ISSN 0002-306X. Изв. НАН РА и ГИУА. Сер. ТН. 2011. Т. LXIV, № 4.

ՀՏԴ 004. 056. 57

ՀԱՇՎՈՂԱԿԱՆ ՏԵԽՆԻԿԱ ԵՎ ԻՆՖՈՐՄԱՏԻԿԱ

Ա. Յու. ՂԱԶԱՐՅԱՆ

ՏԵՂԵԿԱՏՎԱԿԱՆ ՑԱՆՑԵՐՈՒՄ ԳՐՈՀՆԵՐԻ ՀԱՅՏՆԱԲԵՐՄԱՆ ԱՎՏՈՄԱՏԱՑՎԱԾ ՄԻՋՈՑՆԵՐԻ ՆԱԽԱԳԾՈՒՄ ՆԵՅՐՈՑԱՆՑԵՐԻ ՄԻՋՈՑՈՎ

Տեղեկատվական ցանցերում արտաքին գրոհների հայտնաբերման նպատակով նախագծվել է ծրագրային փաթեթ: Ծրագրային փաթեթում կիրառված են արհեստական նեյրոցանցեր, որոնց միջոցով կարելի է դուրս բերել նոր և ձևափոխված գրոհներ:

Առանցքային բառեր. բաշխված գրոհներ, հիբրիդային ցանց, ավտոմատացված միջոցներ:

Ներածություն: Շատ կազմակերպություններ և ձեռնարկություններ ամբողջ աշխարհով մեկ օգտագործում են քոմփյութերային համակարգերի ավտոմատացված միջոցներ՝ արտադրական գործընթացների ղեկավարման, ռեսուրսների բաշխման և այլ նպատակներով: Ավտոմատացված միջոցների օգտագործումը մի շարք բացահայտ առավելություններ ունի: Դրանք են՝ վերադիր ծախսերի նվազեցում, արտադրական գործընթացների արագ կատարում: Բացի դրանից, շուկայում առաջ են եկել նոր բնույթի ծառայություններ՝ բանկային հաշիվների հեռակառավարում, ինտերնետի միջոցով ապրանքների և ծառայությունների պատվեր ու վճարում և այլն: Նշված պատճառներով մարդու գործունեության մեջ էապես բարձրացել է տեղեկությունների փոխանակման դերը:

Սակայն ավտոմատացված միջոցների բուռն աճը հանգեցրեց նաև քոմփյութերային հանցագործության զարգացմանը: Այսօր գերակշռող գրոհներից են համարվում բաշխված ցանցային գրոհները, որոնց կանխումը և վնասազերծումը դարձել է արդիական հիմնախնդիր: Այդ գրոհների նպատակն է կաթվածահար անել գրոհող web հանգույցը: Բացի այդ, ցանցային գրոհները հաճախակի փոփոխվում են՝ գրոհողների անհատական մոտեցումների, նաև համակարգում ծրագրային ապահովվածության և ապարատային միջոցների պարբերաբար փոփոխությունների պատճառով: Գրոհների բացահայտման բոլոր օգտագործվող մեթոդները հանգեցվում են մի հիմնախնդրի. հաճախակի փոփոխվող ցանցային գրոհների բնութագրերը պահանջում են ճկուն պաշտպանող ավոտամատացված միջոցներ (ծրագրային փաթեթ), որոնք արդյունավետ կլինեն, եթե անգամ հայտնի չեն գրոհների ճշգրիտ բնութագրերը:

1. Ուսումնասիրության նպատակը և խնդիրները: Կան գրոհի հայտնաբերման երկու հիմնական տեխնոլոգիաներ՝ նորմից շեղված և չարաշահող: Նորմից շեղման

երևույթների հայտնաբերման մշակված մեթոդները կարող են օգտագործվել նոր գրոհների բացահայտման համար, սակայն ունեն վերլուծության ցածր արագություն: Նորմից շեղման երևույթների հայտնաբերման հիմնադրույթն այն է, որ գրոհները տարբերվում են նորմալ վարքից:

Երկրորդ և ամենատարածված գրոհների հայտնաբերման մոտեցումը չարաշահումների բացահայտումն է (Misuse Detection Instrusion Systems, MD-IDS): Այս համակարգը հիշեցնում է ցանցին միացված հակավիրուսային ծրագրերը: Այս մեթոդով իրականացվում է օգտագործողի գործունեության համեմատումը հայտնի շաբլոնների հետ: Սովորաբար նման համակարգերն ունեն սիգնատուրների հավաքածու, որոնք նկարագրում են միացությունների և ցանցային թրաֆիկի տեսակները և կարող են ցույց տալ գրոհի առկայությունը [1]: Չարաշահումների հայտնաբերման համակարգի հիմնական առավելությունն այն է, որ տվյալների բազայի վերլուծությունը կենտրոնացված է, և սովորաբար քիչ են կեղծ ահազանգեր առաջացնում: Չարաշահումների հայտնաբերման համակարգի հիմնական թերությունը կարող են որոշել միայն հիմնական գրոհները, որոնց համար սիգնատուր կա: Նոր գրոհներ հայտաբերելու համար պետք է մշակել համապատասխան նոր մոդել՝ ավելացնելով սիգնատուրների բազայի մեջ:

Գրոհների հայտնաբերման մեթոդից անկախ, տեղեկատվություն ստանալու համար գրոհների բացահայտման արդյունավետությունը մեծ մասամբ կախված է կիրառվող վերլուծության մեթոդներից [2]. դրանցից են՝ վիճակագրական մեթոդը, կանխագուշակող շաբլոների օգտագործումը, մի վիճակից մյուսին անցնելու վերլուծությունը, ոչ պարզ տրամաբանությունը, փորձագիտական համակարգերը, գենետիկական ալգորիթմները, մարկովյան գաղտնի մոդելները, Data Mining մեթոդները, արհեստական նեյրոցանցերը: Ուսումասիրությունները ցույց են տվել, որ արհեստական նեյրոնային ցանցերը, ի տարբերություն կիրառվող վերլուծության մյուս մեթոդների, աշխատում են ոչ ամբողջական տվյալների հետ, նաև ունեն գրոհներ դուրս բերելու և կանխատեսելու հնարավորություն [3]:

2. Առաջարկվող մեթոդները: Իմանալով ցանցային գրոհների, մասնավորապես, բաշխված գրոհի գործելու սկզբունքը՝ առաջարկվում է օգտագործել արհեստական նեյրոնային ցանցեր: Արհեստական նեյրոցանցը ունակ է §ուսումնասիրելու¦ կանխամտածված գրոհների բացահայտումը և նույնականացնելու տարրերը (թրաֆիկը), որոնք նման չեն նախկինում եղած տարրերին: Նեյրոցանցը կարող է մեծ ճշտությամբ հայտնաբերել կասկածելի դեպքերը: Դա համարվում է լավ հատկանիշ, քանի որ հակերները շատ հաճախ նմանակում են ուրիշների §հաջողությունները¦:

Գրոհների բացահայտման ավտոմատացված միջոցները նախագծելու նպատակով անհրաժեշտ է լուծել հետևյալ խնդիրը.

1) Գտնել արհեստական նեյրոնային ցանցի հիման վրա նորմից շեղված երևույթների հայտնաբերման մեթոդ, որը թույլ է տալիս բացահայտել չգրանցված գրոհները:

2) Ավտոմատացնել բաշխված ցանցային գրոհների բացահայտման համակարգը, որն իրականացվում է համադրված երկու արհեստական նեյրոնային ցանցի (հիբրիդային արհեստական նեյրոցանցի) գյուտով:

Ներմուծենք հետևյալ նշանակումները.

