ԷԼԵԿՏՐԱՄԱԳՆԻՍԱԿԱՆ ՃԱՌԱԳԱՅԹՄԱՆ ԱՐԴՅՈՒՆՔՈՒՄ ՀԱՅՏՆԱԲԵՐՎԱԾ ԱՐՏԱՔԻՆ ՄԻՋՈՑՆԵՐԻ ԿԻՐԱՌՄԱՄԲ ՑԱՆՑԻ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՊԱՀՊԱՆՄԱՆ ՄԵԹՈԴՆԵՐ

ԱՄԻՐԽԱՆՅԱՆ ՍՈՒՐԵՆ
ՀԱՊՀ ԷԷ ինստիտուտի
կենսագործունեության անվտանգության
և արտակարգ իրավիճակների
ամբիոնի լաբորատորիայի վարիչ
էլփոստ՝ amirkhanyansuren@yandex.ru

Ժամանակակից տեղեկատվական համակարգերը հիմնված են հեռահաղորդակցման տեխնոլոգիաների օգտագործման վրա, և այսօր ամենաարդիական հարցերից մեկը տարբեր սպառնալիքների պայմաններում համակարգչային ներքին ցանցի կայուն գործունեության ապահովումն է:

Ցանցային պաշտպանության ոլորտում գոյություն չունի սպառնալիք լուծում: Ցանցային պաշտպանության հիմնական մոտեցումը ընկերություններում համարվում է պաշտպանիչ էկրանի կիրառումը կամ, ինչպես նրանց անվանում են, Brandmauer-ը կամ Firewall-ը:

Հիմնականում կայուն ցանց ունենալու համար անհրաժեշտ են հուսալի ցանցային սարքավորումներ, և ամենակարևոր գերխնդիրներից մեկն է համարվում ներքին ցանցի պաշտպանությունը տարբեր գերկարճհմպուլսային (ԳՃԻ) էլեկտրամագնիսական ճառագայթումներից (ԷՃ), քանի որ ամեն տարի ի հայտ են գալիս առավել հզոր ֆիքսված և մոբիլ ճառագայթներ, որոնք ձևավորում են պարբերական և միանվագ գերկարճ էլեկտրամագնիսական իմպուլսներ, որոնք ունեն ազդող իմպուլսի և տեղեկատվական ազդանշանի տևողության համաչափություն:

Ցանցային անվտանգության խնդիրները պետք է լուծվեն համակարգված: Սա նշանակում է, որ պաշտպանության տարբեր միջոցները (ապարատային, ծրագրային, ֆիզիկական, կազմակերպչական և այլն) պետք է կիրառվեն միաժամանակ և կենտրոնացված վերահսկողությամբ: Բացի դրանից՝ համակարգի բաղադրիչները պետք է «իմանան» միմյանց գոյության մասին, փոխազդեն և ապահովեն պաշտպանությունը ինչպես արտաքին, այնպես էլ ներքին վտանգներից:

Բանալի բառեր՝ *էլեկտրամագնիսական ճառագայթում, ազդանշաններ, դեդեկտորներ, տեղային համակարգչային ցանց, սերվերներ:*

Ցանկացած հաշվողական համակարգի և ցանցի անսարքությունների հսկումն ու արատորոշումը իրականացվում են երկու հիմնական եղանակով՝ ապարատային և ծրագրային, որոնք բովանդակային և իրականացման առումով տարբեր են, բայց միմյանց փոխլրացնող:

Ապարատային միջոցներն ու եղանակները լրացուցիչ սարքավորումներ են պահանջում, հետևաբար ծախսատար են և հիմնականում կիրառվում են մեծ կազմակերպությունների կողմից՝ ապահովելով բարձր արդյունավետություն: Մասնավորապես ապարատային միջոցների կիրառությունը արդյունավետ է հաշվողական ցանցերի հսկման և արատորոշման համար, օրինակ, կիլոմետրերով ձգվող ցանցային մալուխների խոտանների ճշգրիտ տեղը անհրաժեշտ համապատասխան սարքավորմամբ որոշելու դեպքում:

Ծրագրային եղանակների և միջոցների դեպքում հսկումն ու արատորոշումը կատարվում են նախապես մշակված նպատակային ծրագրերի միջոցով, որոնցից առավել տարածվածը թեստային ծրագրերն են: Ի տարբերություն ապարատայինի՝ ծրագրայինն ավելի քիչ ծախսեր, սակայն լրացուցիչ ժամանակ է պահանջում, հետևաբար զիջում է արդյունավետությամբ:

