R.H. GEGHAMYAN, A.K. SAGHATELYAN, A.G. QAMALYAN

HARDWARE IMPLEMENTATION OF THE DEVICE CARRYING OUT CALCULATIONS WITH TRIGONOMETRIC FUNCTIONS

From a standpoint of fast operation, an efficient method for calculating the trigonometric function and its synthesis by applying modern methods of design is considered.

Keywords: trigonometric functions, hardware realization, tabular choice, PROM memory.

ՀՏԴ 530.15

Տ.Ա. ՖԼՋՅԱՆ

ԱՊԱՀՈՎԱԳՐԱԿԱՆ ԸՆԿԵՐՈՒԹՅԱՆ ՔՈՄՓՅՈՒԹԵՐԱՅԻՆ ՑԱՆՑԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՄԻՋՈՑՆԵՐԻ ՀԵՏԱԶՈՏՈՒՄԸ, ՀԱՄԵՄԱՏԱԿԱՆ ԳՆԱՀԱՏՈՒՄԸ ԵՎ ԲԱՐԵԼԱՎՈՒՄԸ

Հետազոտվել է ապահովագրական ընկերության քոմփյութերային ցանցի կառուցվածքը՝ անվտանգության տեսակետից, դիտարկվել են նրա անվտանգության բարձրացման գործիքամիջոցները, և կատարվել է դրանց հիմնավոր ընտրությունը: Իրականացվել է գործող և առաջարկվող ապահովագրական ընկերության մասնագիտացված քոմփյութերային ցանցի կառուցվածքների աշխատունակության, անվտանգության և արդյունավետության համեմատական գնահատումն ու բարելավումը:

Առանցքային բառեր. քոմփյութերային ցանց, ցանցային անվտանգություն, գործիքամիջոց, ցանցային աշխատունակություն և արդյունավետություն, ապահովագրական ընկերության ցանց:

Ներածություն: Ապահովագրական ընկերության քոմփյութերային ցանցերում անվտանգության ապահովման հիմնախնդիրները միշտ եղել են ուշադրության կենտրոնում և շարունակում են մնալ արդիական, քանի որ այդ ընկերությունների մասնագիտացված քոմփյութերային ցանցերին ներկայացվող անվտանգության պահանջները մշտապես վերանայվում ու խստացվում են [1]: Որպես կանոն, յուրաքանչյուր ապահովագրական ընկերության մասնագիտացված քոմփյութերային ցանցի համար անհրաժեշտ է ունենալ իր եզակի անվտանգության ապահովումը, որպեսզի հնարավոր լինի պատշաճ մակարդակով կազմակերպել ցանցի անվտանգության գործընթացը, հաշվի առնելով կենտրոնական բանկի, արտաքին աուդիտի, հաճախորդների և այլոց պահանջներն ու շահերը [1]: Այսպիսի մասնագիտական քոմփյութերային ցանցում անվտանգության կազմակերպումը և իրականացումը ձևավորվում են հիմնական ռիսկերի գնահատումով, կրի-

