7. ԿՐԻՏԻԿԱԿԱՆ ԵՆԹԱԿԱՌՈՒՑՎԱԾՔՆԵՐ. ՈՐՈՇ ԵՐԿՐՆԵՐԻ ՓՈՐՁԸ

7.1 Ենթակառուցվածք. հասկացությունը, սահմանումները և տիպերը

Ենթակառուցվածք (*инфраструктура, infrastructure)* եզրը ծագում է հին հունարեն «անդր/ենթա» և «կառուցվածք» բառերի համակցությունից, իսկ մասնագիտական շրջանակներում այն սկսեց կիրառվել 20-րդ դարում: Եզրույթի լայն բովանդակային մեկնությունը, ինչպես նաև տերմինի համատեքստային կիրառման փորձը ենթադրում է ժամանակակից հասարակության և պետության՝ որպես համակարգի անընդհատ բարդացող կենսապահովման միջավայրի գոյությունը: Ենթակառուցվածքի ներքո հասկանում են սպասարկող կառույցների և օբյեկտների մի համալիր ամբողջություն, որը տվյալ համակարգի ֆունկցիոնալության և կենսունակությունն ապահովող բաղադրիչ մասն է հանդիսանում: Անգլերեն լեզվում այն սկսեց գործածվել 1920-28թթ. և ի սկզբանե կիրառվում էր ռազմական ոլորտի պարագայում՝ որպես զինված ուժերի գործունեությանն օժանդակող/ապահովող կառույցների (շինությունների) փոխկապակցված միասնականություն: Ռուսերենում ենթակառուցվածք եզրն ավելի հաճախ գործածվում և ընկալվում է իբրև կառավարման համակարգերի, կապի և տարաբնույթ հաստատությունների և ձեռնարկությունների ամբողջություն, որը կոչված է ապահովե-

լու հասարակության (կամ հասարակության ինչ-որ մի հատվածի) կենսագործունեությունը: Մասնագետների կարծիքով՝ գործնականում ենթակառուցվածքն ավելի դյուրին է մատնանշել, քան նկարագրել այն [1, p. 50]:

Լայն իմաստով՝ բոլոր այն կառույցների և ցանցերի ամբողջությունը, որն անհրաժեշտ ծառայություններ է մատակարարում զանազան բնագավառներին և տարբեր հանրույթներին, ու նպաստում է ազգի/պետության ընդհանուր զարգացմանը, սահմանվում է որպես ենթակառուցվածք:

Ենթակառուցվածքները դասակարգվում են ըստ տարբեր չափանիշների (օրինակ՝ ընդհանրական առումով դրանք կարող են լինել նյութական և սոցիալական), բայց 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 ենթակառուցվածքներ [1, p. 51]:

Հայտնի է, որ տնտեսական աճն ու ենթակառուցվածքը սերտորեն փոխկապված են և ներազդում են միմյանց վրա: Օրինակ՝ 1% ենթակառուցվածքային հավելումը բոլոր երկրների դեպքում բերում է ՀՆԱ 1% աճի [2]:

Կրիտիկական ենթակառուցվածք. տիպեր և փոխկախվածության տեսակներ. Կրիտիկական ենթակառուցվածքների պաշտպանվածության ապահովումը որպես այդպիսին արտացոլում է ազգային անվտանգության ապահովման մի շարք չափումներ: Դրանք տարբերվում են անմիջական կամ (արտաքին)

օտարերկրյա ուղղակի սպառնալիքների՝ արդեն ավանդական դարձած պաշտպանության կամ անմիջական հակադարձման տրամաբանությունից՝ թե՛ հայեցակարգային և թե՛ գործնական մեխանիզմների օգտագործման առումներով: Կրիտիկական ենթակառուցվածքների պարագայում առաջին հերթին կարևորվում է վերջիններիս «դիմադրողականության» բնութագրիչը, որն, ի թիվս այլոց, ենթադրում է հարձակման/վնասի պարագայում՝ ֆունկցիոնալության հարաբերականորեն արագ վերականգնում, վնասի նվազեցման մեխանիզմների առկայություն, այլընտրանքային միջոցների և ռեսուրսների օգնությամբ՝ վերականգնման նոր եղանակների ներդրում: Ի տարբերություն նախորդ դարաշրջանի, երբ հիմնական սպառնալիքներն ու վտանգները կապված էին արտաքին դերակատարների, առաջին հերթին՝ պետական միավորներից ծագող ագրեսիվ և նախահարձակ նկրտումների հետ, ժամանակակից սպառնալիքները պարունակում են «ավելի տարրալուծված և անորոշ բնույթի ռիսկեր, որոնց առանձնահատկությունն է թշնամու հստակ ախտորոշման դժվարությունը»[1]: Կրիտիկական ենթակառուցվածքները՝ որպես ժամանակակից պետության և հասարակության անվտանգային սպեկտրի կարևորագույն բաղադրիչներ, հայտնվել են հենց այդ կարգի ռիսկային համադրույթի թիրախում, երբ հակառակորդի միանշանակ կամ անմիջական հավաստանշումը վերածվել է բավականաչափ բարդ գործի:

Օրինակ, ԱՄՆ-ում, ի տարբերություն «սովորական» կամ «ավանդական» ենթակառույցների՝ կրիտիկական նշանակություն կրող ենթակառուցվածք է համարվում «փոխկախված

[1] *McAveLty,* 'Critical Information Infrastructure: Vulnerabilities, Threats and Responses', UNIDIR Disarmament Forum, no. 3, 2007, pp. 15–22.

ցանցերի և համակարգերի շրջանակը, որը ներառում է որոշակի ինդուստրիալ միավորներ, ինստիտուտներ (ներառյալ՝ մարդկանց ու ընթացակարգեր) և բաշխիչ կարողություններով օժտված ակտիվներ, որոնք ապահովում են ինչպես ԱՄՆ պաշտպանության և տնտեսական անվտանգության ապահովման տեսանկյունից խիստ էական ապրանքների և ծառայությունների անխափան մատակարարումը, այնպես էլ կառավարության և ողջ հասարակության գործունեության հենքը»[2]:

ԳԴՀ-ն նույնպես հայեցակարգային և օրենսդրական մակարդակով սահմանում է կրիտիկական ենթակառուցվածքները՝ «կազմակերպական և ֆիզիկական կառույցներ, որոնք այն աստիճան կենսական կարևորություն ունեն հասարակության և տնտեսության համար, որ նրանց խաթարումը կամ դեգրադացիան կարող է հանգեցնել (…) հանրային անվտանգության և ապահովության նշանակալի վատթարացման, կամ այլ դրամատիկ հետևանքների» [3, p. 4]:

ԱՄՆ-ում առաջին պաշտոնական փորձը՝ սահմանելու կրիտիկական ենթակառուցվածքներն ու ըմբռնելու դրանց կարևորության ընդհանուր շրջանակն ու պարամետրերը, վերագրվում է 1997թ. հոկտեմբերին Բ.Քլինթոնի նախագահական վարչակազմի կողմից ստեղծված Կրիտիկական ենթակառուցվածքների պաշտպանության նախագահական հանձնաժողովին *(PCCIP):* Առաջին հերթին հստակեցվեցին այն 8 բնագավառները (սեկտորները), որոնց պարագայում հանձնաժողովը մատնանշեց, թե վերջիններիս «անվտանգությունը, հարատևությունն ու

[2] Presidential Policy Directive -- Critical Infrastructure Security and Resilience, PRESIDENTIAL POLICY DIRECTIVE/PPD-21, Feb. 12, 2013,
https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

հասանելիությունն ապահովելուց զատ չկան էլ ավելի կարևոր և հրատապ գերակայություններ»[3]: Այդ ութ բնագավառներն էին.

- հեռուստահաղորդակցությունը,
- էլկտրահամակարգը,
- բնական գազն ու նավթը,
- բանկային ոլորտն ու ֆինանսները,
- տրանսպորտային համակարգը,
- ջրամատակարարման համակարգը,
- կառավարության գործունեությունը,
- արտակարգ իրավիճակների ծառայությունը:

Հետագայում, արդեն Ջ.Բուշի և Բ.Օբամայի վարչակազմերի օրոք, բնագավառների թիվն ու ընդգրկումն ընդլայնվեցին. ներկայում 16 սեկտոր է ընդգրկված ԱՄՆ կրիտիկական ենթակառուցվածքների մեջ. ի հավելումն նախորդների, ցուցակում հայտնվել են քիմիական արտադրության ոլորտը, կրիտիկական նշանակության արտադրանքը, միջուկային ռեակտորներն ու վառելիքը (էներգետիկ ոլորտից զատ), պաշտպանության ինդուստրիալ ակտիվները, առողջապահությունը, սննդամթերքն ու գյուղատնտեսությունը և տեղեկատվական տեխնոլոգիաները[4]:

Պաշտպանության և անվտանգային հարցերով ամերիկյան հետազոտողները մատնանշում են, որ բոլոր վերոհիշյալ (կրիտիկական) ենթակառուցվածքներն ըստ էության փոխակերպվող համակարգեր են այն առումով, որ վերջիններս օժտված են ինչպես «ուսանելու», այնպես էլ որոշակի «համակարգային հիշողություն» ձևավորելու կարողություններով: Վերջիններս՝

[3] President's Commission on Critical Infrastructure Protection, Critical Foundations: Protecting America's Infrastructures (1997), www.ciao.org
[4] Department of Homeland Security: https://www.dhs.gov/critical-infrastructure-sectors

որպես համալիր և բարդ համակարգեր, բաղադրիչների սովորական հանրագումար չեն, այլ բարդ երևույթ են՝ օժտված ինքնակենսունակության ապահովման որոշակի ալգորիթմներով, որոնց հիմքում կարող է ընկած լինել ինչպես մարդկային «գործոնը», այնպես էլ իներցիոն բնույթի հանգամանքներ, որոնք կարող են պայմանավորված լինել արհեստական ինտելեկտի գործարկմամբ:

Փոխկախվածության գործոնը և փոխկախվածության տիպերը. Իբրև համալիր բնույթի երևույթ՝ կրիտիկական ենթակառուցվածքների կարևորագույն բնութագրիչներից են փոխկապվածությունը («համակարգերի համակարգ», *«system of systems»*) և փոխկախվածությունը: Առավել պարզ՝ երկկողմանի կախվածությունը ենթադրում է մի իրողություն, երբ երկու ենթակառուցվածքներ փոխկախված են միմյանցից: Գործնականում, սակայն, նման կարգի փոխկախվածություններն էապես բարդացնում են ողջ համակարգի գործունեությունը: Առանձնացնում են փոխկախվածությունների չորս չափում՝ ֆիզիկական, կիբեռ, աշխարհագրական և տրամաբանական փոխկախվածություններ [4, pp. 14-16]:

Ենթակառուցվածքների ֆիզիկական փոխկախվածության ներքո հասկանում են մի իրավիճակ, երբ մեկ ենթակառուցվածքի արտադրանքը/վերջնարդյունքը հանդիսանում է մեկ այլ ենթակառուցվածքի գործունեության համար անհրաժեշտ ռեսուրս, որի բացակայության պարագայում վերջինը չի կարող ապահովել իր արտադրանքը/վերջնարդյունքը: Օրինակ, երկաթգիծն ու ջերմաէլեկտրակայանը ֆիզիկական փոխկախվածության մեջ են գտնվում միմյանցից: Երկաթգծի միջոցով մատակարարվում են ածուխ և անհրաժեշտ սարքավորումներ ջեր-

մաէլեկտրակայանի կողմից էլեկտրաէներգիայի գեներացման համար, բայց երկաթգիծն իր հերթին կախված է էլհոսանքից (երկաթգծային ազդանշաններ և այլն)՝ իր անխափան աշխատանքն ապահովելու համար:

Կիբեռֆոխկախվածությունը հարաբերականորեն նոր երևույթ է. այն, առաջին հերթին, վերջին տասնամյակների ընթացքում համատարած համակարգչայնացման հետևանք է: Ենթակառուցվածքը կիբեռկախվածության մեջ է գտնվում, երբ վերջինիս գործունեությունը կախված է տեղեկատվական ենթակառուցվածքի միջոցով տեղեկատվության փոխանցումից: Հայտնի է, որ շատ համակարգեր վերահսկվում, կարգավորվում և կառավարվում են ավտոմատացված տեղեկատվական մեխանիզմների միջոցով. համապատասխանաբար՝ տեղեկատվական ենթակառուցվածքի արտադրանքից (ինֆորմացիա) է կախված մյուս ենթակառուցվածքների (այդ թվում նաև կրիտիկական) գործունեությունը: Այս իմաստով, տեղեկատվական հոսքերը վերածվում են ենթակառուցվածքների միջև փոխանցվող/փոխանակվող հիմնական «ապրանքի»:

Աշխարհագրական փոխկախվածության չափումը ենթադրում է տեղայնացմամբ պայմանավորված մի իրավիճակ, երբ տարբեր ենթակառուցվածքներում տեղի ունեցող փոփոխությունները հանգեցնում են փոփոխությունների մեկ այլ ենթակառուցվածքում, որի պատճառն է տարածական մերձավորությունը: Օրինակ, կամուրջներով անցնող էլեկտրական, տեղեկատվական, ֆիբերօպտիկական կամ հաղորդակցության այլ մալուխները ֆիզիկապես կամ կիբեռկախվածության առումով ուղղակի կապի մեջ չեն գտնվում կամուրջներով անցնող տրանսպորտային հոսքերի հետ: Սակայն տրանսպորտային

խափանումը կարող է հանգեցնել նույն կամրջի միջոցով իրականացվող կոմունիկացիոն հոսքերի խափանման՝ հաշվի առնելով երկու տիպի ենթակառուցվածքների աշխարհագրական/տարածական մոտիկության հանգամանքը:

Տրամաբանական փոխկախվածությունը վերահսկման համադրույթի հետ կապված երևույթ է, երբ մեկ ենթակառուցվածքի բաղադրիչը կապված է մեկ այլ ենթակառուցվածքային բաղադրիչի հետ՝ առանց որևէ ֆիզիկական, կիբեռ- կամ աշխարհագրական մեկտեղման: Այսպես, ապակենտրոնացման քաղաքականությունը կամ մրցակցության խթանմանը միտված քայլերը էներգետիկայի ոլորտում (օրինակ՝ էլցանցերի սեփականության տարանջատումը էկեկտրականություն գեներացնող հզորություններից) կարող է բերել լուրջ խնդիրների ֆինանսական համակարգում՝ հանգեցնելով ներդրումային քաղաքականության փոփոխությունների (թե՛ դրական, թե՛ բացասական): Ենթակառուցվածքների տրամաբանական փոխկախվածության մեկ այլ օրինակ. ամառային ամիսներին կամ հանգստյան ժամանակահատվածում ամերիկյան բենզալցակայաններում կարող են մեծ հերթեր առաջանալ, որոնք, իրենց հերթին, հանգեցնում են տրանսպորտային խցանումների: Երկու ենթակառուցվածքները փոխկապված չեն միմյանց հետ ոչ ֆիզիկապես, ոչ կիբեռ- և ոչ էլ աշխարհագրական կապերով, բայց պայմանավորված է ամերիկյան վարորդների կոլեկտիվ որոշմամբ [4, pp. 15-16]:

7.1 ենթագլխի գրականություն

1. *Kumari A.K. Sharma,* Infrastructure financing and development: A bibliometric review, in International Journal of Critical Infrastructure Protection, N 16, 2017.

2. World Bank, World Development Report, Infrastructure for Development, Washington, DC, 1994.
3. National Strategy for Critical Infrastructure Protection (CIP Strategy), Federal Republic of Germany, Federal Ministry of the Interior, 17th June 2009.
4. *Rinaldi M, J. Peerenboom, T.K.Kelly,* Critical Infrastructure Interdependencies: Identifing, Understanding, and Analyzing, IEEE Control System Magazine, December 2001.

7.2 Կրիտիկական ենթակառուցվածքները ԱՄՆ ազգային անվտանգության և համաշխարհային ռիսկերի գնահատման զեկույցներում

Կրիտիկական ենթակառուցվածքների՝ ներքին ու արտաքին բնույթի սպառնալիքներից խոցելիության նվազեցման հիմնահարցերը պաշտոնապես հայտնվեցին ամերիկյան անվտանգության և քաղաքականության մշակողների տեսադաշտում դեռևս 1990-ական թթ.: Պաշտոնապես կրիտիկական ենթակառուցվածքների անվտանգության ապահովման ինչպես դոկտրինալ հիմնադրույթները, այնպես էլ օպերացիոնալ արձագանքման ձևաչափերը սկսեցին ներառվել ԱՄՆ անվտանգային հանրության ամենամյա զեկույցներում (առանձին ենթաբաժիններով) 2010-ական թթ. ի վեր[5]: Ընդ որում, կրիտիկական ենթակառուցվածքների՝ իբրև համապարփակ երևույթի անվտանգության ապահովման թե՛ հրատապության և թե՛ ենթակառուցվածքնե-

[5] ԱՄՆ ԿՀՎ տնօրենը յուրաքանչյուր տարեսկզբին ԱՄՆ Կոնգրեսին է ներկայացնում ամերիկյան հետախուզական հանրության (տարբեր ծառայությունների և գործակալությունների մասնակցությամբ պատրաստված) ընթացիկ տարվա անվտանգության սպառնալիքների գլոբալ գնահատականների զեկույցը: Փաստաթուղթն ուշագրավ է այն առումով, որ համապարփակ ձևով ներկայացնում է անվտանգության ոլորտում աշխատող տարբեր մարմինների կողմից «ագրեգացված» գնահատականները: Զեկույցների հանրության համար բաց տեքստերը հասանելի են *www.dna.gov* կայքում:

րին վերաբերող տեղեկատվության ծավալները տարեցտարի ընդլայնվում են: Մասնավորապես, 2011թ. զեկույցում գլոբալ սպառնալիքներն աստիճանակարգված էին հետևյալ կերպ. առաջին հերթին մատնանշվում էր ահաբեկչության վտանգն իր տարածաշրջանային բոլոր չափումներով, այնուհետև՝ զանգվածային բնաջնջման զենքի և տեխնոլոգիաների տարածումը[6]: Կրիտիկական ենթակառուցվածքները հիշատակվում էին զուտ «ռազմական կարողությունների ինստիտուցիոնալացման» համատեքստում՝ ելնելով այն հանգամանքից, որ ռազմական ոլորտի մատնանշված միտումը խոցելի է դարձնում, ըստ ամերիկյան հետախուզական հանրության, կրիտիկական ենթակառուցվածքների ողջ համալիրը:

2012թ. հերթական զեկույցում կրիտիկական ենթակառուցվածքների խոցելիության հետ կապված հիմնախնդիրներն ու անվտանգության ապահովման հնարավոր լուծումները գլխավորապես ներկայացված էին կիբեռսպառնալիքների՝ ռազմավարական նշանակության պրոբլեմի վերածման համատեքստում: Մասնավորապես՝ մատնանշվում էր, որ «կիբեռսպառնալիքները ազգային և տնտեսական անվտանգության կրիտիկական հիմնախնդիր են դարձել՝ նկատի ունենալով տեղեկատվական տեխնոլոգիաների հարատև առաջընթացն ու կախվածության աստիճանի աճը՝ ժամանակակից հասարակության բոլոր հատվածներում»[7]: Համանման մոտեցում էր գերակայում նաև 2013թ. զեկույցում, որում կիբեռսպառնալիքներին և կրիտիկա-

[6] U.S. Intelligence Community: Worldwide Threat Assessment, J.R.Clapper, March 10, 2011, pp. 1-6.

[7] Unclassified Statement for the Record on the Worldwide Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence, J.R.Clapper, 31 January, 2012, p. 7. https://www.dni.gov/files/documents/Newsroom/Testimonies/20120131_testimony_ata.pdf

կան ենթակառուցվածքներին վերաբերող ենթաբաժինը հայտնվել էր արդեն առաջին էջի վրա. «մենք գտնում ենք, որ ԱՄՆ կրիտիկական ենթակառուցվածքների համակարգի վրա լայնածավալ կիբեռհարձակման հեռավոր հնարավորություն գոյություն ունի, որը կհանգեցնի ծառայությունների երկարաժամկետ և լայնածավալ խաթարմանը»[8]:

2017թ. զեկույցում ամերիկյան անվտանգության խնդիրներով զբաղվող փորձագիտական հանրությունն արդեն ավելի առարկայական և հասցեական էր իր գնահատականների մեջ. «Ռուսաստանը լիարժեք կիբեռդերակատար է, որը կշարունակի մնալ էական սպառնալիք ԱՄՆ կառավարության, ռազմական, դիվանագիտական, առևտրային և կրիտիկական ենթակառուցվածքների համար: Մոսկվայի տնօրինության ներքո չափազանց կատարյալ կիբեռհարձակումների ծրագրեր կան, և վերջին շրջանում Կրեմլը էլ ավելի ագրեսիվ կեցվածք է ընդունել… Մենք գտնում ենք, որ Ռուսաստանի կիբեռգործողությունները կշարունակեն թիրախավորել Միացյալ Նահանգները և նրանց դաշնակիցներին՝ հավաքագրելով հետախուզական տվյալներ, օժանդակելով որոշումների կայացմանը ՌԴ-ում, իրականացնելով ներազդման գործողություններ, որպեսզի սատարեն Ռուսաստանի ռազմական և քաղաքական նպատակների ապահովմանը և համապատասխան կիբեռմիջավայր ստեղծեն ապագա գործողությունների համար»[9]:

[8] Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, House Permanent Select Committee on Intelligence, J.R.Clapper, 11 April, 2013, p. 1. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-090.pdf

[9] Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, Daniel R. Coats Director of National Intelligence, May 11, 2017, p. 1.

Ընդհանուր առմամբ, դատելով ամերիկյան հետախուզական և անվտանգային հանրության բաց զեկույցների բովանդակությունից, ակնհայտ է, որ կրիտիկական ենթակառուցվածքների հիմնախնդրի կարևորությունը ոչ միայն շեշտակիորեն ընդգծվել է վերջին տարիների ընթացքում, այլև աճել են վերջիններ՝ հասարակության և պետական ինստիտուտների ներթափանցման ինտենսիվությունը և էքստենսիվությունը: Ընդլայնվել են թե՛ ֆիզիկական ու տնտեսական կյանքի տարբեր չափումների վրա սպառնալիքների ներազդման ծավալները և թե՛ վերջինների հոգեբանական հետևանքների դաշտը: Ավելին, 2017թ. ԱՄՆ-ում անցկացված վարժանքների արդյունքները փաստեցին, որ առավել լուրջ վտանգ կարող են ներկայացնել կրիտիկական ենթակառուցվածքների վրա հարձակման հետևանքով առաջացող կասկադային էֆեկտները[10]:

7.3 Կրիտիկական ենթակառուցվածքների պաշտպանության և անվտանգության ապահովման առանձնահատկությունները Գերմանիայում

Գերմանացի հետազոտողների կարծիքով՝ կրիտիկական ենթակառուցվածքների պաշտպանության պարագայում կարևորվում են երկու ընդհանուր նկատառումներ. որևէ պետություն գործնականում ի վիճակի չէ 100% ապահովել այդ ենթակառուցվածքների անվտանգությունը, մինչդեռ հիշյալ հիմնահարցի լուծման որևիցե ունիվերսալ եղանակ նույնպես գոյություն չունի: Դրա հետ մեկտեղ, կրիտիկական ենթակառուցվածքների

[10] *J. Schneider,* Cyber Attacks on Critical Infrastructure: Insights from War Gaming, July 27, 2017, https://warontherocks.com/2017/07/cyber-attacks-on-critical-infrastructure-insights-from-war-gaming/

պաշտպանության երեք մոտեցումներ են առկա, որոնք էլ ընկած են համապատասխան քաղաքականությունների հենքում:

Առաջինը կրիտիկական տեղեկատվական ենթակառուցվածքների պաշտպանության *(CIIP, Critical Information Infrastructure Protection)* մոտեցումն է: Այստեղ կարևորվում են բացառապես *IT* ցանցերի և *IT* ոլորտի անվտանգությունն ու հիշյալ խնդրի հետ կապված լուծումները, մինչդեռ նյութական օբյեկտների անվտանգությունն ապահովվում է այլ կազմակերպական շրջանակներում: Կրիտիկական ենթակառուցվածքներին վերաբերող գործառույթները և մասնագիտական պատասխանատվությունը ցրված են տարբեր մարմինների միջև, իսկ մասնավոր հատվածի ինտեգրումը *ԿԵ* պաշտպանության համակարգում կարևորվում է բոլոր մակարդակներում:

Երկրորդ մոտեցումը ենթադրում է թե՛ կրիտիկական *IT* ենթակառուցվածքների և թե՛ նյութական/ֆիզիկական ենթակառուցվածքների պաշտպանություն համապարփակ եղանակներով: Այստեղ նյութական համակարգերի պաշտպանությունը հանդիսանում է քաղպաշտպանության անքակտելի չափումը, մինչդեռ *ԿԵ* պաշտպանության և անվտանգության ապահովման կենտրոնական մարմինը զբաղվում է և՛ *IT* անվտանգության հարցերով, և՛ քաղպաշտպանությամբ, և՛ աղետների ռիսկերի կառավարմամբ: Նման համադրույթի շրջանակներում առանձնահատուկ դերակատարություն է վերապահվում պաշտպանության նախարարությանը, իսկ մոտեցումը հայտնի է «բոլոր (վտանգների) դեպքում» պայմանական անվանմամբ:

Վերոնշյալ երկու մոտեցումներն էլ ձգտում են ինտեգրել և միասնականացնել ԿԵ ոլորտին առնչվող պետական և մասնավոր կողմերին մեկ ազգային կազմակերպական շրջանակի մեջ,

սակայն ռազմավարական պլանավորման մակարդակում հանրային/պետական/–մասնավոր որևէ լուրջ համակարգում գրեթե չի նկատվում:

Երրորդ մոդելի առանձնահատկությունն, ըստ գերմանացի մասնագետների, վերաբերում է զուտ չինական փորձին: Գլխավոր յուրահատկությունն այն է, որ Չինաստանում կրիտիկական ենթակառուցվածքների պաշտպանության ոլորտում բացակայում է որևիցե համագործակցություն պետական և մասնավոր դերակատարների միջև, իսկ *ԿԵ* անվտանգության ապահովման գործն ամբողջության ներառված է կառավարության իրավասության մեջ[11]:

Գերմանիայի *ԿԵ* պաշտպանությունը հենվում է երկրորդ մոտեցման, այն է՝ միասնական «բոլոր (վտանգների) դեպքում» սկզբունքի վրա[12]:

Ի տարբերություն, օրինակ, Սինգապուրի, որտեղ կրիտիկական ենթակառուցվածքների պաշտպանության ապահովումը դրված է հենց վերջիններիս սեփականատերերի վրա[13], Գերմանիայում *ԿԵ* անվտանգության ապահովման հիմքում ընկած է պետության և մասնավոր հատվածների համագործակցության սկզբունքը: Դաշնային հանրապետությունում կրիտիկական կարևորության օբյեկտների և ենթակառուցվածքների պաշտպանվածության և անվտանգության ապահովման համար պատասխանատու գերատեսչությունը՝ Տեղեկատվական անվտան-

[11] Critical Infrastructure Protection: Survey of World-Wide Activities, Jörn Brömmelhörster, Sandra Fabry and Nico Wirtz for BSI KRITIS, 4/2004, Bundesamt fur Sicherheit in der Informationstechnik, pp. 1-2:

[12] *Ch.Eismann,* Trends in Critical Infrastructure Protection in Germany, Transactions of the VSB – Technical University of Ostrava, Vol. IX, N 2, 2014, pp. 26-31.

[13] Կարող են լինել մասնավոր ընկերություններ, որոնց նկատմամբ վերահսկման քաղաքականություն է իրականացվում Սինգապուրի կառավարության կողմից:

գության դաշնային գերատեսչությունը *(Bundesamt für Sicherheit in der Informationstechnik - BSI),* հիմնվեց 1997թ.՝ այն նույն ժամանակ, երբ լույս տեսավ ԱՄՆ *PDD-63* հրամանագիրը, որով սահմանվում էր ամերիկյան կրիտիկական ենթակառուցվածքների ցուցակը: Ավելի ուշ՝ ԳԴՀ կրիտիկական ենթակառուցվածքների պատասխանատուների մարմիններում ընդգրկվեց նաև ներքին գործերի նախարարությունը, ինչպես նաև Գերմանիայի աշխատանքի և տնտեսության նախարարությունը, քանի որ կրիտիկական ենթակառուցվածքների ճնշող մեծամասնությունը մասնավոր հատվածում էր (մոտ 90%)[14]:

Հաշվի առնելով կրիտիկական ենթակառուցվածքների համալիր բնույթն ու կարևորությունը Գերմանիայի տնտեսական և հասարակական կենսագործունեության համար՝ 2000-ական թթ. սկզբից կրիտիկական ենթակառուցվածքների անվտանգության ապահովման գործն իրականացվում է միջգերատեսչական ընթացակարգերի ձևաչափում՝ ներքին գործերի նախարարության առաջատար դերակատարման ներքո: Ըստ ԳՖՀ Կրիտիկական ենթակառուցվածքների պաշտպանության ազգային ռազմավարության՝ «կրիտիկական» եզրույթի կիրառումը պայմանավորված է վերջիններիս էական կարևորությամբ՝ ժամանակակից հասարակության գործառույթների ապահովման տեսանկյունից, մինչդեռ *ԿԵ* խափանումը կարող է հանգեցնել ամբողջ համակարգի երկարաժամկետ խափանման: Նման կարգի «կրիտիկական» բնույթ արտացոլվում է երկու չափումներում.