Ենթադրենք՝ M–ը գրոհների հայտնաբերման մուտքային տվյալների մեծությունն է: Համակարգը սահմափակված է մուտքային տվյալների ծավալով. այն կարող է վերամշակվել իր աշխատանքի որոշակի տակտի ընթացքում: Դա նշանակում է, որ M-ը վերջավոր մեծություն է: Տվյալ M բազմությունը բաժանենք երկու ենթաբազմության՝ A և B: A ենթաբազմությանը վերաբերում են այնպիսի տվյալներ, որոնք համարվում են գրոհներ, իսկ B ենթաբազմությանը՝ այնպիսի տվյալներ, որոնք անվտանգ են համարվում համակարգի համար: Այստեղից էլ կարելի է հետևություն անել՝

$$A \in M,\ B \in M,\ A \cap B \neq 0,\ A \cup B = M: \qquad (1)$$

Ցանցային թրաֆիկում նորմից շեղված գրոհների որոման մեթոդը հիմնված է տվյալների համընկնումների վրա, որոնք ներթափանցում են տեղեկատվական համակարգ՝ B ենթաբազմության տարրերի միջոցով: Այն դեպքում, երբ համընկնումը գտնված չէ, հաշվում են, թե որ մուտքային տվյալներն են համարվում գրոհներ: Այս մեթոդի համար B ենթաբազմության, հետևաբար՝ նաև A ենթաբազմության բոլոր տարրերը տեսականորեն ճանաչելի են և պարզ: Չնայած դրան՝ գործնականում շատ դժվար է լիարժեք և հստակ ձևավորել B ենթաբազմության տարրերը: Նորմից շեղված գրոհների հայտնաբերման մեթոդի համար առաջին կարգի սխալի հավանականությունը կազմում է.

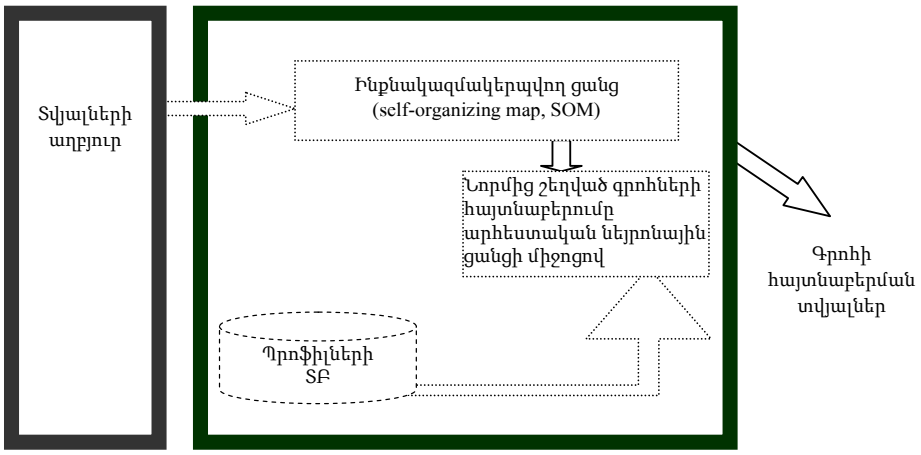
$$P_I = \frac{\psi(Y(B_{\text{ձև}}^{\,n}{}_{x=0} \cap A))}{\psi(A)}: \qquad (2)$$

Երկրորդ կարգի հավանականության սխալը համապատասխանաբար հավասար է

$$P_{II} = \frac{\psi(B) - \psi(Y(B_{\text{ձև}}^{\,n}{}_{x=0} \cap B))}{\psi(B)}: \qquad (3)$$

Խոցելիության հայտնաբերման ընթացքում ի հայտ են գալիս խոցելիության ձևակերպման բոլոր խնդիրները, այսինքն՝ հնարավոր չէ թվարկել տեղեկատվական համակարգում բոլոր խոցելիությունները, և, հետևաբար, նաև անծանոթ է A ենթաբազմության տարրերի ամբողջական հավաքածուն: Մեթոդն ունակ է ի հայտ բերելու միայն ճանաչված գրոհները: Ըստ վերոհիշյալի, B ենթաբազմության տարրերի հստակ և լիարժեք ձևակերպման խնդիրը շատ դժվար է լուծվում: Սրա հետևանք է առաջին կարգի հավանականության սխալների առավել մեծ արժեքը: Ի հայտ է գալիս մեթոդի նախագծման խնդիրը, որը կպարունակի երկու մեթոդների առավելությունները, այսինքն՝ առաջին և երկրորդ կարգի սխալների նվազեցման խնդրի լուծումը: Վերլուծելով գոյություն ունեցող գրոհների բացահայտման դասական մեթոդների առավելություններն ու թերությունները և հետազոտելով թերությունների առաջ գալու պատճառները՝ առաջանում է գրոհների

բացահայտման ավտոմատացված միջոցների նախագծման խնդիր, որի միջոցով կարելի է հայտնաբերել գրոհը (նկ. 1):

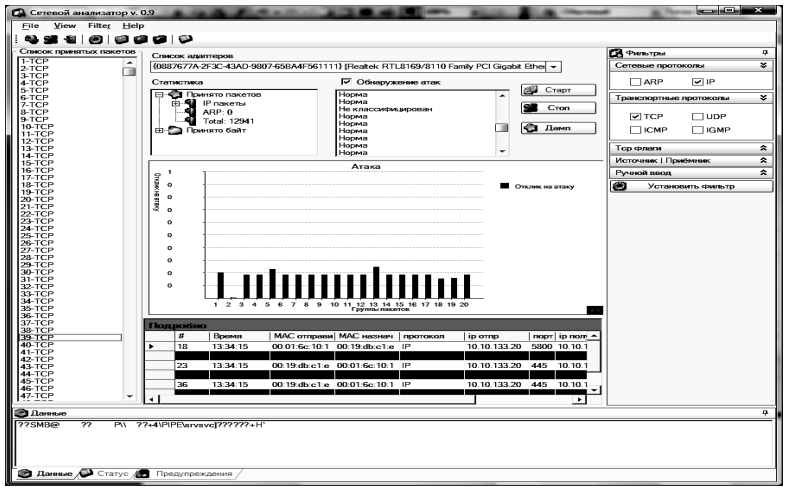


Նկ. 1. Գրոհների բացահայտման մեթոդի ընդհանրացված սխեմա

Բաշխված գրոհների բացահայտման համար առաջարկվում է կիրառել հիբրիդային նեյրոնային ցանց, որը բաղկացած է ինքնակազմակերպվող ցանցից (self-organizing map, SOM) և բազմաշերտ տեսակի պերսեպտրոնից: Ինքնակազմակերպվող ցանցն օգտագործվում է դասակարգելու կիրառական մակարդակում օգտագործվող ծանրաբեռնվածության առաջիկա հիսուն նիշերը (ASCII-կոդում) հանգույցների, որտեղ իրադաձությունները խմբավորված են որոշակի կանոնակարգով: Դրանից հետո փաթեթների վերնագրերի և խմբավորման մասին տվյալները հանդես են գալիս որպես բազմաշերտ պերսեպտրոնի մուտքային տվյալներ: Դասակարգված իրադարձությունները (վեկտորները) պերսեպտրոնի մուտքի վեկտորներ են: Բազմաշերտային պերսեպտրոնը ուսուցանված է ցանցային թրաֆիկի նորմից շեղումը դասակարգելու նպատակով, բայց արդեն հաշվի առնելով տեղեկատվությունը իրադարձության մասին, այսինքն՝ փաթեթի պատկանելությունը այս կամ այն սցենարի խմբին: Դա թույլ է տալիս ոչ միայն բացահայտել նորմից շեղումը միավոր փաթեթներում, այլ նաև դուրս բերել փաթեթում ներառված գրոհը: Վերահսկվող ցանցում թրաֆիկի <վարքագիծն> ունի իր կանոնակարգումները: Կանոնակարգումների առկայությունը հանգեցնում է վեկտոր-կերպարների վիճակագրական հատկանիշների, որոնք մոտ են բազմաչափ տարածության մեջ: Հիմնելով այս հատկանիշների վերլուծության վրա՝ պերսեպտրոնային ցանցը տարածությունը բաժանում է երկու մասի՝ նորմալ և ոչ նորմալ: Փաստորեն, տվյալ խնդիրը IP փաթեթների վերնագրերի դասակարգումն է հետևյալ սկզբունքով. կան արդյո±ք նրանում գրոհի հատկանիշներ, թե± ոչ: Քանի որ պերսեպտրոնը կերպար-