Հաճախ ցանցի անվտանգության և արատորոշման տակ հասկացվում է միայն մալուխային տնտեսության թեստավորումը, որն ըստ էության ներառում է կապի գծերի ֆիզիկական բնութագրերի չափումը:

Մալուխային տնտեսության թեստավորումը, անշուշտ, արատորոշման կարևոր մասն է կազմում, մինչդեռ դա միակը չէ: Գոյություն ունեն այդ նպատակով կիրառվող բազում հատուկ սարքեր, որոնց թվում են մալուխային անալիզատորները կամ սկաներները:

Առավել դժվար գործընթաց է ապարատածրագրային միջոցներում թաքնված թերությունների հայտնաբերումը:

Թաքնված թերությունները ոչ պարբերաբար հայտնվող պատահական թերություններ են, որոնք կարող են երբեմն հայտնվել ամենաանհարմար պահերին: Փոքր ցանցերում թաքնված թերությունները քիչ են արտահայտվում, և դրանց հատուկ ուշադրություն չի դարձվում: Ցանցի ընդլայնմանն ու ծանրաբեռնվածությանը զուգընթաց թաքնված թերությունների կարևորությունը մեծանում է:

Գոյություն ունի թաքնված թերությունների արտահայտման և տեղային ցանցի որակի ճարտարապետական գնահատման երկու հիմնական մոտեցում: Պասիվ արատորոշում և սթրեսային փորձարկում:

Պասիվ արատորոշման դեպքում դիտարկվում են ցանցի կարգավիճակի և վարքի փոփոխությունները: Այս մեթոդը լայն տարածում ունի և իրականացվում է արատորոշող գործիքների և փորձագիտական համակարգի կիրառմամբ:

Սթրեսային արատորոշման դեպքում ստուգվում է ցանցի աշխատունակությունը մեծ ծանրաբեռնվածության և էքստրեմալ պայմաններում:

Դիտարկված մոտեցումները միմյանց փոխլրացնում են: Տեղային ցանցի վատ աշխատանքի տարածված պատճառներից է ցանցում մալուխային տնտեսության ինքնաբուխ զարգացումը, իր ընդլայնման ռազմավարության բացակայության պատճառով: Հաճախ Տեղային ցանցը ստեղծվում է միջոցների կոպիտ տնտեսման պայմաններում, որն ազդում է տեխնիկական որոշումների ընդունման վրա: Ցանցը ոչ մեծ քանակով օգտվողների (30-40) դեպքում աշխատում է առանց ընդհատման: Աստիճանաբար, ցանցի ընդլայնմանը զուգընթաց դժվարություններ են ի հայտ գալիս: Մալուխային համակարգի տարածված թերություններից է էլեկտրական հոսանքի հողանցման ընդհանուր և համակարգիչների համար առանձին սնուցման կետի բացակայությունը:

Քանի որ ցանկացած էլեկտրոնային համակարգի աշխատանք ուղեկցվում է ճառագայթմամբ, ներկայացնենք ցանցային ադապտերների անսարքությունների հայտնաբերման և վերացման մի շարք խորհուրդներ:

1. Ստուգել ցանցային սարքավորման մոնտաժի և կարգավորման ճշտությունը՝ համաձայն արտադրողի ցուցումների: Բացի դրանից՝ ծանոթանալ արտադրողի կողմից տրամադրված տեղեկությանը ցանցային հարթակի մասին ըստ օպերացիոն համակարգի: Դա կօգնի գտնել սարքի անհամատեղության հետ կապված անսարքությունները:

2. Երբ օգտագործվում է ցանցային ադապտեր PCI շինայի վրա, համոզվել, որ թույլատրված է տվյալների հաղորդման կառավարումը PCI շինայով:

3. Ստուգել ցանցային մալուխի հուսալի կապը ցանցային ադապտերի և ցանցի այլ մասերի հետ: Հարկ եղած դեպքում փոխել մալուխը:

4. Համոզվել, որ մալուխի տեսակը համապատասխանում է ցանցային ադապտերի պահանջներին:

5. Համոզվել, որ ցանցային ադապտերի դրայվերը տեղադրված է:

6. Համոզվել, որ օգտագործվում են այն դրայվերները, որոնք տրված են ադապտերի հետ:

7. Եթե քոմփյութերում տեղադրված են ցանցային այլ ադապտերներ, դրանք կարող են կոնֆլիկտի պատճառ հանդիսանալ:

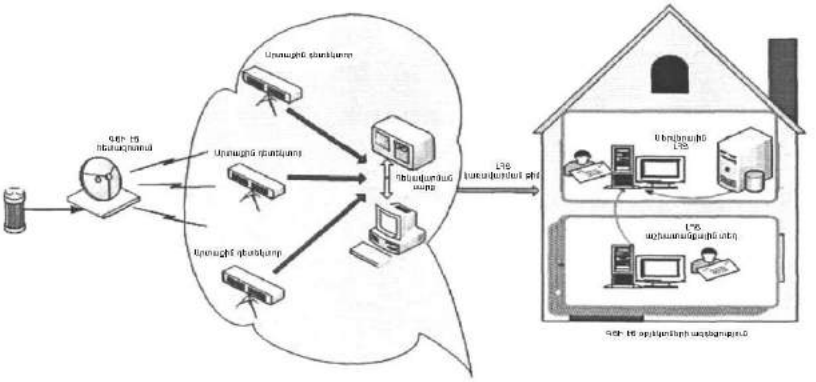
8. Քոմփյութերի վրա օգտագործել BIOS–ի վերջին թողարկումը:

9. Windows միջավայրում ստուգել դրայվերների բեռնավորումը և հղումների տեղադրումը:

Ելնելով վերը թվարկվածներից՝ պետք է նշել ամենակարևորը, որ ցանկացած էլեկտրոնային համակարգի աշխատանք ուղեկցվում է ճառագայթմամբ, և հեռահաղորդակցման տեխնոլոգիաների տարաբնույթ միջոցների կիրառումն էապես մեծացնում է համակարգչային ցանցի աշխատանքի որակի հետ կապված պահանջները:

Այսօր գերխնդիրներից մեկն է համարվում ներքին ցանցի պաշտպանությունը տարբեր գերկարճիմպուլսային (ԳՃԻ) էլեկտրամագնիսական ճառագայթումներից (ԷՃ), քանի որ ամեն տարի ի հայտ են գալիս առավել հզոր ֆիքսված և մոբիլ ճառագայթներ, որոնք ձևավորում են պարբերական և միանվագ գերկարճ էլեկտրամագնիսական իմպուլսներ, որոնք ունեն ազդող իմպուլսի և տեղեկատվական ազդանշանի տևողության համաչափություն (1, էջ 23-37):

ԷՃ-ի ազդեցությունից տեղեկատվության պաշտպանության համար որպես մեթոդ առաջարկվում է օգտագործել արտաքին դետեկտորներ (6, էջ 34-45): Օգտագործվող դետեկտորների համախումբը պետք է լինի ճյուղավորված ցանց, որի բաղադրիչները պետք է տեղաբաշխված լինեն հաղորդակցման գծի երկայնքով և ներքին ցանցի հանգույցներում (նկար 1): Դետեկտորի կողմից ԳՃԻ-ի ազդեցության փաստի ֆիքսման դեպքում դրանից դեպի սարքի տարբեր կողմեր հաղորդվում է ձևավորված տեղեկատվական ազդակ:



Նկար 1. Արտաքին դետեկտորների կիրառում ԳՃԻ ԷՃ ազդեցության բացահայտման համար:

Համապատասխան ազդանշանի առկայության դեպքում ցանցում ԳՃԻ ԷՃ ազդանշանի հայտնաբերման կառավարման սարքը մշակում է կառավարման հրահանգներ, որոնք հաղորդակցման գծերով փոխանցվում են սերվերի տվյալների փոխանցման համակարգ երթուղիչի օգնությամբ: Ընդ որում ներթափանցող կառավարման հրահանգները հաշվի են առնում ցանցի կազմի մեջ մտնող հեռահաղորդակցման բոլոր սարքերի ֆունկցիոնալ առանձնահատկությունները, ինչպես նաև դրանց աշխատանքի հնարավոր խափանումները և դրանց բնույթը: Այդ պատճառով նախապես ԳՃԻ ԷՃ ազդեցության հետ կապված փորձեր են անցկացվել, որոշվել են ցանցի խոցելի տարրերը, և տարբեր տիպի տարրերի չափանիշների մակարդակի հիման վրա տրվել են կառավարման հրահանգներ:

Ընդհանուր առմամբ ուսումնասիրվել են ավելի քան 60 համակարգչային ցանցերի նմուշներ և դրանց հիման վրա աշխատող սարքեր: Հետազոտությունները անցկացվել են ինչպես լաբորատոր պայմաններում, այնպես էլ հետազոտվող օբյեկտներում: Փորձերի ընթացքում հաստատվեց, որ տարրերի խոցելիության մակարդակը կտրուկ նվազում է իմպուլսի տևողության և ճառագայթման ալիքի երկարության մեծացմանը զուգընթաց: Իսկ ինչ վերաբերում է իմպուլսների տրման հաճախությանը, ապա այդ պարամետրը չի հանդիսանում որոշիչ և արդյունքների վրա առավել քիչ ազդեցություն ունի: Աղյուսակ 1-ում և 2-ում ներկայացված են փորձի արդյունքում ստացված տվյալներ ընդհանուր նշանակության սերվերների խոցելիության, ինչպես նաև ճառագայթման ալիքի երկարության և իմպուլսի տևողության

միջև եղած կապով: Այստեղ ներկայացված է նաև համակարգչային ցանցի տարրերի վնասման տոկոսը, որը սահմանվում է որպես փորձի արդյունքում վնասված նմուշների թվի հարաբերություն նմուշների ընդհանուր թվին:

Աղյուսակ 1.

Ազդեցության գործակիցներ	**Ալիքի երկարություն**				
	35սմ	24սմ	17սմ	10սմ	3սմ
ՆԷՄ, Վտ/սմ^2	0,15	0,15	1	2	40
Վնասման տոկոս, %	100	100	100	90	70

Աղյուսակ 2.

Ազդեցության գործակիցներ	**Իմպուլսի տևողություն**		
	70 վրկ	1 վրկ	2,5 վրկ
ՆԷՄ, Վտ/սմ^2	10	3	2
Վնասման տոկոս, %	90	90	90

Լայնածավալ փորձարարական աշխատանքները թույլ են տալիս պարզել համակարգչային ցանցի LAN տարրերի ֆունկցիոնալ վնասման մակարդակը և մշակել համակարգչային ցանցի ամբողջական պաշտպանության կառավարման հրահանգներ:

Ստացված արդյունքների վերլուծությունը թույլ է տալիս եզրակացնել, որ ԳՃԻ ԷՃ–ի ենթարկված սերվերների խափանման պատճառները.

- ✓ Pentium և ավելի ցածր պրոցեսորով սերվերների մոտ խափանվում են տվյալների մուտքագրման սարքերը (ստեղնաշար),
- ✓ Pentium II և բարձր պրոցեսորով սերվերների մոտ խափանվում է կոշտ սկավառակների կրիչների աշխատանքը:

Ընդ որում սերվերի մակարդակով խափանման ի հայտ գալը ընդհանուր առմամբ գործնականում միշտ արտահայտվում է դրա «գործողության ընդհատմամբ», որը հանգեցնում է օպերացիոն համակարգի վերաթողարկման անհրաժեշտության: Սերվերի օպերացիոն համակարգի աշխատանքի ժամանակավոր ընդհատման հրահանգի՝ ժամանակին ընդունման դեպքում

սերվերը պահպանում է իր աշխատունակությունը, և ֆունկցիոնալ համակարգը ընդհանուր առմամբ չի վնասվում: Քանի որ տիպային LAN-երը հիմնականում գտնվում են կառույցների և շենքերի ներսում, ընդհանուր նշանակության համակարգչային ցանցերը ԳՃԻ ԷՃ-ի ազդեցությունից պաշտպանելու առաջարկվող մեթոդների ուսումնասիրության հետ մեկտեղ պետք է հետազոտել նաև շենքերում և կառույցներում ծագող ճառագայթումները: Նմանատիպ կառույցներում էլեկտրամագնիսական դաշտերի առաջացման փորձնական հետազոտությունները ցույց տվեցին, որ 3 ԳՀց և ավելի հաճախականությունների դեպքում աղյուսե կամ երկաթ-բետոնե պատերի էկրանացնող ունակությունը կարող է հասնել տասնյակ դեցիբելների (դԲ): Կառույցներում էլեկտրամագնիսական դաշտերից ներթափանցող 0.3 ԳՀց-ից ոչ մեծ արժեքով ճառագայթումների հետազոտությունը ցույց տվեց, որ դռների և պատուհանների առկայության դեպքում թուլացման իրական մակարդակը նվազում է մինչև 1- 5 դԲ-ով: Օրինակ՝ էկրանացված պահոցում գտնվող LAN տարրերի ԳՃԻ-ի ճառագայթումից հետո սերվերի աշխատունակության խախտում դիտվել է բաց տարածքում՝ 65մ հեռավորության վրա ազդեցության արդյունքում, այլ ոչ թե տիպային կառույցում՝ 20-30մ հեռավորության վրա:

Ուստի համակցելով արտաքին դետեկտորների կիրառմամբ պաշտպանական և էկրանավորման ընդհանուր մեթոդները՝ փաստացի կարելի է խուսափել ԳՃԻ ԷՃ ազդեցության հետևանքներից:

ԳՃԻ ԷՃ–ի ազդեցության ուսումնասիրությունը տեղային համակարգչային ցանցերի տարրերի վրա կարևոր է դրանց աշխատանքին բնորոշ և խափանման ռեակցիային համապատասխան հատուկ հրահանգների մշակման համար: Հաստատված է, որ արագընթաց համակարգերը ավելի հեշտ են ենթարկվում խափանումների: LAN տարրերից, որոնք առավել քիչ են ենթարկվում նկարագրված խափանումներին, երթուղավորիչներն են:

Տեղեկատվության փոխանցման և վերամշակման համակարգերի էլեկտրամագնիսական ճառագայթներով վնասման դեպքում առաջացած խափանումները բերված են աղյուսակ 3-ում:

Աղյուսակ 3.

№	**Խափանման տեսակներ**
1	Տեստային տեղեկատվական փաթեթների մասնակի կորուստ, ցանցային հզորության կրճատում
2	Տեստային տեղեկատվական փաթեթների ամբողջական կորուստ, ցանցային հզորության արգելափակում
3	Երթուղիչի ժամանակավոր արգելափակում
4	LAN կազմի մեջ մտնող սերվերներից մեկի «կախում»
5	LAN կազմի մեջ մտնող սերվերներից մեկի տեղեկատվության մուտքի և ելքի «կախում»

LAN-ի վրա 1,7 ԳՀց հաճախությամբ ԳՃԻ էՃ-ի ազդեցության դեպքում համակարգի աշխատանքի խափանումները ի հայտ եկան հետազոտության արդյունքներին համապատասխան՝ իմպուլսի 15-600 մվտ/սմ^2 մակարդակում:

LAN-ի վրա 3 ԳՀց հաճախությամբ և 0,1-1 մկվրկ տևողությամբ ԳՃԻ էՃ-ի իմպուլսի ազդեցության դեպքում համակարգի խախտումներ դիտվում են իմպուլսի ներուժային էներգիայի մակերևույթի (ՆԷՄ) 0,35-5,0 վտ/սմ^2 մակարդակում:

LAN-ի վրա 10 ԳՀց հաճախությամբ ԳՃԻ էՃ-ի ազդեցության դեպքում համակարգի աշխատանքի խափանումներն ի հայտ եկան հետազոտության արդյունքներին համապատասխան՝ իմպուլսի 6,0-20,0 վտ/սմ^2 մակարդակում:

Փորձի արդյունքների վերլուծությունը թույլ է տալիս հետևություններ անել ուսումնասիրվող համակարգում ճառագայթային ազդեցության ուժային մեխանիզմի վերաբերյալ:

LAN-ի վրա գերլայնաշերտ իմպուլսային ճառագայթման դեպքում դիտվող հիմնական ազդեցություններից է ցանցով տեղեկատվության փոխանցման աղավաղումը:

Անհրաժեշտ է նշել, որ որպես արտաքին դետեկտոր՝ հետազոտությունների ընթացքում օգտագործվել են գծավոր կերպափոխիչներ, որոնք միացված են եղել ցանցի հայտնաբերմանը և կառավարման հրահանգների մշակմանը: «Հայտնաբերման ցանցը» տեղաբաշխվել է համակարգչային ցանցերի տարրերի հետ մեկտեղ ու ԳՃԻ էՃ-ի ազդեցության սկզբում և