- *համակարգային կրիտիկական միավորներ*՝ ընդհանուր համակարգի շրջանակում տվյալ ենթակառուցվածքային

[14] Защита критической инфраструктуры: Подходы государств Европейского Союза к определению элементов критической инфраструктуры, *М. Сметана,* Ph.D. ВШБ - Технический Университет Острава, 2014/15, стр. 38.

սեկտորի կառուցվածքային, գործառութային և տեխնիկական դիրքով պայմանավորված փոխկախվածության բարձր աստիճան (օրինակ՝ տեղեկատվական ցանցեր, էլեկտրականություն), որի խափանումը կարող է հանգեցնել ողջ հասարակության և պետության համար անվտանգային լուրջ հետևանքների;

- *սիմվոլիկ կրիտիկական միավորներ,* որոնք կապված են ինքնության, հասարակության հուզական կամ մշակութային չափումների հետ և նույնպես կարող են զարգացման բացասական սցենարի պարագայում հասցնել երկարատև հոգեբանական «ապահավասարակշռման էֆեկտի»[15]:

Հատկանշական է, որ *ԿԵ* պաշտպանության խնդիրն ըստ ընդունված համապատասխան ռազմավարության վերաբերում է ինչպես կառավարությանը, այնպես էլ ողջ հասարակությանն ընդհանուր առմամբ՝ հաշվի առնելով պրոբլեմի թե՛ արդիականությունը և թե՛ իրական ծավալները: Որպես ԿԵ համակարգային պաշտպանության շահառուներ են դիտարկվում երեք խմբեր՝ կառավարությունը (հանրային կառավարման համակարգը), հասարակությունը (քաղաքացիական հասարակությունը) և ոլորտում աշխատող ընկերությունները (ներառյալ՝ գերազանցապես մասնավոր հատվածը)[16]:

ԱՄՆ 16 կրիտիկական սեկտորների համանմանությամբ՝ ԳԴՀ կառավարությունը ևս առանձնացնում է հետևյալ կրիտիկական ոլորտներն ու ենթակառուցվածքները.

[15] National Strategy for Critical Infrastructure Protection (CIP Strategy), Federal Ministery of Interior, Berlin, 17th June, 2009, p. 7.
[16] Նույն տեղում:

- Փոխադրամիջոցները և տրանսպորտային հոսքերը
- Էներգետիկ համակարգը
- IT և հեռահաղորդակցությունը
- Ֆինանսական և ապահովագրական հատվածը
- Հանրային կառավարման հատվածը
- Սննդամթերքի հատվածը
- Ջրամատակարարման և հարակից ոլորտները
- Առողջապահությունը
- ԶԼՄ-ն և մշակույթը:

Ուշագրավ է, որ կրիտիկական ենթակառուցվածքները Գերմանիայում դասակարգվում են ըստ վերջիններիս *տեխնիկական բազայի*[17] կամ սոցիալ-տնտեսական ծառայությունների կարևորության[18]:

Կրիտիկական ենթակառուցվածքների պաշտպանությունն ու անվտանգության ապահովումը Գերմանիայում հենվում են երեք սկզբունքների վրա՝ կանխարգելում (պրոակտիվ նախապատրաստվածություն), արձագանքում (ճգնաժամերի գործուն կառավարում) և հարատևություն (կայունություն): *ԿԵ* պաշտպանությունն ընկալվում է իբրև համընդհանուր խնդիր, որի ապահովման գործում ներգրավված են բոլոր երեք շահառուները, այդ թվում նաև կրիտիկական բնագավառում աշխատող մասնավոր ընկերությունները (մոտ 2000 ընկերություն): Բացի

[17] Էներգետիկա և մատակարարման համակարգ, տեղեկատվական համակարգ, տրանսպորտ, ջրամատակարարում *(National Strategy for Critical Infrastructure Protection (CIP Strategy), p. 7.*

[18] Առողջապահություն, սննդամթերք, արտակարգ իրավիճակների ծառայություն, հանրային կառավարում և իրավապահ մարմիններ, ֆինանսական հատված և ապահովագրական գործ, մեդիա և մշակույթ (National Strategy for Critical Infrastructure Protection (CIP Strategy), p. 7.

այդ, ԳԴՀ կրիտիկական ենթակառուցվածքների պաշտպանության հիմքում ընկած է սուբսիդիարության[19] սկզբունքը, որը կիրառելի է ոչ միայն ներազգային համադրույթում (տեղական–դաշնային մակարդակներ), այլև վերաբերում է Եվրոպական միության շրջանակում կրիտիկական ենթակառուցվածքների պաշտպանության մեխանիզմներին և ընթացակարգերին:

7.4 Կրիտիկական տեղեկատվական ենթակառուցվածքների անվտանգության ապահովման ռուսաստանյան փորձը

Սառը պատերազմի դարաշրջանում միջուկային զսպման գաղափարի հենքում ընկած էր «փոխադարձ ոչնչացման» մասին թեզը, որը ենթադրում էր հակառակորդ կողմին անընդունելի վնասի հասցնում: Դեռևս 1960-ական թթ. ԱՄՆ ռազմավարական նշանակության օդուժի նշանակետում էր Խորհրդային Միության ռազմական նշանակության 25 թիրախների և 151 քաղաքային-ինդուստրիալ կենտրոնների վերացումը, ներառյալ պողպատի և ցեմենտի գործարաններ, միջուկային օբյեկտներ, ռադիոկայաններ, նավթարդյունաբերության կենտրոններ և տրանսպորտային հանգույցներ[20]: Կարիբյան ճգնաժամի շրջանում (1960-ական թթ.) առաջին անգամ ուշադրության կենտրոնում հայտնվեց հեռահաղորդակցության ոլորտը՝ որպես կրիտիկական կարևորության բնագավառ, որի պաշտպանությունը հասցվեց ռազմավարական նշանակության գերխնդրի: Իսկ արդեն 1980-ական թթ. ամերիկյան մասնագետները սահմանե-

[19] Համաձայն այդ սկզբունքի՝ անհատի, փոքր սոցիալական խմբերի իրավունքները և շահերն ավելի առաջնային են, քան պետության իրավունքները և շահերը:
[20] Russian critical infrastructures: Vulnerabilities and policies, K. Pynnöniemi (ed.), The Finnish Institute of International Affairs, pp. 16-17.

ցին ենթակառուցվածքի բովանդակությունն իբրև «փոխկապակցված կառուցվածքային տարրերի ամբողջություն, որոնք պահպանում են կառույցի ամբողջականությունը և կիրառելի են, որպես կանոն, միայն արհեստականորեն ստեղծված կառույցների պարագայում»[21]:

Ըստ ռուսաստանյան պաշտոնական աղբյուրների՝ ներկայում ՌԴ-ում մոտ 90 մլն մարդ ապրում է բարձր ռիսկայնության գոտիներում, իսկ երկրում առկա են ավելի քան 45000 հավանական վտանգ ներկայացնող օբյեկտներ[22]: Ֆինլանդիայի միջազգային հարաբերությունների ինստիտուտի հետազոտողների կարծիքով՝ ՌԴ կրիտիկական կարևորության օբյեկտների պաշտպանության և անվտանգության ապահովման հարացույցի հենքում ընկած են նախկին խորհրդային մոտեցումները՝ «բոլոր տիպի վտանգներին» պատրաստ լինելու ԽՍՀՄ քաղպաշտպանության սկզբունքը: Հետազոտության հեղինակները պնդում են, որ հիշյալ մոտեցումը դիտարկում էր ոչ թե առանձնացված կրիտիկական ենթակառուցվածքների պաշտպանությունը որպես այդպիսին, այլ համընդհանուր պատրաստությունը՝ արձագանքելու և պաշտպանվելու տարաբնույթ վտանգներից և սպառնալիքներից[23]:

Կրիտիկական ենթակառուցվածքները որպես առանձին իրավական բնույթի սահմանազատում կրող կատեգորիա՝ ՌԴ-ում սկսեց գործածվել 2010-ական թթ. սկզբներից, երբ բավակա-

[21] Infrastructure for the 21st Century: Framework for a Research Age, Washington: National Academies Press, 1987, [e-resource].

[22] «Основы государственной политики в области обеспечения безопасности РФ и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года», 15 ноября, 2011, пр. 3400.

[23] *K. Pynnöniemi (ed.),* The Finnish Institute of International Affairs, p. 39.

նաչափ ծավալուն աշխատանքներ տարվեցին ՌԴ կրիտիկական տեղեկատվական ենթակառուցվածքների *(ԿՏԵ)* սահմանման և իրավական պաշտպանության ուղղությամբ[24]: Ընդ որում, ՌԴ կրիտիկական տեղեկատվական ենթակառուցվածքների կանոնակարգման շրջանակը ներառում է՝ բացի հանգուցային նշանակության օբյեկտներից, նաև էլիաղորդակցության ցանցերը, որոնք օգտագործվում են կրիտիկական տեղեկատվական ենթակառուցվածքի օբյեկտների միջև փոխգործակցության համար: Այս համադրույթում ինտերնետի օգտագործումն է հանդիսանում կարգավորման հիմնական առարկան[25]:

Հարկ է նշել, սակայն, որ թեև կրիտիկական ենթակառուցվածք եզրույթը մերթ ընդ մերթ օգտագործվում է ՌԴ պաշտոնական կամ փորձագիտական տեքստերում, այդուհանդերձ, մի շարք եզրույթներ «փոխլրացնում» են տվյալ բնագավառին վերաբերող հասկացությունների ամբողջությունը: Դրանց շարքում են, օրինակ, «ռազմավարական օբյեկտ» *(стратегический объект),* «վտանգավոր ինդուստրիալ օբյեկտ» *(опасный производственный объект),* «հատուկ նշանակության օբյեկտ» *(особо важный объект)* և այլն[26]:

Ինչ վերաբերում է *ԿՏԵ* հիմնախնդրին, ապա *ԿՏԵ* անվտանգության ապահովման հիմնախնդիրները ՌԴ-ում սկսել է քննարկվել դեռևս 2000-ական թթ. կեսերից, իսկ 2006թ. ռուսաս-

[24] 2016թ. ընդունված ՌԴ Տեղեկատվական անվտանգության դոկտրինի համաձայն՝ Ռուսաստանի տեղեկատվական ենթակառուցվածքի ներքո հասկացվում է «տեղեկատվայնացման օբյեկտների, տեղեկատվական ցանցերի, ինտերնետում գտնվող կայքերի ամբողջությունը, որը գտնվում է ՌԴ տարածքում, ինչպես նաև ՌԴ իրավասության տակ գտնվող տարածքներում կամ օգտագործվում է ՌԴ միջազգային պայմանագրերի համաձայն». «Доктрина информационной безопасности РФ», утверждена Указом No646 2016г.

[25] «О безопасности критической информационной инфраструктуры РФ».

[26] Russian Critical Infrastructures: Vulnerabilities and Policies, The Finnish Institute of International Affairs, K.Pynnoniemi (ed.), FIIA Report 35, Tampere 2012, p. 42.