ների տարածությունները բաժանում է երկու մասի, նրա ելքային շերտը պետք է բաղկացած լինի երկու նեյրոններից, որոնցից մեկի ակտիվացումը կնաշանկի գրոհի բացակայություն, իսկ մյուսինը՝ դրա առկայություն: Այսպիսով, [1,0] կերպարների ֆայլերի գրանցումը պետք է համապատասխանի նորմալ հատկանիշներին, իսկ [0,1] կհամապատասխանի նորմից շեղմանը [4]:

Տեղեկատվական ցանցերում արտաքին գրոհների հայտնաբերման նպատակով նախագծված է ծրագրային փաթեթ: Նեյրոնային ցանցերի ուսուցման առաջարկվող ծրագրային փաթեթը նախատեսված է հիբրիդային ցանցի՝ կոխոնենային ցանցի և բազմաշերտ նեյրոնային ցանցերի կիրառման համար: Ծրագրային փաթեթը հարմարեցված է ցանցային գրոհների, ինչպես նաև նոր և ձևափոխված գրոհների բացահայտմանը: Այս փաթեթը կազմված է երկու ծրագրից, որոնք միմյանց հետ փոխգործակցում են. առաջինը՝ MATLAB R2008a-ի կիրառությունն է, որը համարվում է փաթեթի հիմնական ծրագիրը: Նրա միջոցով ընտրվում են նեյրոնային ցանցի կառուցվածքը, ուսուցման օրինակների բազմությունը, ցանցի պարամետրերի սկզբնական արժեքների վերագրման եղանակն ու միջակայքը, ուսուցման ալգորիթմը, որի հաստատունների ու գործակիցների արժեքների տրման հնարավորությամբ էլ իրականացվում է ուսուցումը: Երկրորդ ծրագիրը՝ NetMon, իրական ժամանակում գրոհների բացահայտման ավտոմատացված միջոցն է, ինչպես նաև իրագործվում է ցանցային փաթեթների հավաք, այնուհետև դրանց ձայնագրում MATLAB-ում՝ բինարային ֆորմատով: NetMon ծրագրի արտաքին տեսքը պատկերված է նկ. 2-ում:



Նկ. 2. NetMon ծրագրի արտաքին տեսքը

Ուսուցման ընտրանքի ֆայլը կարելի է ստեղծել կամ խմբագրել ինչպես ցանկացած տեքստային խմբագիր օգտագործելու ճանապարհով, այնպես էլ NetMon ծրագրի միջոցով: MATLAB ծրագրի կիրառմամբ կարելի է ավտոմատացնել նեյրոնային ցանցի ուսուցման գործընթացը: Այն ունի ամբողջ նախագծի բեռնավորման և հիշելու հնարավորություն: Ծրագիրն աշխատում է ուսուցման ընտրանքի և քաշային գործակիցների հետ: Աշխատանքը կազմված է երկու փուլից՝ հիբրիդային ցանցի ուսուցում և գրոհի բացահայտում: Ուսուցման ընտրանքը ստեղծելու համար հավաքում են ցանցային փաթեթները, այնուհետև գրանցվում են դրանք MATLAB-ում՝ բինարային ֆորմատով: Դրա համար օգտագործվում է Matlab Compiler-ի Net հավաքածուն save_vectors.dll ֆայլը:

Իրականացվել է ծրագրային փաթեթի փորձարարական հետազոտումը: Փորձի համար ընտրվել է web տիպային կոնֆիգուրացիա ունեցող սերվեր, որտեղ աշխատեցվում են web, ftp, torrent սերվերներով ծառայություններ: Այդպիսի կոնֆիգուրացիա ունեցող սերվերներն ավելի հաճախակի են հանդիպում և համապատասխանաբար ավելի հաճախ են գրոհի ենթարկվում:

Գրոհների բացահայտման ավտոմատացված միջոցների նախագծված փաթեթի փորձարարական հետազոտումը կազմված է չորս հիմնական փուլերից [5].

1. **Տվյալների հավաքման փուլ:** Ցանցային վերլուծաբան NetMon ծրագրի միջոցով հավաքվել են 33000 հատ ցանցային փաթեթներ, որոնք բնութագրում են (Web, ftp, torrent) ծառայություններ ունեցող սերվերի նորմալ ցանցային թրաֆիկը, 33000 գրոհող ցանցային փաթեթներ, որոնք բնութագրում են FTP-bruteforce գրոհի ցանցային թրաֆիկը, և 33000 ցանցային փաթեթներ, որոնք պարունակում են DDoS գրոհներ (TCP SYN Flood գրոհներ՝ պատահական պորտերի համարներով և զրոյական արժեքներով [6]).

2. **Ուսուցանվող ընտրանքի ձևավորման փուլ:** Ուսուցանվող ընտրանքը ձևավորված է հավաքված ցանցային փաթեթի տվյալներից՝ 12000-ը նորմալ, 12000-ը գրոհող, ընդամենը՝ 24000 փաթեթ, իսկ մնացածը՝ թեստային: Ուսուցանվող ընտրանքի չափսը սահմանվել է, առաջին հերթին՝ հիշողության և ժամանակի չափի հիման վրա, որն անհրաժեշտ է Կոխոնենի ցանցի ուսուցման ամենառեսուրսատար մասի համար:

3. **Ուսուցման փուլ:** Կոխոնենի ցանցի ուսուցանումն իրականացվում է առանձին փաթեթներում: Ուսուցման տևողությունը մոտ հիսուն րոպե է: Բոլոր տվյալները նորմավորվում են [0,1] տիրույթում՝ մինչ Կոխոնենի և բազմաշերտ պերսպետրոնային ցանցի մուտքագրվելը: Կոխոնենի ցանցն ունի բազմանկյան նեյրոնային կապերի կառուցվածք, որն առաջարկվում է MATLAB ծրագրի միջոցով՝ լռելյայն: Կոխոնենի ցանցի չափականությունն է՝ som_x = 25, som_y = 20, ցանցի նեյրոնների (կլաստերների) քանակն է՝ som_size = 500: Կոխոնենի ցանցում միասին կապակցող կլաստերների քանակն է՝ cluster_step = 5:

4. **Ճանաչման փուլ:** Ճանաչումն իրականացվում է թեստային ընտրանքի հիման վրա: Հաշվի են առնվում էտալոնին մոտիկ տվյալներ: Ճանաչումը համարվում է հաջող, եթե փաստացի և էտալոնայինի բացարձակ արժեքների

տարբերությունները յուրաքանչյուր ելքային վեկտորի բաղադրիչի համար չեն գերազանցում 0.3-ը: Կոխոնենի ցանցի ցանցային փաթեթների դասակարգման արդյունքները սխեմատիկորեն բերված են աղյուսակում: Ճանաչման փուլում ստացվում են աղյուսակում բերված արդյունքները:

Աղյուսակ

	Վեկտորների ընդհանուր քանակը	Որից ճիշտ է դասակարգված	Որից սխալ է դասակարգված	Սխալի տոկոսը
Նորմալ	140	138	2	1,4%
Գրոհ	360	360	0	0%
Ընդհանուր	500	498	2	0,4%

Առաջին կարգի սխալը կազմում է՝ 1,4 %, երկրորդինը՝ 0%, ընդհանուր սխալը՝ 0,4%:

Եզրակացություն. Նախագծվել է գրոհների բացահայտման ավտոմատացված միջոցների մեթոդ, որը հիմնված է մի շարք այլ եղանակների վրա՝ ցանցային թրաֆիկում նորմից շեղման բացահայտում, որը վկայում է գրոհի առկայության մասին: Մեթոդը հնարավորություն է տալիս շտկել դասական մեթոդների թերությունները, մասամբ փոքրացնել գրոհների բացթողման քանակը և բացահայտել նոր և ձևափոխված գրոհներ: Այսպիսով, փորձնականորեն նախագծված մոդելի թեստավորման արդյունքները, որոնք օգտագործվում են երկու տարբեր արհեստական նեյրոցանցի հիման վրա, հնարավորություն են տալիս օգտագործել այն գործնականում: Գրոհի բացթողման հավանականությունը կազմում է 0,001, կեղծ ահազանգինը՝ 0,014: Նշենք, որ արտադրությունը իրական համակարգում կախված կլինի ցանցում մուտքային տվյալների արագությունից և այն ԷՀՄ-ից, որտեղ պետք է գործի այս ավտոմատացված համակարգը:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Лукацкий А.В.** Обнаружение атак. - 2-е изд., перераб. и доп.-СПб.: БХВ-Петербург, 2003. - 564 с.
2. **Медведовский И. Д. Семьянов П.В., Платонов В.В**. Атака через Интернет / НПО ”Мир и семья-95”, 1997. - 147с.
3. **Лукацкий А.В.** Новые подходы к обеспечению информационной безопасности сети //Компьютер-Пресс. - 2000.-N7. 140с.
4. **Markarov Vahan, Ghazaryan Armen.** Detection of distributed attacks based on hybrid neural networks // Proceedings of the 2010 International Conference on Security & Management- SAM 2010.- July 12-15, 2010 Las Vegas Nevada, USA, 2 Volumes. CSREA Press 2010, ISBN 1-60132-163-5, 589-593.
5. **Казарян А.Ю**. Выявление распределенных атак в компьютерных сетях // Вестник Государственного инженерного университета Армении (ВГИУА). Серия “Моделирование, оптимизация, управление”. - Ереван, 2010. – Вып. 13, том 1. - С. 46 –50.

ՀՊՃՀ (Պ): Նյութը ներկայացվել է խմբագրություն 10.04.2011:

А. Ю . КАЗАРЯН

ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННЫХ СРЕДСТВ ОБНАРУЖЕНИЯ СЕТЕВЫХ АТАК В ИНФОРМАЦИОННЫХ СЕТЯХ ПОСРЕДСТВОМ ИСКУССТВЕННЫХ НЕЙРОСЕТЕЙ

В целях выявления внешних атак в информационных сетях спроектирован программный пакет. В программном пакете использованы искусственные сети, с помощью которых можно выявить новые и модифицированные атаки.

Ключевые слова: распространенные атаки, гибридная сеть, автоматизированные средства.

A.Yu. Ghazaryan

DESIGNING OF NETWORK ATTACK BY AUTOMATED SENSORS BY MEANS OF ARTIFICIAL NEURAL NETWORKS

To reveal external attacks in information networks, a software package is designed. Artificial networks are used and with their help it is possible to reveal the new and modified attacks.

Keywords: widespread attacks, hybrid network, automated facilities.