım 5-də isə modelin qeyri-səlis çıxışlarının defazzifikasiyası məsələsinə baxılmış və 1-ci və 2-ci tərtib əlaqələr üçün Poulsen modelinin çıxışlarının defazzifikasiyası təyin edilmişdir.

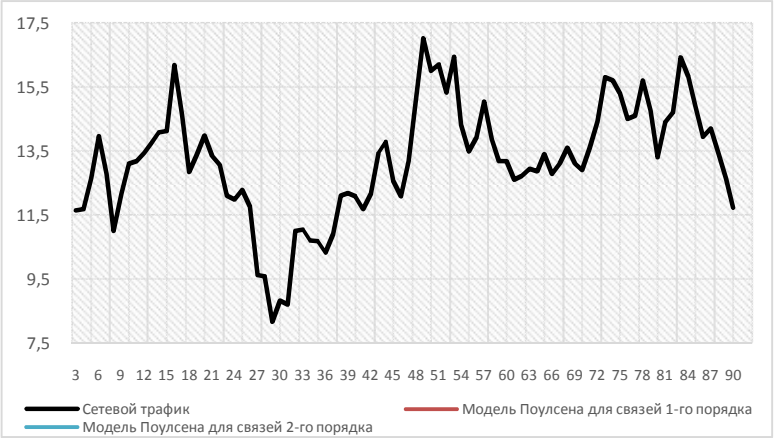
Proqnozlaşdırma nəticələrinin müqayisəsi aparılmış və əldə edilmiş nəticələr cədvəl şəklində təqdim edilmişdir. Daha sonra şəbəkə trafikinin S.Çen, Sonq-Çissom və Poulsen modeli verilmişdir.



Şəbəkə trafikinin Çen modeli

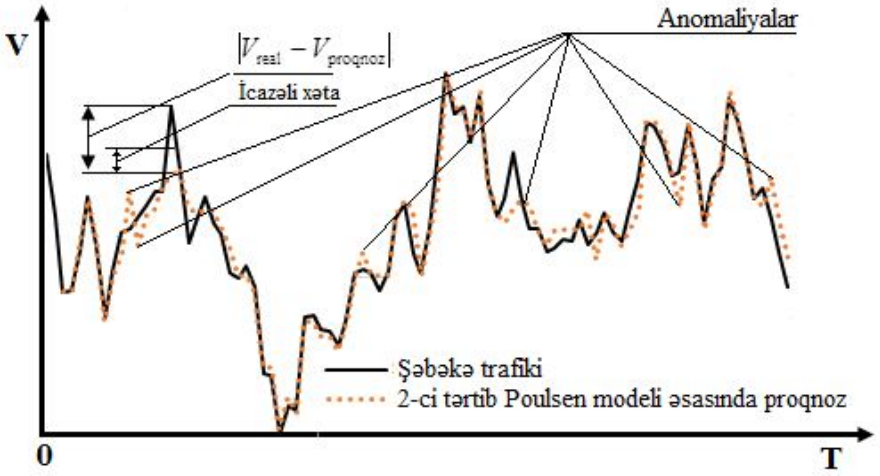


Şəbəkə trafikinin Sonq-Çissom modeli



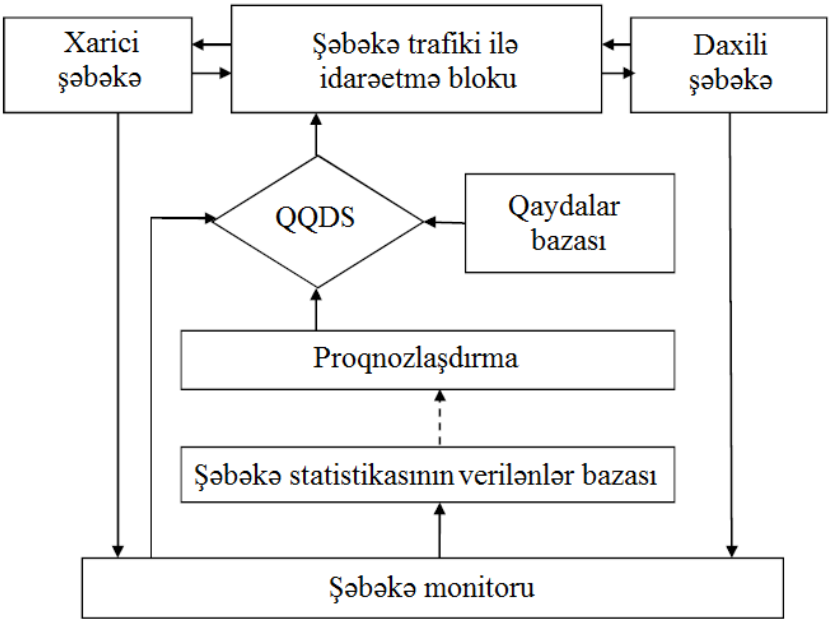
Şəbəkə trafikinin Paulsen modeli

Sonra şəbəkə trafikinin həcmində anomaliyanın axtarışı və miqdarının qiymətləndirilməsi aparılmış və niticədə şəbəkə trafikinin anomaliyalarını özündə əks etdirən qrafik əldə edilmişdir.



Daha sonra anomaliyanın aşkar edilməsinə reaksiyanın göstərilməsi müəyyən edilmişdir.

Beləliklə, şəbəkə trafiki ilə idarəetmənin ümumi sxemi təsvir edilmişdir.



İşin əsas nəticələri:

Aparılan tədqiqatların nəticələrinə görə iddiaçı tərəfindən müdafiəyə çıxarılan müddəalar aşağıdaki kimi qısaca və dürüst ifadə edilmişdir:

1. Korporativ İT şəbəkələrin informasiya mühafizə sistemlərinə biosistemlərə xas olan evolyusiya xüsusiyyətlərini və ilk növbədə inkişaf və adaptivlik imkanlarının mənimsədilməsinin zəruriliyi göstərilmişdir.

2. Adaptiv informasiya mühafizə sisteminin bioliji oxşarlıq prinsipinə əsaslanan iyerarxiq modeli və korporativ İT şəbəkəsinin mühafizə olunmasının qiymətləndirilməsi metodikasını daxil etməklə layihələndirilməsinin qeyri-səlis üsulları təklif edilmişdir.

3. Korporativ İT şəbəkələrin informasiya təhlükəsizliyinə təsir göstərən faktorların böyük bir qismini əhatə edən koqnitiv xəritə modeli işlənilmişdir.

4. Korporativ İT şəbəkələrdə informasiya təhlükəsizliyi səviyyəsini qiymətləndirmək məqsədilə tipik qeyri-səlis koqnitiv model işlənilmiş və təsvir edilmişdir.

5. Qeyri-səlis qaydalarla idarə olunan koqnitiv xəritənin modelinin və dinamiki sıraların verilənlərinin qeyri-səlis təhlilinə əsaslanan şəbəkə trafikinin həcminin proqnozlaşdırma modelinin sintezi əsasında şəbəkə trafiki ilə effektiv idarəetmə modeli işlənilmişdir.

6. Şəbəkə trafiklərində IP-paketlərin həcmlərinin dəyişməsinin qeyri-səlis təhlilinə və orada volatilliyin mövcudluğuna əsaslanaraq şəbəkə trafiklərinin həcmlərinin dəyişməsinin proqnozlaşdırılması məsələsi həll olunmuşdur. Nəticədə şəbəkə trafikində mümkün ola bilən anomaliyaların aşkar edilməsi üçün yeni yanaşma təklif edilmişdir.

Dissertasiya işinin əsas nəticələri aşağıdakı elmi məqalələrdə dərc edilmişdir.

1. **V.İ.Həsənov.** Korporativ şəbəkələrin təhlükəsizliyini təmin etmək məqsədi ilə təhlükəsizlik siyasəti və məlumatlandırma işlərinin aparılması. // Gəncə Dövlət Universitetinin Elmi Xəbərləri №3, səh. 47-53, 2013

2. **Rzayev R.R., Camalov Z.R., Mehtiyev T., Həsənov V.İ.** Моделирование временных рядов на основе нечеткого анализа позиционно-бинарных составляющих исторических данных. // Нечеткие системы и мягкие вычисления, Т. 10, №1, ст.37-73, 2015

3. **Əliyev E.R., Camalov Z.R., Xudadova A.K., Həsənov V.İ.** Нечёткая когнитивная модель для комплексной оценки

информационной безопасности. // Transaction of Azerbaijan National Academy of Sciences, Series of Physical-Technical and Mathematical Sciences: Informatics and Control Problems, vol. XXXV, No.6, s. 72-85, 2015

4. **Rzayev R.R., Əliyev E.T., Camalov Z.R., Həsənov V.İ.** Нечёткая когнитивная модель для комплексной оценки продовольственной безопасности. // Azərbaycan Mühəndislik Akademiyasının Xəbərləri, cild 8, №3, s. 109-123, 2016

5. **V.İ.Həsənov.** Прогнозирование сетевого трафика на основе нечёткого анализа изменения объёмов IP-пакетов. // Bakı Dövlət Universitetinin Xəbərləri, Fizika-riyaziyyat elmləri seriyası, №4. s. 123-132; 2016

6. **V.Hasanov, H.Bayramov, T.Mehdiyev.** Prediction of network traffic based on neural-fuzzy analysis of changes in the volume of IP-packets. Procedia Computer Science, Vol. 120, pp. 438–445, 2017;

7. **V.İ.Həsənov.** IP-paketlərin həcminin dəyişməsinin qeyri-səlis təhlili əsasında şəbəkə trafikinin həcmində anomaliyaların aşkar edilməsi. // AMEA Gəncə bölməsi, Xəbərlər məcmuəsi, № 1 (71), s. 232-242, 2018.

8. **V.İ.Həsənov.** Выявление аномалий в сетевых трафиках на основе нечёткого моделирования динамических рядов изменений ОБЪЁМОВ IP-пакетов. // Автоматизация и приборостроение: проблемы, решения, ст.115-117, 2018.

9. **V.İ.Həsənov.** Выявление аномалий в сетевом трафике на основе нейросетевого моделирования динамики изменения объёмов IP-пакетов // “Mathematıcal machınes and systems”, № 2, ст.40-45, 2018

Həmmüəlliflərlə birgə yerinə yetirilmiş işlərdə iddiaçının rolu

[2] Tarixi verilənlər arasında məntiqi əlaqələrin təyin edilməsi üçün qeyri-səlis çıxarış qaydaların qurulmasına dair tövsiyələrin verilməsi və onların icra mexanizminin araşdırılması.

[3] Kompleksli informasiya mühafizəsini təmin etmək üçün konseptual qeyri-səlis koqnitiv xəritənin və onun əsasında qeyri-səlis koqnitiv modelin işlənməsi.

[4] Qida təhlükəsizliyi proqramını icra etmək məqsədilə uyğun qeyri-səlis koqnitiv xəritənin və onun əsasında qeyri-səlis koqnitiv modelin işlənməsi.

Васиф Илкан оглу Гасанов

Построение интеллектуальных интеграционных систем обеспечения информационной безопасности в открытой среде корпоративной сети

Аннотация

В работе исследуется подход к адаптивному моделированию информационной безопасности, осуществляемый на основе биосистемой аналогии с использованием интеллектуальных инструментов нейронных сетей и нечёткой логики.

В работе предлагается методология создания перспективных систем защиты информации с использованием интеллектуальных средств, таких как: системы нечёткой логики, реализующихся в виде нечётких когнитивных моделей, поддерживающих эволюционные свойства средств защиты информации, их адаптации, самоорганизации, обучения, возможности наследования и представления опыта экспертов информационной безопасности в виде доступной для анализа системы нечётких правил If-Then.

Описанное в работе решение задачи управления сетевым трафиком представляет собой нечёткую математическую модель прогнозирования объема сетевого трафика, основанной на нечётком анализе исторических данных временных рядов с привлечением методов статистической обработки данных, и модели когнитивной карты, управляемой нечеткими правилами. Подобный синтез позволил построить эффективную модель управления сетевым трафиком, и предложить техническое решение, которое способствует повышению информационной безопасности сетей общего пользования.

Полученные результаты могут быть использованы для обнаружения неисправностей сетевого оборудования, поиска ошибок в настройке программного обеспечения, выявления случайных и преднамеренных деструктивных действий со стороны легитимных пользователей и злоумышленников.

Vasif Ilkan oglu Hasanov

CONSTRUCTION OF INTELLECTUAL INTEGRATION SYSTEMS PROVIDING INFORMATION SECURITY IN THE OPEN CORPORATE NETWORK ENVIRONMENT

Summary

The approach to adaptive modeling of information security, based on a biosystem of analogy using intelligent tools of neural networks and fuzzy logic is investigated.

The given work proposes a methodology for creating advanced information security systems using intelligent means, such as: fuzzy logic systems implemented as fuzzy cognitive models that support the evolutionary properties of information protection tools, their adaptation, self-organization, training, the possibility of inheritance and the presentation of the expertise of information security experts In the form of an unclear If-Then rules system available for analysis.

The solution of the task of managing network traffic described in this paper is a fuzzy mathematical model for predicting the volume of network traffic based on a fuzzy analysis of historical time series data with the use of statistical data processing methods and a cognitive map model controlled by fuzzy rules. Such a synthesis allowed to build an effective model of managing network traffic, and to offer a technical solution that enhances the information security of public networks.

The results obtained can be used to detect network equipment malfunctions, to find errors in software configuration, to detect accidental and deliberate destructive actions by legitimate users and intruders.

Çapa imzalanıb: 10.07.2018. Tiraj: 100 nüsxə
GDU-nun mətbəəsi. Gəncə şəhəri, Heydər Əliyev prospekti, 429
Tel: (+99422) 256-33-58
e-mail: elm@gdu.edu.az

НАЦИОНАЛЬНАЯ АКАДЕМИЯ НАУК АЗЕРБАЙДЖАНА

ИНСТИТУТ СИСТЕМ УПРАВЛЕНИЯ

На правах рукописи

ВАСИФ ИЛКАН ОГЛУ ГАСАНОВ

ПОСТРОЕНИЕ ИНТЕЛЛЕКТУАЛЬНЫХ ИНТЕГРАЦИОННЫХ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОТКРЫТОЙ СРЕДЕ КОРПОРАТИВНОЙ СЕТИ

3338.01 – «Системный анализ, управление и обработка информации»

А В Т О Р Е Ф Е Р А Т

диссертации на соискание ученой степени
доктора философии по технике

БАКУ - 2018