տանյան օրենսդիրներին ներկայացվեց «տեղեկատվական և հաղորդակցային ենթակառուցվածքի կրիտիկական կարևորության օբյեկտների տեղեկատվական անվտանգության ապահովման առանձնահատկությունների մասին» օրենքի նախագիծը, որը ստացավ օրենքի կարգավիճակ: Ավելի ուշ՝ 2013թ., մեկ այլ իրավական փաստաթուղթ պատրաստվեց՝ «ՌԴ կրիտիկական տեղեկատվական անվտանգության» մասին, որը նախատեսվում էր առանձին *ԿՏԵ* ռեեստրի ստեղծում և գնահատման ու խոցելիությունների նախանշման ընթացակարգեր[27]: ՌԴ *ԿՏԵ*-ի մեջ ներառվում են ավտոմատացված համակարգերն ու հեռահաղորդակցության ցանցերը, որոնք օգտագործվում են պետական կառավարման և պետության անվտանգության ու պաշտպանունակության ապահովման գործում:

ՌԴ Ազգային անվտանգության հայեցակարգում (2015թ.) պետության և հանրության անվտանգությանն ուղղված սպառնալիքների շարքում (կետ 43) մատնանշվում է «ահաբեկչական և ծայրահեղական կազմակերպությունների գործունեությունը, որն ուժային միջոցներով նպատակաուղղված է ՌԴ սահմանադրական կարգի փոփոխմանը, պետական իշխանության մարմինների գործունեության խաթարմանը, ռազմական և ինդուստրիալ կառույցների գործառույթների աղճատմանը, կրիտիկական հանրային ենթակառուցվածքների և տրանսպորտային ենթակառուցվածքների ոչնչացմանը, բնակչության ահաբեկմանը, այդ թվում նաև զանգվածային ոչնչացման զենքի, ռադիոակտիվ, թունավոր, տոքսիկ, քիմական կամ կենսաբանական միջոցների օգտագործմամբ, միջուկային ահաբեկչությունը, ՌԴ *IT* ենթակառուցվածքի

[27] *Н.Рудычева*, Критическая инфраструктура РФ: сегодня ответственных нет. By Digital Report on 06.12.2016, https://digital.report/kiberbezopasnost-rossii-otvetstvennyih-za-sboi-net/

դեմ հարձակումն ու վերջինիս եկարամյա խափանումը»[28]:

2017թ. դեկտեմբերին ռուսաստանյան օրենսդիրներն ընդունեցին «ՌԴ կրիտիկական տեղեկատվական ենթակառուցվածքի անվտանգության» մասին օրենքի նախագիծը, որտեղ սահմանվում էին կրիտիկական տեղեկատվական ենթակառուցվածքի անվտանգության ապահովման հիմնական սկզբունքները, պետական մարմինների լիազորություններն այդ ոլորտում, ինչպես նաև *ԿՏԵ* օբյեկտների սեփականատերերի իրավունքներն ու պարտականությունները[29]: Ըստ 2018թ. ընդունված օրենքի՝ *ԿՏԵ* սեփականատերերը պարտավոր են տեղեկացնել իշխանություններին համակարգչային միջադեպերի մասին, կանխարգելել ոչ իրավական գործողությունները և ապահովել տեղեկատվական ռեզերվային կրկնօրինակման միջոցով կորսված տեղեկատվական օբյեկտների վերականգնումը:

Ըստ 2018թ. հունվարին ընդունված օրենքի՝ *ԿՏԵ* օբյեկտների շարքին են դասվում.

- պետական մարմինների ինֆոհամակարգերը
- ռազմարդյունաբերական համալիրի ձեռնարկությունները
- առողջապահությունը
- տրանսպորտը
- հեռահաղորդակցությունը
- ֆինանսավարկային համակարգը
- էներգետիկ և միջուկային ոլորտը
- տիեզերագնացությունը և հրթիռաշինությունը
- քիմիական արդյունաբերությունը և մետալուրգիան[30]:

[28] Russian National Security Strategy, December 2015, Presidential Edict 683, “The Russian Federations’ National Security Strategy”.
[29] За кибератаки будут сажать и штрафовать, Коммерсантъ, 12.07.2017.
[30] Вступил в силу закон о защите критической информационной инфраструктуры, РИА Новости, 01.01.2018.

Ոլորտի կարգավորման գործառույթները Ռուսաստանում գլխավորապես դրված են ՌԴ Անվտանգության դաշնային ծառայության *(ՓՍԲ),* Տեխնիկական և արտահանման վերահսկման դաշնային ծառայության *(ՓՏԷՔ),* ինչպես նաև ՌԴ Կապի և հեռահաղորդակցության նախարարության վրա:

Հատկանշական է, որ ի տարբերություն Գերմանիայի, որտեղ կրիտիկական ենթակառուցվածքների պաշտպանությունն ապահովվում է համատեղ ջանքերի շրջանակում՝ տարբեր շահառուների ներգրավմամբ, Ռուսաստանում հիմնական շեշտը դրված է կարգավորիչ գործիքակազմի վրա, իսկ համագործակցության ձևաչափերն ավելի շատ վերաբերում են անվտանգության բնագավառում կենտրոնական և տեղական իշխանությունների միջև աշխատանքային հարաբերությունների կայացմանը:

7.5 Իսրայելի գիտատեխնոլոգիական ոլորտի կրիտիկական ենթակառուցվածքները

Իսրայելը դասվում է, թերևս, այն բացառիկ պետությունների շարքին, որի կրիտիկական ենթակառուցվածքների[31] համակարգի ողջ սպեկտրը այս կամ այն չափով փոխկապակցված է երկրի, բնակչության անվտանգության և մասնավորապես՝ պաշտպանական անվտանգության ոլորտի հետ: Եվ սա, ըստ էության, բնական գործընթաց պետք է համարել, քանի որ 1948թ. Իսրայել պետության հիմնադրումից մինչև օրս երկիրը շարունակում է զարգանալ հարևան երկրների ու զինյալ տարբեր խմբավորումների կողմից ռազմական սպառնալիքների իրական վտանգի ներքո:

Ընդհանուր առմամբ, Իսրայելի կրիտիկական ենթակա-

[31] *Գագիկ Հարությունյան*, «Կրիտիկական ենթակառուցվածքներ և գաղափարախոսություն», «21-րդ ԴԱՐ», թիվ 4 (74), 2017թ., http://www.noravank.am/arm/articles/detail.php/detail.php?ELEMENT_ID=16030