մշակվել է կառավարման հրահանգներ LAN-ի ֆունկցիոնալության կառավարման սարքերի ուղղությամբ:

Այսպիսով, այս մեթոդը թույլ է տալիս ժամանակին արձագանքել հեռահաղորդակցման սարքերի, տեղեկատվության պահպանման և վերամշակման համակարգերի և ամբողջ համակարգչային ցանցերի վրա ԳՃԻ ԷՃ-ի աղբյուրների կործանարար ազդեցության սպառնալիքների ի հայտ գալուն: Բացի դրանից՝ հաշվի է առնվում LAN կազմի մեջ մտնող ամեն մի տարրի ֆունկցիոնալ առանձնահատկությունը, որպեսզի առավել արդյունավետ կասեցվի դրա գործողությունը՝ զանգվածային տեղեկատվության մշակման կամ փոխանցման գործընթացի հնարավոր կորուստները և խափանումները հասցնելով նվազագույնի:

Օգտագործված գրականության ցանկ

1. Подосенов С. А., Потапов А. А., Соколов А. А., Импульсная электродинамика широкополосных радиосистем и поля связанных структур, Москва, 2003.
2. Уильяме Т., ЭМС для разработчиков продукции, М., Издательский Дом «Технологии», 2003.
3. Уильяме Т., Армстронг К., ЭМС для систем и установок, М., Издательский Дом «Технологии», 2004.
4. Сахаров К. Ю., Излучатели сверхкоротких электромагнитных импульсов и методы измерений их параметров, Монография, Москва, 2006.
5. Кечиев Л. Н., Пожидаев Е. Д., Защита электронных средств от воздействия статического электричества, М., Издательский Дом «Технологии», 2005.
6. Кечиев Л. Н., Степанов П. В., Арчаков О. Н., Ольшевский А. Н., Электромагнитная совместимость технических средств: проблемы и решения. Московский союз научных и общественных объединений, сборник научно-технических статей, Москва, 2006, с. 34-45.
7. Гусева Ю. А., Кармашев В. С., Кечиев Л. Н., Основы технического регулирования в области ЭМС, М., «Европейский центр по качеству», 2004, 149 с.
8. Акбашев Б. Б., Степанов П. В., Ольшевский А. Н. Современное состояние телекоммуникационных технологий// Сборник научных трудов МИЭМ, под ред. Кечиева Л. Н., 2007, с. 7-15.

NETWORK PROTECTION METHODS THROUGH THE EXTERNAL USE OF ELECTROMAGNETIC RADIATION DETECTION MEANS

AMIRKHANYAN SUREN
Anpu (Fund) sector "Ecology and Life"
EE Institute, Head of laboratory
e-mail: amirkhanyansuren@yandex.ru

Today the use of various telecommunication means, including a new approach to IT technology solutions implies high demands for a quality of work in general. Modern information systems are based on the use of telecommunication environment, therefore there emerges one of the topical issues of sustainable functioning provision of the LAN in a standardization variety.

Key words: *Electromagnetic radiation, signals, detectors, local area networks, servers.*

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТИ НА ОСНОВЕ ПРИМЕНЕНИЯ ВНЕШНИХ СРЕДСТВ ОБНАРУЖЕНИЯ ЭЛЕКТРОМАГНИТНОГО ИЗЛУЧЕНИЯ

АМИРХАНЯН СУРЕН
Заведующий лабораториией
кафедры Экология и безопасность жизнедеятельности института
ЭЭ АНПУ (фонд)
электронная почта: amirkhanyansuren@yandex.ru

На сегодняшний день использовать различные средства телекоммуникации, в том числе новейший подход для решения IT-технологий, предъявляет собой повышенные требования к качеству работы в целом. Современные информационные системы основаны на использовании телекоммуникационной среды, поэтому тут возникает один из актуальных вопросов обеспечения устойчивого функционирования ЛВС в условиях различных стандартизаций.

Ключевые слова: *Электромагнитное излучение, сигналы, детекторы, локальные сети, серверы.*

Հոդվածը ներկայացվել է խմբագրական խորհուրդ 21.08.2021թ.:
Հոդվածը գրախոսվել է 05.11.2021թ.: