ԿՐԻՏԻԿԱԿԱՆ ՈԼՈՐՏՆԵՐԻ (ԵՆԹԱԿԱՌՈՒՑՎԱԾՔՆԵՐԻ) ՆԿԱՏՄԱՄԲ ՄՈՏԵՑՈՒՄՆԵՐԸ ԹՈՒՐՔԻԱՅՈՒՄ

Արեստակես Սիմավորյան
ՀՀ ՊԿԱ ՏՀԿ կրտսեր գիտաշխատող

Տեխնիկական զարգացման ներկա պայմաններում, տարաբնույթ ճգնաժամերի, բնական և տեխնածին աղետների կանխարգելման, ռիսկերի նվազեցմանն ուղղված քաղաքականության մշակման գործում էական նշանակություն են ձեռք բերում կրիտիկական ենթակառուցվածքների պաշտպանության և բարելավման աշխատանքները:

Ենթակառուցվածքի ներքո հասկանում են սպասարկող կառույցների և օբյեկտների մի համալիր ամբողջություն, որը տվյալ համակարգի ֆունկցիոնալության և կենսունակությունն ապահովող բաղադրիչ մասն է: Լայն իմաստով՝ բոլոր այն կառույցների և ցանցերի ամբողջությունը, որն անհրաժեշտ ծառայություններ է մատակարարում զանազան բնագավառներին և տարբեր հանրություններին ու նպաստում է ազգի/պետության ընդհանուր զարգացմանը, սահմանվում է որպես ենթակառուցվածք: Կրիտիկական ենթակառուցվածքները դասակարգվում են ըստ տարբեր չափանիշների: Առավել կարևորվում են տեղեկատվական ենթակառուցվածքները (տեղեկատվության կազմակերպական կառույցների (ենթա)համակարգ(եր), սոցիալական ենթակառուցվածքները (ոլորտների և ձեռնարկությունների ամբողջություն, որն ապահովում է հասարակության կենսագործունեությունը. կրթություն, գիտություն, առողջապահություն և այլն), տրանսպորտային, ռազմական, ինովացիոն և այլ ենթակա-

ռուցվածքներ[11][1]:

Ամեն երկիր, ելնելով իր առանձնահատկություններից, սահմանում է սեփական կրիտիկական ենթակառուցվածքները: Նման աշխատանքներում, սովորաբար, տարբեր երկրներում ներգրավված են հանրային նշանակության կարևորագույն օբյեկտների գործունեությունը համակարգող պետական, որոշ դեպքերում՝ մասնավոր սուբյեկտները: Կրիտիկական ոլորտների և դրանց մեջ մտնող ենթակառուցվածքների պաշտպանության, թարմացման ու արդիականացման, անվտանգության մակարդակի բարձրացման, ֆինանսական ներդրումների ավելացման հետ կապված հիմնահարցերը համեմատաբար վերջերս են հայտնվել Թուրքիայի պետական քաղաքականության ուշադրության կենտրոնում: Կրիտիկական ոլորտների (ենթակառուցվածքների) և դրանց պաշտպանության հարցերը հիմնականում գնահատվել են «ազգային տեղեկատվական անվտանգության» համատեքստում: 1990-ականներից մինչև 2006թ. Տեղեկատվական ավտանգության համակարգված աշխատանքները տարվում էին, և ոլորտի անվտանգության վերաբերյալ օրինագիծն էլ մշակվում էր Ազգային պաշտպանության նախարարության կողմից, որի շրջանակներում նախատեսվում էր տեխնիկական, տեխնոլոգիական և դրանցից ածանցված տասնյակ միջոցառումների իրագործում, սակայն օբյեկտիվ և սուբյեկտիվ պատճառներով տվյալ

