# Պաշտոնական ընդիմախոսի կարծիք

Թիմուր Ջամոարյանի «Տեղեկատվական ցանցում տվյալների ամբողջականության ապահովման համակարգի մշակումը» թեմայով Ե.13.04 «Հաշվողական մեքենաների, համալիրների, համակարգերի և ցանցերի մաթեմատիկական և ծրագրային ապահովում» մասնագիտությամբ տեխնիկական գիտությունների գիտական աստիճանի հայցման ատենախոսության վերաբերյալ

Թ. Ջամոարյանի ատենախոսությունը նվիրված է տեղեկատվական ցանցերում փոխանցվող տվյալների ամբողջականության դեմ հնարավոր գրոհների հայտնաբերմանը՝ օգտագործելով մեքենայական ուսուցմամբ ներխուժման հայտնաբերման համակարգեր: Առաջարկվում է տեղեկատվական ցանցերում, ցանցի միջուկի մակարդակում փոխանցվող տվյալների ամբողջականության խախտման հայտնաբերման համակարգ՝ չարագործի կողմից մեքենայական ուսուցման հիման վրա գրոհի դեպքում:

Ատենախոսությունը, որը բաղկացած է 138 էջերից, ներառում է ներածությունը, չորս գլուխ, 6 հավելված և օգտագործված գրականության ցանկը:

Ներածությունը ներառում է ատենախոսությունը, որը հաստատում է հետազոտության արդիականությունը, ներկայացնում է աշխատանքի նպատակը, ընդգծում գիտական նորարարությունը և կարևորում գործնական նշանակությունը:

Առաջին գլուխը ներկայացնում է գոյություն ունեցող ցանցային ճարտարապետությունները և տարբեր ներխուժման հայտնաբերման համակարգերի վերլուծությունը: Դիտարկվում է ցանցային ենթակառուցվածքի կառուցման երեք մակարդակի հիերարխիկ մոդելը, ցանցային ենթակառուցվածքի դեմ հնարավոր հարձակումները, և գոյություն ունեցող բաց ելակետային կոդով ներխուժման հայտնաբերման համակարգերը: Ձևակերպված են մեքենայական ուսուցմամբ ներխուժման հայատնաբերման համակարգերի հետազոտողների առջև ծառացած հիմնական խնդիրները: Գլուխը ուրվագծում է աշխատանքի նպատակները և բացահայտում հետազոտական խնդիրները, որոնք պետք է լուծվեն այդ նպատակներին հասնելու համար:

Երկրորդ գլխում հեղինակը ներկայացնում է ցանցային ենթակառուցվածքի կայունությունն գնահատելու և դրանում փոխանցվող տվյալների ամբողջականությունը ապահովելու մշակված մաթեմատիկական մոդելը: Մշակվել է ցանցային ենթակառուցվածքում փոխանցվող տվյալների ամբողջականությունն խախտող գրոհի մոդել, չարագործի կողմից մեքենայական ուսուցման մեթոդների կիրառման դեպքում: Ցանցային ենթակառուցվածքում փոխանցվող տվյալների ամբողջականության դեմ գրոհի մոդելը մշակվել է այն ենթադրությամբ, որ չարագործը ունի Դոլեվ-Յաոյի սպառնալիքի մոդելում նկարագրված հնարավորությունները: Մշակվել է նեյրոնային ցանցերը վարժեցնելու համար վնասաբեր ծրագրային ապահովման տվյալների հավաքածուների գեներացնելու ալգորիթմ և ծրագրային ապահովում: Վնասաբեր ծրագրային ապահովման տվյալների հավաքածուների գեներացնելու համար կիրառվել է աուգմենտացիայի և բուստինգի մեթոդները: Բուստինգի մեթոդի ընտրությունը, որպես տվյալների հավաքածուների գեներացման գործիք պայմանավորված է նրանով, որ անհրաժեշտ է

կատարել նախապատրաստվող տվյալների քանակական փոփոխություն՝ առանց ներկայացուցչությունը նվազեցնելու: Կիրառվող մեթոդներում նեյրոնային ցանցերի վերուսուցման հայտնաբերման և ճշգրիտ փոփոխության կատարելու համար (ինչպես նաև հետադարձ ճարտարագետությունը իրականացնելու համար), կատարվել է վնասաբեր ծրագրային ապահովման հեշի և ժամանակի պիտակի գումարների հեշի հաշվարկը:

Երրորդ գլխում ներկայացվում է բազմաչափ լոգիստիկ ֆունկցիայի փոփոխության առաջարկվող լուծումը՝ ցանցային ենթակառուցվածքում փոխանցվող տվյալների ամբողջականության խախտումների հայտնաբերման ճշգրտությունը բարձրացնելու նպատակով: Մշակվել և ուսումնասիրվել է նեյրոնային ցանցերի օգտագործմամբ փոխանցվող տվյալների ամբողջականության խախտումների հայտնաբերման և վնասաբեր ծրագրային ապահովման հայտնաբերման ծրագրային մոդել՝ կիրառելով փոխանցման ուսուցման և հատվածաբար համատեքստային անորոշ հեշավորման մեթոդները: Առաջարկվել է «իրավիճակների մատրիցների» հիման վրա ցանցային ենթակառուցվածքում փոխանցվող տվյալների ամբողջականությունը խախտող վնասաբեր ծրագրային հայտնաբերման մեթոդը: Արդյունքները, ըստ տրված պարամետրերի, համեմատվել են տարբեր ծրագրային և ապարատային-ծրագրային ներխուժման հայտնաբերման համակարգերի հետ:

Չորրորդ գլխում հեղինակը ներկայացրել է մեքենայական ուսուցման միջոցով ներխուժման հայտնաբերման համակարգի հուսալիության բարձրացման մշակված ալգորիթմ և ծրագրային ապահովում: Գնահատվել է մեքենայական ուսուցմամբ ներխուժման հայտնաբերման համակարգի արդյունավետությունը: Առաջարկվել է նեյրոնային ցանցերի վրա հիմնված մեքենայական ուսուցմամբ ներխուժման հայտնաբերման համակարգի հուսալիության բարձրացման խնդրի լուծում: Որպես մաթեմատիկական ապարատ ընտրվել է *k մոտակա հարևանների* մեթոդը: Իրականացվել է նեյրոնային ցանցի ինտեգրումը «Snort» ներխուժման հայտնաբերման համակարգի հետ: Գլուխում ներկայացված են փորձարարական արդյունքներ, որոնք հիմնավորում են առաջարկվող մեթոդների արդյունավետությունը:

Ատենախոսությունը ներկայացված է մանրամասն, սակայն առկա են շարադրման հետ կապված էական թերություններ, և դրանցից ուշագրավ են հետևյալները.

1. Հետազոտության արդիականությունը լիակատար ներկայացված չէ: Մասնավորապես CIA (Confidentiality, Integrity, Availability) անվտանգության մոդելի կիրառման մակարդակը, որն ընդգծում է գաղտնիության, ամբողջականության և տվյալների հասանելիության պաշտպանությունը:
2. Առաջարկվում է բարելավված սպառնալիքների մոդել, սակայն իրականացված չէ բավարար քանակական վերլուծություն լիովին հիմնավորելու մոդելի արդյունավետությունը գոյություն ունեցող տարբեր մոտեցումների և ալգորիթմների հետ:

3. Ուսումնասիրված չեն տվյալների ամբողջականության վրա ցանցային ենթակառուցվածքներում հասանելիության և բաշխման մակարդակներում գրոհները:
4. Ոչ բոլոր նկարները և գրաֆիկներն են պարունակում թվային արժեքներ: Մասնավորապես, 4-րդ գլխում, արդյունավետության գնահատման ժամանակ, չեն նշված արդյունավետության չափականության ելքային արժեքների տեսանելիացման արդյունքները:
5. Գրականության ցանկը պարունակում է բավականին քիչ արդի ուսումնասիրություններ, որոնք վերաբերվում են ցանցային ենթակառուցվածքի, հասանելիության և բաշխման մակարդակի ներխուժման հայտնաբերման համակարգերին:

Այնուամենայնիվ, նշված թերությունները չեն նվազեցնում ատենախոսության արժեքը: Միևնույն ժամանակ աշխատանքն արդիական է, որը ներդրվել Հայաստանի Հանրապետության ՉՈՒ կապի համակարգում ապահովելով ցանցային ենթակառուցվածքում փոխանցվող տվյալների ամբողջականության խախտումների հայտնաբերումը:

Թիմուր Ջամոդյանի ատենախոսությունը համապատասխանում է Ե.13.04 մասնագիտության գծով ներկայացվող թեկնածուական ատենախոսությունների պահանջներին, իսկ հեղինակը արժանի է տեխնիկական գիտությունների թեկնածուի աստիճանի շնորհմանը:

Պաշտոնական ընդդիմախոս՝

ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման

պրոբլեմների ինստիտուտի տնօրեն,

Գիտական հաշվարկների կենտրոնի ղեկավար, տ.գ.դ. Հ.Վ. Ասցատրյան

«19» հունվարի 2024թ.

ՀՀ ԳԱԱ Ինֆորմատիկայի և ավտոմատացման պրոբլեմների ինստիտուտի տնօրեն, գիտական հաշվարկների կենտրոնի ղեկավար, տեխնիկական գիտությունների դոկտոր Հ.Վ. Ասցատրյանի ձեռքի ստորագրությունը հաստատում եմ՝

ՀՀ ԳԱԱ ԻԱՊԻ գիտական քարտուղար Հ. Սահակյան