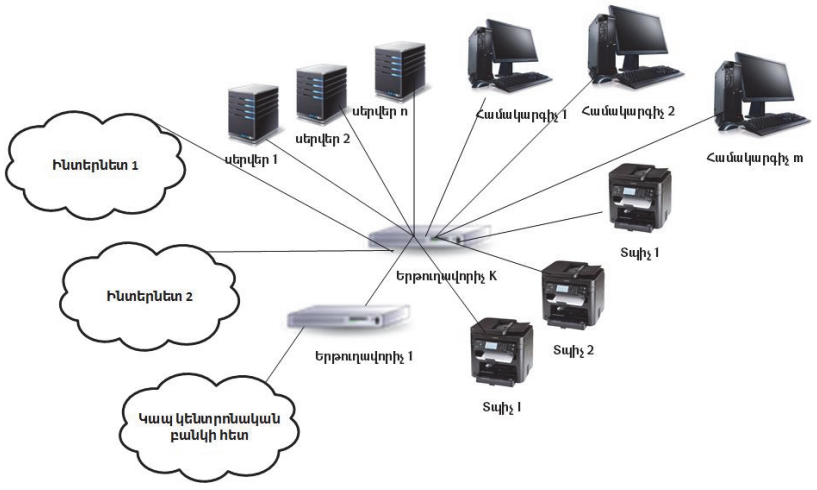
տիկական (բիզնես անընդհատությունը ապահովող) ռեսուրսների որոշմամբ, հնարավոր սպառնալիքների գնահատմամբ և որոշմամբ: Այդ հիմնախնդիրո իրականացնելու համար որպես պարտադիր պայման անհրաժեշտ է ապահովել ապահովագրական ընկերության կողմից մատուցվող ծառայությունների անընդհատությունը, հասանելիությունը, գաղտնիությունը և հուսալիությունը [2, 3]:

Խնդրի դրվածքը: Հետազոտվում են ապահովագրական ընկերության քոմփյութերային ցանցի կառուցվածքը, կազմակերպումը, անվտանգության ապահովման միջոցները, կատարվում են դրանց համեմատական գնահատումը և առաջարկվում է տվյալ մասնագիտացված ցանցի բարելավված անվտանգության ապահովումը:

Ներկայացված խնդրի լուծման համար անհրաժեշտ են հետևյալ քայլերը.

- վերլուծել ապահովագրական ընկերությունների քոմփյութերային ցանցի կառուցվածքը և կազմակերպումը,
- հետազոտել ապահովագրական ընկերությունների քոմփյութերային ցանցի անվտանգության ապահովման միջոցները,
- իրականացնել ապահովագրական ընկերությունների քոմփյութերային ցանցի անվտանգության միջոցների համեմատական գնահատումը,
- կատարել ապահովագրական ընկերության մասնագիտացված քոմփյութերային ցանցի անհրաժեշտ կառուցվածքային փոփոխությունները՝ առաջարկելով նրա բարելավված անվտանգության ապահովումը:

Ապահովագրական ընկերության մասնագիտացված գործող քոմփյութերային ցանցի ընդհանուր կառուցվածքի օրինակը բերված է նկ. 1-ում:



Նկ. 1. Ապահովագրական ընկերության գործող քոմփյութերային ցանցի ընդհանուր կառուցվածքը

Բերված քոմփյութերային ցանցում ներկայացված են երթուղավորիչներ (K հատ), սերվերներ (n հատ), համակարգիչներ (m հատ) և այլ սարքավորումներ: Ներկայացված մասնագիտացված քոմփյութերային ցանցի հիմնական թերությունն այն է, որ ապահովագրական ընկերությունում ներդրված և գործող բոլոր համակարգերը գտնվում են նույն ցանցում, և երթուղավորիչները չեն կարող ապահովել համապատասխան անվտանգությունը:

Ըստ միջազգային ստանդարտների (ISO 27001) [4]՝ քոմփյութերային ցանցի անվտանգության արդյունավետ կազմակերպման համար պետք է իրականացնել մի շարք գործողություններ, որոնցից են.

- անվտանգության քաղաքականության ձևավորումը,
- անձնակազմի հետ կապված անվտանգության ապահովումը,
- ցանցային միացումների անվտանգության ապահովումը,
- ֆիզիկական անվտանգության ապահովումը,
- իրավասությունների կառավարումը,
- միջադեպերի կառավարումը,
- բոլոր այլ օրենսդրական ակտերին համապատասխանության ապահովումը:

Օգտագործելով առկա փորձը և ունենալով համապատասխան պահանջները [2], ստեղծվել է անվտանգության գործիքամիջոց, որի հիմնական բաղադրիչներից են նույնականացումը, ամբողջականությունը և ակտիվ ստուգումը: Նույնականացումը նախատեսված է՝ կանխելու վտանգը և չարտոնված մուտքը դեպի համակարգ: Ամբողջականությունը երաշխավորում է տեղեկատվության չթույլատրված (սխալմամբ կամ դիտավորյալ) փոփոխության անհնարինությունը: Ակտիվ ստուգումը հնարավորություն է տալիս հայտնաբերելու չարտոնագրված մուտքերը դեպի ցանց: Այն իրականացնելու համար անհրաժեշտ է հավասար ժամանակահատվածում կատարել ստուգումներ: Ստուգման ժամանակ պետք է ուշադրություն դարձնել նոր տեղադրվող համակարգերին և դրանց ազդեցությանը ցանցին, ինչպես նաև ներքին աշխատակիցների գործողություններին: Անվտանգության գործիքամիջոցում ներառված են լինում օգտագործվող բոլոր արձանագրությունները. տրանսպորտային մակարդակի արձանագրությունները՝ SSL և Secure Shell Protocol (SSH), որոնք ապահովում են տվյալների անվտանգ փոխանցումը հաճախորդների և սերվերի միջև, ցանցային մակարդակի արձանագրությունները՝ IP (IPSec), որոնք ապահովում են տվյալների փոխանցման ամբողջականությունը և գաղտնիությունը [4]: Արձանագրությունները ապահովագրական ընկերության մասնագիտացված քոմփյութերային ցանցում համակարգերի աշխատանքի համար կարևորագույն պարամետրերից են, որոնց մի-

ջոցով հստակ ձևակերպվում են բոլոր համակարգերի միջև տվյալների փոխանցման ուղիները, և սահմանվում են համապատասխան սահմանափակումները: Կան նաև մի շարք այլ արձանագրություններ, որոնց անվտանգության պահանջներ չեն ներկայացվում, կայքերում http (80), էլեկտրոնային փոստի աշխատանքի համար՝ SMTP, POP3, IMAP արձանագրությունները [5]: Ֆիզիկական և ցանցային միացումների անվտանգության ապահովման համար, նախ և առաջ, անհրաժեշտ է մալուխներն անցկացնել հասանելիություն չունեցող հատվածով, որը կդժվարացնի արտաքին ֆիզիկական միացումը և կպաշտպանի արտաքին գործոններից: Կախված ցանցին ներկայացվող պահանջներից և մալուխի անցկացման միջավայրից՝ կատարվում է մալուխի ընտրությունը: Երթուղիչները նույնպես պետք է լինեն պաշտպանված: Դրանք պետք է ունենա MAC հասցեների ղեկավարում, որը թույլ կտա սահմանափակել այն հանգույցները, որոնց մասին տեղեկություն առկա չէ, ինչպես նաև կհայտնաբերվի միանման MAC հասցեի միացումը տարբեր հանգույցների: Դա կօգնի հայտնաբերելու հակերների կողմից իրական MAC հասցեի փոփոխումը այլ հասցեի: Կառուցվածքային առումով անվտանգության ապահովման համար անհրաժեշտ է ունենալ ցանցի աստղաձև կառուցվածք, որտեղ հնարավոր կլինի ցանցը բաժանել ենթացանցերի: Այն պետք է բաղկացած լինի առնվազն 3 ենթացանցերից [6].

- ընդհանուր համակարգիչների ենթացանց,
- սերվերային համակարգերի ենթացանց,
- համակարգերի ենթացանց, որոնք պետք է հասանելիություն ունենան արտաքին աշխարհից (demilitarized zone):

Ապահովագրական ընկերության քոմփյութերային ցանցի անվտանգության գործընթացում մեծ դեր ունի նաև իրավասությունների և միջադեպերի կառավարման համակարգը: Ի սկզբանե ընդունվում են հետևյալ մոտեցումները.

- «Այն ամենը, ինչ ակնհայտորեն չի թույլատրվում, արգելվում է»:
- «Նվազագույն արտոնություն»՝ օգտագործողի իրավասությունները համակարգում պետք է սահմանափակվեն նվազագույն անհրաժեշտով՝ պարտականությունները կատարելու համար:
- «Անհրաժեշտ է իմանալ». օգտագործողին պետք է հասանելի լինի միայն այն տեղեկությունը, որն անհրաժեշտ է իր պարտականությունները կատարելու համար:
- «Պարտականությունների սահմանազատում»՝ օգտագործողների պարտականությունները և դրանցից բխող իրավասությունները համակարգերում պետք է բացառեն զգայուն գործընթացներին միանձնյա տիրապետումը:

Տվյալ մասնագիտացված քոմփյութերային ցանցում տեղեկատվական անվտանգության միջադեպերի կառավարման գործընթացն իրականացվում է հետևյալ փուլերով.

- իրադարձությունների և միջադեպերի հայտնաբերում և տեղեկացում,
- միջադեպերի գնահատում,
- միջադեպերի արձագանքման պլանավորում և նախապատրաստում,
- միջադեպերի արձագանքում,
- միջադեպերի վերլուծություն և բարելավում:

Քանի դեռ ապահովագրական ընկերությունների քոմփյութերային ցանցերին ներկայացվող անվտանգության պահանջները խիստ սահմանված չէին, չկար անվտանգության ապահովման հստակ տեխնիկական պահանջներ, օգտագործվում էր առանց ենթացանցերի կառուցվացքով ցանց, որտեղ չկար սահմանված որևէ պահանջ մալուխների ընտրության և ֆիզիկական անվտանգության, սարքավորումների ընտրության, պահպանման և պահուստավորման համար: Չէին ստուգվում և սահմանափակվում օգտագործվող արձանագրությունները, չկար միջադեպերի կառավարման և իրավասությունների տրամադրման համակարգ:

Դրական կողմերն էին.

- քոմփյութերային ցանցի նախագծումը և կառուցումը հեշտ էր և էժան,
- կառուցվում էր պարզ և էժան սարքավորումներով,
- սպասարկման գործընթացը հասցված էր նվազագույնի:

Բացասական կողմերն էին.

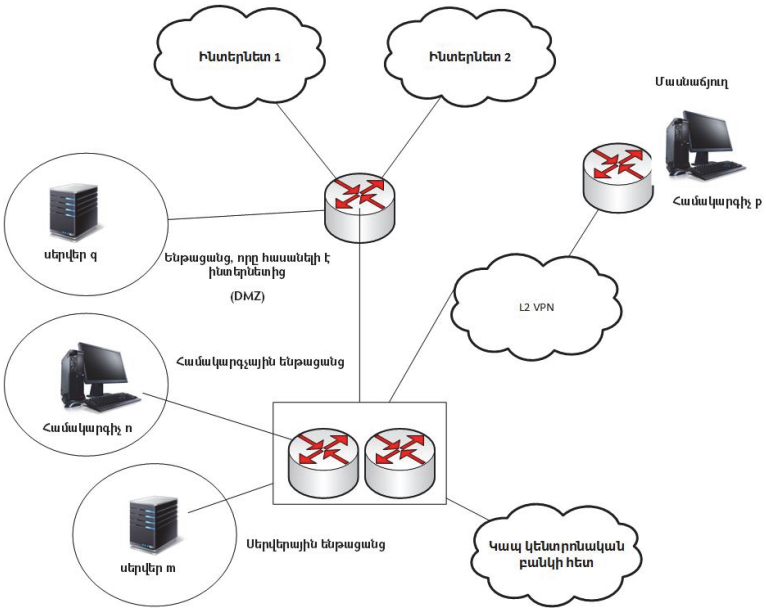
- չկար ներքին և արտաքին համակարգերի տարանջատման հնարավորություն. համակարգը խոցելի էր,
- բացակայում էր վերահսկման հնարավորությունը,
- չկար տեղեկություն ցանցի իրավիճակի մասին. կա արդյոք ցանցում որևիցե միջադեպ, թե ոչ:

Օգտագործելով գործիքամիջոցը, կատարվեց ցանցի վերակառուցում, որոշվեցին երթուղիչների քանակը, մոդելը, տրվեց համապատասխան ցանցի բաժանումը ենթացանցերի (նկ. 2), հստակեցվեցին համակարգերի աշխատանքային արձանագրությունները (աղ.):

Համակարգերի աշխատանքային արձանագրությունները

N	Source	Destination	Web-Resource	HTTP LINK	Source Port	Local IP	Local Port
1	0.0.0.0/0	212.212.34.45	Exchange Server		443,110, 25	100.100.100.4	443,110, 25
2	0.0.0.0/0	212.212.34.46	Web resource 1	https://test.am	443	100.100.100.5	443
3	212.112.35.48	212.212.34.47	Web resource 2	https://test1.am	443	100.100.100.6	443

Աղյուսակում ցույց են տրված բոլոր այն համակարգերը, որոնք հասանելի են արտաքին աշխարհից՝ աշխատանքի համար նախատեսված համապատասխան արձանագրություններով:



Նկ. 2. Ցանցի վերակառուցված մոդելը

Եզրակացություն.

1. Հետազոտվել և վերլուծվել են ապահովագրական ընկերության քոմփյութերային ցանցի առկա վիճակը, և առաջարկվել է ցանցի վերակառուցված մոդել:

2. Սահմանվել են հիմնական անվտանգության ապահովման գործիքամիջոցները:

3. Վերլուծելով ուսումնասիրությունները՝ առաջարկվել և ներդրվել է «Ինգո Արմենիա» ապահովագրական ընկերության քոմփյութերային ցանցի անվտան-

գության բարձրացման նպատակով Juniper SRX240 մոդելի սարքավորումը, որի արդյունքում ապահովագրական ընկերությունն ունի.

- ✓ իրական ռեժիմում աշխատող 47 մասնաճյուղ՝ միացված VPN կապով,
- ✓ 1,000 - 1,500 գործակալներ, որոնք աշխատում են ինտերնետ կապի միջոցով:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. http://www.ombuds.am/
2. **Հայաստանի Հանրապետության Կենտրոնական Բանկ** - խորհրդի թիվ 173-ն որոշում, 09.07.2016:
3. **Олифер В. Г., Олифер Н. А.** Компьютерные сети. Принципы, технологии, протоколы.- 2015. – 944 с.
4. **Трошин С.В.** Мониторинг работы корпоративных пользователей // Вопросы современной науки и практики /Университет им. В.И. Вернадского. - 2009. - № 2 (16). - С.59-72.
5. **Кулябов Д.С., Королькова А.В.** Архитектура и принципы построения современных сетей и систем телекоммуникаций. –М., -2008. - 309 с.
6. http://www.itsec.ru/articles2/pravo/standartizaciya-v-oblasty-ib-zarubezhn-opyt-chast-1 - Ստանդարտացումը SS բնագավառում. արտասահմանյան փորձը:

Т.А. ФЛДЖЯН

ИССЛЕДОВАНИЕ СРЕДСТВ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ СТРАХОВОЙ КОМПАНИИ И СРАВНИТЕЛЬНАЯ ОЦЕНКА

Исследованы средства безопасности компьютерных сетей страховой компани и их особенности. Из основных параметров рассмотрена безопасность корпоративной сети.

Ключевые слова: компьютерная сеть, безопасность сети, инструментальное средство, надежность и эффективность сети, сеть страховой компании.

T.A. FLJYAN

RESEARCH OF TOOLS FOR COMPUTER NETWORK SECURITY OF AN INSURANCE COMPANY AND A COMPARATIVE EVALUATION

The security of computer network of an insurance company, and its peculiarities have been investigated. Among the main parameters, the security of the corporate networks is considered.

***Keywords*:** computer network, network security, tools, reliability, insurance company, network efficiency.