11 ԱՄՆ-ում պաշտոնապես առաջին անգամ կրիտիկական ենթակառուցվածքները սահմանվել են 1997թ. հոկտեմբերին Բ. Քլինթոնի նախագահական վարչակազմի կողմից ստեղծված **«Կրիտիկական ենթակառուցվածքների պաշտպանության նախագահական հանձնաժողով»**-ի կողմից: Մասնավորապես հստակեցվեցին 8 բնագավառներ (հեռուստահաղորդակցությունը, էլեկտրահամակարգը, նավթագազային ու ֆինանսաբանկային ոլորտները, տրանսպորտային և ջրամատակարարման համակարգերը, կառավարության գործունեությունը, արտակարգ իրավիճակների ծառայությունը), որոնց պարագայում հանձնաժողովը մատնանշեց, թե վերջիններիս «անվտանգությունը, հարատևությունն ու հասանելիությունն ապահովելուց զատ չկան էլ ավելի կարևոր և հրատապ գերակայություններ»: Հետագայում ավելացան այլ ոլորտներ ևս, հասցնելով դրանք 16-ի: ԱՄՆ 16 կրիտիկական սեկտորների համանմանությամբ՝ Գերմանիայի կառավարությունը սահմանեց իր երկրի կրիտիկական ոլորտներն ու ենթակառուցվածքները՝ փոխադրամիջոցներ և տրանսպորտային հոսքեր, էներգետիկ համակարգ, IT և հեռահաղորդակցություն, ֆինանսական և ապահովագրական հատված, հանրային կառավարման հատված, սննդամթերքի հատված, ջրամատակարարման և հարակից ոլորտներ, առողջապահություն, ՋԼՄ-ն և մշակույթ[1]:

օրենսդրական նախագիծը հավանության չի արժանացել:

2012թ. Թուրքիայի գիտատեխնիկական հետազոտությունների խորհրդի (TÜBİTAK) ներգրավմամբ, Տրանսպորտի և ենթակառուցվածքների նախարարության հովանավորությամբ՝ Զարգացման նախարարության ներդրումային ծրագրերին նվիրված «Կրիտիկական ենթակառուցվածքների տեղեկատվական անվտանգության կառավարման նախագիծ»-ով ակտուալ դարձավ կիբեռանվտանգության հարցը՝ ենթակառուցվածքների պաշտպանության տեսանկյունից: Նույն թվականին ստեղծվեց **Կիբեռանվտանգության խորհուրդը** (խորհրդի անդամները ներկայացնում են գրեթե բոլոր պետական հաստատությունները), որն առաջին իսկ համաժողովին ընդունեց «Ազգային կիբեռանվտանգության ռազմավարությունը և 2013-2014թթ. գործողությունների պլանը», որի համաձայն՝ առաջին փուլի համար սահմանվեցին կիբեռանվտանգության հետ անմիջականորեն փոխկապակցված և միմյանց վրա փոխազդող հիմնական խոցելի ոլորտներ, որոնք են՝

1. տրանսպորտային,
2. էներգետիկ,
3. էլեկտրոնային կապ,
4. ֆինանսաբանկային,
5. ջրային ռեսուրսների կառավարում,
6. հանրային ծառայությունների (կրիտիկական)[12] [2]:

Սահմանելով և հաշվի առնելով վերը հիշատակված ոլորտները՝ Տրանսպորտի և ենթակառուցվածքների նախարարության կողմից հրապարակվեց «Ազգային կիբեռանվտանգության ռազմավարություն և 2016-2019 թթ. գործողությունների պլան» նոր նախագիծը, որտեղ գնահատվել են հիմնական սպառնալիքներն ու համակարգի հետ կապված ռիսկերը (մասնավորապես՝ ներքին և անդրսահմանային կիբեռհարձակումներ և այլն), նաև մասնակիորեն դրանց անվտանգության մակարդակի բարձրացմանն ուղղված այնպիսի ռազմավարական նպատակներ, ինչպիսիք են կրիտիկական ենթա-

12 Հարկ է նշել, որ Կիբեռանվտանգության խորհրդի անդամները ներկայացնում են գրեթե բոլոր պետական հաստատությունները:

կառուցվածքների ինվենտարիզացիան և պաշտպանությունը, կիբեռհանցագործությունների դեմ պայքարի ուժեղացումը, կիբեռանվտանգության էկոհամակարգի զարգացումը, կադրերի (վերա)պատրաստումը, կիբեռանվտանգության ինտեգրումն ազգային անվտանգությանը, տեղեկատվական-հաղորդակցական տեխնոլոգիաների նորացումը և հարակից այլ հարցեր [3]: Վերոհիշյալ ոլորտների հետ կապված առաջադրանքների և բուն աշխատանքների իրագործման գլխավոր պատասխանատուներն են մի շարք գերատեսչական մարմիններ (դրանց թվում են գրեթե բոլոր ուժային կառույցները) և ենթակառուցվածքների անվտանգությունն ապահովող առանձին ստորաբաժանումներ:

Կրիտիկական ենթակառուցվածքների կարևորագույն բնութագրիչներից է կիբեռփոխկախվածությունը, որը համատարած համակարգչայնացման հետևանք է: Այդ իսկ պատճառով ինչպես այլ երկրներում, այնպես էլ Թուրքիայում կարևորվում է կիբեռ-կրիտիկական ենթակառուցվածքներ փոխկախվածության հարցը: Ստորև բերենք մի քանի օրինակներ, որոնք զգալի վնասներ են հասցրել Թուրքիայի կրիտիկական ոլորտներին՝

1. 2008 թ. `Բաքու-Թբիլիսի-Ջեյհան նավթամուղի պայթյուն,
2. 2009թ.՝ կիբեռհարձակում Աթաթյուրքի անվան օդանավակայանի համակարգիչների վրա,
3. 2015թ.՝ էլեկտրամատակարարման զանգվածային խափանում Թուրքիայի 79 նահանգներում: Կատարվածը գնահատվել է 1999թ. երկրաշարժից հետո էլեկտրամատակարարման ամենամասշտաբային խափանումը: Հոսանքազրկման հետևանքով երկիրը մեկ ժամվա ընթացքում ունեցել է 100 մլն ԱՄՆ դոլարի կորուստ:
4. 2015թ.՝ տաս օր տևողությամբ կիբեռհարձակումներ պետական հաստատությունների, նոտարական գրասենյակների և բանկերի կայքերի վրա,
5. 2016թ.՝ Կիբեռհարձակում առողջապահության նախարարության ենթակայության ներքո գործող բուժհաստատությունների համա-

կարգիչների վրա, որի արդյունքում հափշտակվել են հիվանդների բժշկական ապահովագրության և բժշկական ծառայություններ մատուցող մասնագետների վերաբերյալ տեղեկատվական բազաները, որից հետո ցանցահենները ոչնչացրել են համակարգիչներում առկա ողջ տեղեկատվությունը:

6. 2017թ.՝Կիբեռհարձակում թուրքական «Turcas Petrol» էներգետիկ ընկերության համակարգիչների վրա ռուսական «Էներգետիկ արջ» կիբեռխմբի կողմից: Ցանցահենները հնարավորություն են ստացել հափշտակել էներգետիկ կրիտիկական ենթակառուցվածքների պաշտպանության գծով հաշվառված մասնագետների տվյալները:

Կրիտիկական ոլորտների ռիսկերը: Թուրքիայի Աղետների և արտակարգ իրավիճակների կառավարման վարչության շրջանակներում գործող տեխնոլոգիական աղետների ռիսկերի նվազեցման աշխատանքային խմբի կողմից 2014թ. հրապարակվեց նաև Թուրքիայի «2014-2023 թթ. կրիտիկական ենթակառուցվածքների պաշտպանության ճանապարհային քարտեզ» զեկույցը [4]: Համաձայն զեկույցի՝ Թուրքիայի կրիտիկական ոլորտներ են համարվում էներգետիկան, կիբեռ ու կապի տեխնոլոգիաների ոլորտները, տրանսպորտային (ծովային և ցամաքային) կոմունիկացիաները, մշակույթն ու տուրիզմը, ջրային ռեսուրսների կառավարման հատվածը (ջրամբարների պաշտպանությունը), ֆինանսաբանկային և առողջապահության համակարգը, գյուղատնտեսությունը և սննդամթերքի անվտանգությանն առնչվող (ենթա)ոլորտները, բարձր տեխնոլոգիաների և հանրային պաշտպանության (կրիտիկական) բնագավառները:

Այս ոլորտների արդյունավետության վրա ազդող սպառնալիքների (աղետների) աղբյուր են համարվում՝

1. բնական՝ երկրաբանական, օդերևութաբանական, բիոլոգիական երևույթները,
2. մարդկային գործոնով պայմանավորված վտանգներ՝ տեղեկատվական պատերազմ, կիբեռհանցագործություններ, միջազգային և տեղական մասշտաբների ահաբեկչական գործողություններ,

տրանսպորտային խոշոր պատահարներ, տեխնոլոգիական վտանգներ և այլն:

Դրանց առկայությամբ պայմանավորված՝ առաջանում են միկրո և մակրոմակարդակների աղետներ՝ ազդելով ենթակառուցվածքների վրա ու խաթարելով դրանց կենսագործունեությունը, ընդ որում՝ նման իրավիճակներում միմյանց հետ փոխկապակցված ենթակառուցվածքներից մեկի խափանումը կարող է ազդել մյուսների վրա: Նման աղետներից են՝

1. բնական՝ երկրաշարժեր, սողանքներ, ջրհեղեղներ, ձյունահյուսեր,
2. տեխնածին՝ խոշոր արդյունաբերական համալիրների, ռադիոակտիվ և միջուկային խնդիրներով պայմանավորված, ծովային և ցամաքային (երկաթուղային) տրանսպորտային հանգույցների, վտանգավոր նյութերի տրանսպորտային փոխադրման հետ կապված աղետներ, էկոլոգիական (կլիմայական փոփոխություններ) աղետներ և այլն[13] [5]:

Ակնհայտ է, որ նման աղետները կարող են հանգեցնել ենթակառուցվածքների քայքայմանը, ազդել կոորդինացիոն և օպերատիվ գործողությունների վրա և անգամ կարճաժամկետ կամ երկարաժամկետ կտրվածքով հանգեցնել համակարգային փլուզմանը: Հաշվի առնելով այդպիսի հնարավոր զարգացումներից եկող ռիսկերը՝ կրիտիկական ենթակառուցվածքների սահմանման և անվտանգության հարցերը դրված են Թուրքիայի այն պետական կառույցների վրա (դրանք հիմնականում պետական հաստատություններ են),

13 Թուրքիայի կառավարությանն առընթեր Աղետների և արտակարգ իրավիճակների կառավարման վարչության շրջանակներում ոլորտ առ ոլորտ գնահատված են թվարկված աղետների առաջացման հետևանքով ի հայտ եկող ռիսկերը, հնարավոր զարգացումներն ու դրանց հետ առնչություն ունեցող ենթակառուցվածքների բարելավման հիմնահարցերը:

որոնք պատասխանատու են իրենց ոլորտների համար[14] [1]:

Համաձայն Աղետների և արտակարգ իրավիճակների կառավարման վարչության զեկույցի՝ այդ շրջանակների մեջ են մտնում հետևյալ կառույցները՝

1. էներգետիկ ոլորտ՝ Թուրքիայի միջուկային էներգետիկայի կազմակերպություն, Էներգետիկայի նախարարություն, Էներգետիկ շուկայի կարգավորման կազմակերպություն,
2. տրանսպորտային ոլորտ՝ Տրանսպորտի և ենթակառուցվածքների նախարարություն,
3. կապի ոլորտ՝ Տեղեկատվական տեխնոլոգիաների և կապի հաստատություն, Տրանսպորտի և ենթակառուցվածքների նախարարություն,
4. ջրային ռեսուրսների կառավարում՝ Գյուղատնտեսության և անտառտնտեսության նախարարություն,
5. ֆինանսաբանկային ոլորտ՝ Գանձապետարանի և ֆինանսների նախարարություն, Թուրքիայի կապիտալի շուկաների խորհուրդ, Բանկային գործերի կարգավորման և վերահսկողության գործակալություն,
6. հանրային պաշտպանության ոլորտ՝ Ներքին գործերի նախարարություն,
7. առևտրաարդյունաբերական ոլորտ՝ Արդյունաբերության և տեխնոլոգիաների նախարարություն, Առևտրի նախարարություն, Թուրքիայի պալատների և բորսաների միություն,
8. առողջապահության ոլորտ՝ Առողջապահության նախարարություն,
9. մշակույթ և տուրիզմ՝ Մշակույթի և զբոսաշրջության նախարարություն,

14 Համաձայն մասնագետների՝ կրիտիկական ենթակառուցվածքներին վերաբերող գործառույթները և մասնագիտական պատասխանատվությունը ցրված են տարբեր կառույցների միջև: Օրինակ՝ Չինաստանում կրիտիկական ենթակառուցվածքների պաշտպանության ոլորտում բացակայում է որևիցե համագործակցություն պետական և մասնավոր դերակատարների միջև, իսկ Գերմանիայում դրանց անվտանգության ապահովման հիմքում ընկած է պետության և մասնավոր հատվածների համագործակցության սկզբունքը:

10. գյուղատնտեսության ոլորտ՝ Գյուղատնտեսության և անտառտնտեսության նախարարություն:

Վերը թվարկված հաստատություններն, ըստ էության, իրենց իրավասությունների շրջանակներում պետք է նպաստեն նաև ենթակառուցվածքների կատարելագործմանը ինչպես ոլորտներում նորագույն տեխնոլոգիաների ներդրմամբ, անհրաժեշտ քանակի և անվտանգության մշակույթին (safety culture) տիրապետող, որակյալ մասնագիտական ուժերի (վեր)ապատրաստմամբ և կազմավորմամբ, այնպես էլ ենթահամակարգերի զարգացմամբ և պաշտպանունակության բարձրացմամբ:

Միևնույն ժամանակ բազմաթիվ գիտահետազոտական և ակադեմիական հաստատություններ իրենց գիտաստեղծագործական, վերլուծական աշխատանքներով և գործնական առաջարկություններով մասամբ աջակցում են կրիտիկական, խոցելի համարվող ենթակառուցվածքների սահմանման, ռիսկերի նվազեցման և այլ հարցերին [6]: Այս համատեքստում առանձնահատուկ է Թուրքիայի գիտատեխնիկական հետազոտությունների խորհրդի դերը գիտատեխնոլոգիական քաղաքականության ռազմավարական մշակման և պլանավորման գործում: Խորհրդին կից գործող Կիբեռանվտանգության ինստիտուտի կրթական ծրագրի (կիբեռանվտանգության կրթական պորտալ) միջոցով իրականացվում է համակարգչային տեխնոլոգիաների, տեղեկատվական հոսքերի կոնտենտ վերլուծությունների, նաև կիբեռկախվածության մեջ գտնվող կրիտիկական ենթակառուցվածքների պաշտպանության ոլորտների համար մասնագիտական կազմի պատրաստում [7]: Նշենք, որ Թուրքիայի Քադիր Հաս համալսարանում 2018 թ.-ից գործում է կիբեռանվտանգության և կրիտիկական ենթակառուցվածքների պաշտպանության կիրառական և հետազոտական նշանակության գիտաուսումնական կենտրոն [8]:

Ամփոփելով նշենք, որ կրիտիկական ոլորտների հիմնախնդիրները Թուրքիայի պետանվտանգության մասն են կազմում և հետևաբար գտնվում են երկրի բարձրագույն իշխանությունների ուշադրության կենտրոնում, համապատասխան կառույցների կողմից սահ-

մանվում և գնահատվում են խոցելի ենթակառուցվածքները, դրանց մեջ մտնող օբյեկտների քանակը, դրանց փոխազդեցությունները և անվտանգային սպառնալիքները: Հարկ է նաև արձանագրել, որ կրիտիկական ենթակառուցվածքների պաշտպանությանն ուղղված ռազմավարական քայլերի իրագործման ճանապարհին կիրառվում է միջազգային փորձը՝ հաշվի առնելով Թուրքիայի յուրահատկությունները:

ԳՐԱԿԱՆՈՒԹՅՈՒՆ

1. Հարությունյան, Գ., Մարջանյան, Ա., Վերանյան, Կ., Սիմավորյան, Ա., Հովյան, Վ., Մանուկյան, Ս., Թևիկյան, Ա. (2018). *Critical Infrastructures and National Security [Կրիտիկական Ենթակառուցվածքներ Եւ Ազգային Անվտանգություն]*.էջ 308-352:
2. URL: http://www.resmigazete.gov.tr/eskiler/2012/10/20121 020-18-1.pdf.
3. 2016-2019 Ulusal siber güvenlik stratejisi, URL: http://www.udhb. gov.tr/doc/siberg/2016-2019guvenlik.pdf.
4. 2014-2023. Kritik Altyapıların Korunması. Yol Haritası Belgesi. URL: https://www.afad.gov.tr/upload/Node/3910/xfiles/kritikaltyapi- son.pdf
5. URL: https://www.afad.gov.tr/tr/3498/Kurumsal-Raporlar
6. Միջազգային ռազմավարական հետազոտությունների կազմակերպության իրականացրած Թուրքիայի էներգետիկ ոլորտի կրիտիկական ենթակառուցվածքների անվտանգության հարցերին նվիրված հետազոտական զեկույցը: Hasan Selim Özertem, Arzu Celalifer Ekinci, Betül Buke Karaçin. Kritik Enerji Altyapı Güvenliği Projesi Sonuç Raporu. URL: https://www.jstor.org/stable/ resrep14227
7. Siber güvenlik eğitim kategorileri, URL: https://egitim.sge.gov.tr/
8. URL: http://www.khas.edu.tr/news/1754