

ՏՆՏԵՍԱԳԻՏՈՒԹՅՈՒՆ

ՏԵԽՆՈԼՈԳԻԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ և «ԵՐԿԱԿԻ ՆՇԱՆԱԿՈՒԹՅԱՆ ՏԵԽՆՈԼՈԳԻԱՆԵՐԻ» ԶԱՐԳԱՑՄԱՆ ԽՆԴԻՐՆԵՐԸ*

Թաթուլ Մանասերյան

Բանալի բառեր՝ տեխնոլոգիական անվտանգություն, «Երկակի նշանակության տեխնոլոգիաներ», տնտեսություն, ներդրումներ:

Կասկածից վեր է, որ երկրի մտավոր և տեխնոլոգիական անվտանգությունը հնարավոր չէ պատկերացնել առանց նրա ռազմա-արդյունաբերական համալիրի կայուն գործունեության: Արցախյան 44-օրյա պատերազմն ամենայն խորությամբ բացահայտեց Հայաստանի և Արցախի տեխնոլոգիական խոցելիությունը և այս ասպարեզում համակարգված գործողությունների բացակայությունը: Ակնհայտ է, որ ռազմա-արդյունաբերական համալիրը համարվում է բարձր տեխնոլոգիաների հիմնական պատվիրատուն և ներդրումների աղբյուրը[1]:

Ետպատերազմյան շրջանում տեխնոլոգիական անվտանգության ապահովման գլխավոր ուղղությունը ռազմական արդյունաբերության «երկակի» տեխնոլոգիաների առաջնահերթ զարգացումն է: Հայ և արևմտյան տնտեսագետների բազմաթիվ ուսումնասիրություններից վաղուց պարզվել է, որ նախորդ տնտեսակարգում տարբեր ուղղությունների ինովացիաների փոխներթափանցման խնդիրն այն չէր, որ զինվորականները չէին ցանկանում հաղորդել իրենց տեխնոլոգիական գաղտնիքները քաղաքացիական արդյունաբերությանը: Խնդիրն այլ էր, այն է՝ վերջինիս մոտ առաջավոր նորացումների ներդրման համար արդյունավետ խթանների բացակայությունը, էժան աշխատուժը, ազատությունը ներքին և միջճյուղային մրցակցությունից, յուրաքանչյուր ձեռնարկության ներդրումային ռեսուրսների կենտրոնացված ձևավորումը, թողարկման պլանի թվային ցուցանիշների գերակայությունը. այս ամենը խորհրդային հիմնարկներին չէին մղում ռազմական արդյունաբերությունից վերցնելու տեխնոլոգիական նորույթները: Մեր ուսումնասիրությունները վկայում են, որ «Երկակի տեխնոլոգիաների» խթանման քաղաքականություն մշակելիս սկզբունքորեն կարելի է հաշվի առնել ամերիկյան փորձը, որտեղ մասնավորապես ներկայիս դեմոկրատական վարչակազմի իշխանության գալու հետ վերաբնակություն է արդյունաբերական քաղաքականության մարտավարությունը[2]: Միջազգային փորձը հուշում է, որ տեխնոլոգիական նորացման խթանման պետական քաղաքականությունը պետք է լինի որոշակի իմաստով՝ ռազմա-քաղաքացիական ինտեգրումը «Երկակի տեխնոլոգիաների» զարգացման և առևտրականացման հիման վրա[3]: Խոսքը քաղաքացիական և ռազմական արդյունաբերության փոխհարստացման գործընթացի խթանման մասին է՝ տնտեսության այդ երկու բաժիններում կազմակերպչա-վարչական և տեխնոլոգիական խոչընդոտների վերացման արդյունքում: Բայց ամերիկյան «Երկակի տեխնոլոգիաների» խթանման քաղաքականության և համապատասխան ԵԱՏՄ անդամ մի շարք երկրների էական տարբերությունն այն է, որ ԱՄՆ-ում պետք չէ զբաղվել հարցի պատասխան փնտրելով, թե ինչպես մասնավոր քաղաքացիական ձեռնարկություններին ստիպել ընդօրինակել պաշտպանական սեկտորի տեխնոլոգիական նորույթները: Քաղաքացիական արդյունաբերության տեխնոլոգիական նորույթների հանդեպ պահանջարկը ավանդաբար մեծ է, քանի

* Հոդվածն ընդունվել է 12.05.21:

Հոդվածը տպագրության է երաշխավորել տ.գ.դ., պրոֆեսոր Մ. Հայրապետյանը: 18.05.21:

որ այն խարսխված է լրացուցիչ եկամուտ ստանալու տնտեսական շահի վրա: Այդ պատճառով ԱՄՆ-ի համար ավելի կարևոր է «երկակի տեխնոլոգիաների» քաղաքականության երկրորդ կողմը՝ քաղաքացիական սեկտորի էժանագին տեխնոլոգիաների փոխառության հիման վրա ռազմական արդյունաբերության վիճակի բարելավումը[4]:

Նախկին խորհրդային բազմաթիվ երկրներում իրավիճակն այլ է: Քաղաքացիական արդյունաբերության նորացումների ակտիվությունը բոլորովին չի աճել խորհրդային ժամանակներից: Պարզապես վերը թվարկված պլանային տնտեսությունում գործող գործոններին փոխարինելու եկան նորացումների ապախթանման «անցումային» պատճառները /ավանդական տնտեսական կապերի խզում, վճարումների ձգնաժամ, ներմուծվող ապրանքների էքսպանսիա, առանձին հիմնարկների և գործունեության ուղորդող վերածումը մենաշնորհների այլն/: Ու քանի որ տեղական պաշտպանական արդյունաբերությունը տեխնոլոգիապես քաղաքացիական վերաձևակող արդյունաբերությունից գրեթե ոչինչ չունի վերցնելու, «երկակի տեխնոլոգիաների» քաղաքականության մարտավարական նպատակը քաղաքացիական և ռազմական արդյունաբերության տեխնոլոգիական մակարդակների միաժամանակյա ամրացումը կարող է լինել՝ նորացումների փոխադարձ ներթափանցումների հիման վրա: Ինչ վերաբերում է տեխնոլոգիական անվտանգության խնդրին, ապա պետք է նկատել, որ «երկակի տեխնոլոգիաների» քաղաքականությունը արդյունավետ է այդ ուղղությամբ միայն այն ժամանակ, երբ այն նպաստում է ինչպես ռազմական արդյունաբերության, այնպես էլ նրա հետ կապված քաղաքացիական ճյուղերի միաժամանակյա տեխնոլոգիական նորացմանը: Իրականացնելով ռազմա-քաղաքացիական ընտեգրումը և միջոցներ ներդնելով «երկակի տեխնոլոգիաների» մեջ՝ պետությունը դրանով իսկ իր վրայից հանում է ծանր ֆինանսական բեռի մեծ մասը, որը պահանջվում է ազգային տեխնոլոգիական անկախությունը պահպանելու համար:

Այուս կողմից՝ «երկակի տեխնոլոգիաների» ոլորտը ընդլայնելով՝ պետությունը բարձրացնում է նաև ազգային տեխնոլոգիական բազայի անկախության աստիճանը, նպաստում է ռազմական և կից ծեռնարկությունների հետ արտադրանքի զարգացմանը այնպիսի տեխնոլոգիաների ճյուղերում, որոնք արդեն գոյություն ունեին միայն արտասահմանում: Երբ բացակայում է ռազմա-քաղաքացիական հատվածների ընտեգրումը, պետությունը հարկադրված իր վրա է վերցնում ռազմական կիրառության տեխնոլոգիաների մշակման անհրաժեշտ ծախսերը՝ ռազմական արդյունաբերության փակ գոտում: Ընդ որում՝ պետք է հաշվի առնել նաև այն, որ ռազմա-տեխնոլոգիական ներուժի զարգացումը հնարավոր է միայն մի որոշակի սահմանում. դրանց հետևում ծանր բեռ է, որը պահվում է պետության հաշվին, և արդեն ի վիճակի չէ դիմակայել քաղաքացիական ճյուղերի «արյունազրկմանը»:

Ռազմական մի շարք տեխնոլոգիաների փոխակերպումը «երկակիների» կարգի՝ պետության վրայից հանում է զգալի ֆինանսական պարտավորություններ այնքանով, որքանով տվյալ տեխնոլոգիաների քաղաքացիական բաժնեմասը ընդունակ է փոխհատուցելու դրանց մշակումների ծախսերը՝ համապատասխան նախագծերի առևտրային իրականացումների միջոցով: Այս իրադրության մեջ կառավարությունը հնարավորություն է ստանում ազատված միջոցների մեծ մասն ուղղել հույժ կարևոր ռազմական տեխնոլոգիաների նորագույն մշակումների վրա: Դրանում է կայանում երկրի տեխնոլոգիական անվտանգության ռազմավարական բաղադրամասը՝ կապված «երկակի տեխնոլոգիաների» հետ:

Այսպիսով՝ երկրի բարձր տեխնոլոգիաների զարգացման առումով տեխնոլոգիական անվտանգության արդյունավետ մարտավարությունը ոչ այնքան «երկակի» կիրառության տեխնոլոգիաների նորացման առաջարկների խթանումն է, որքան մասնավոր հատվածի կողմից վերջինիս պահանջարկի խրախուսման քաղաքականությունը: Քաղաքացիական արտադրանքի զանգվածային շուկաներ դուրս եկող խոշոր միջճյու-

դային ընկերությունները պետք է շահագրգռված լինեն պաշտպանական արդյունաբերության առաջարկած «երկակի տեխնոլոգիաներում» հանդիպական ներդրումների մեջ[5]: Արդյունաբերության արդիականացման ամերիկյան քաղաքականությունը՝ ռազմա-քաղաքացիական ինտեգրման հիմքի վրա, ենթադրում է հզոր կորպորացիաների կողմից պետական գիտական կենտրոնների /լաբորատորիաների/ մշակած, ռազմական նշանակության տեխնոլոգիաների առևտրային կիրառման փոխադարձ շահագրգռություն /նրանք տեղակայված են Սանդիայում, Լոս-Ալամոսում, Լոուրենսում, Լիվերմորում և այլն/: Մեր երկրում «երկակի տեխնոլոգիաների» և պաշտպանական արդյունաբերության փոխարկման խթանման այդպիսի շահագրգռվածության անհրաժեշտություն առաջմ հաշվի չի առնվել: Դրանով իսկ ռեսուրսների սահմանափակ քանակությունը և պաշտպանական հանգուցային գիտահետազոտական ինստիտուտների գոյատևման սպառնալիքը «երկակի տեխնոլոգիաներ» հասկացության իմաստը հասցրին հարուստ ռազմական գիտական հիմնարկություններում բյուջեից դուրս ֆինանսավորման աղբյուրներ փնտրելուն:

Ինչով է սպառնում մեր երկրի բարձր տեխնոլոգիաների զարգացմանը և տեխնոլոգիական անվտանգությանը «երկակի տեխնոլոգիաների» ոլորտում տիրող իրավիճակը: Մեր կողմից երկրի գործարարների, տնտեսագետների և պետական կառավարման միջին օղակների ղեկավարների հետ անցկացրած ուսումնասիրությունների արդյունքները որոշակիորեն հստակեցնում են մտահոգությունների շրջանակները: Ստորև բերվում են հարցումների հիմքի վրա պարզված այդ գործոնների թվարկումը: Ցուցակը կազմված է ըստ կարևորության նվազման /առաջին տեղում է այն հարցը, որը ավելի շատ էր հիշատակվում/: Այսպիսով՝ հիմնական գործոնները հետևյալն են.

1/ գիտական հետազոտությունների նյութական բազայի պակաս վարկավորումը և հիմնարկության գիտա-տեխնոլոգիական պաշարի մաշվածությունը,

2/ ենթակապալառուների տեխնոլոգիական շղթայի քայքայումը, որի հիման վրա նախկին հարակից ձեռնարկությունների՝ այլ արտադրանք թողարկելու վերակողմնորոշումը, տրանսպորտային խնդիրները և այլն/ և տարրական բազայի որակի վատթարացումը³ բարձր տեխնոլոգիական արտադրանք թողարկելու համար;

3/ կոմպլեկտավորող նյութերի գների գերազանցող աճը, որ մատակարարում են ենթակապալառուները՝ նրանց արտադրական հզորությունների թերբեռնվածության արդյունքում,

4/ նույն գերազանցող գների աճը ենթակառուցվածքի ծառայությունների վրա /էլեկտրաէներգիա, տրանսպորտ, գազա- և ջրամատակարարում/, որը հարյուցում է միջազգային շուկաներում բարձր տեխնոլոգիաների շահութաբերության և մրցունակության անկում,

5/ գիտատար արտադրանքի հանդեպ անբավարար ներքին պահանջարկ,

6/ գիտատար արտադրանքի հետ մրցակցող արտերկրից մատակարարումների մենաշնորհացումը և հայրենական արտադրողի դուրս մղումը տեղական շուկայից,

7/ պետական հովանավորչության անբավարար մակարդակը՝ բարձր տեխնոլոգիաների արտահանման և ներկրման գործարքների գծով,

8/ արտահանման ծավալների և եկամուտների անկում:

Անկասկած, բարձր տեխնոլոգիաների առաջնահերթ խնդիրը կապիտալ ներդրումների պակասն է[6]: Սակայն կարևոր է պարզել նաև՝ արդյոք կարող է պետությունը բյուջետային սահմանափակ միջոցների պայմաններում լուծել այդ խնդիրը: Հազիվ թե գտնվեն հիմնավոր փաստարկներ հարցի դրական պատասխանի համար: Դրա փոխարեն ցուցակում 2-7 կետերով բերված, տեխնոլոգիական անվտանգության սպառնալիքների գործոնները պարզ վկայում են արտադրողի մտահոգությունը իրենց գիտատար արտադրանքի պահանջարկի նվազման մասին: Այստեղ հատկապես կարևորվում է հինգերորդ գործոնը:

Բարձր տեխնոլոգիաների զարգացման համար անհրաժեշտ է տեխնոլոգիական շղթայի յուրաքանչյուր փուլում արտադրության ծախսերի փոխհատուցում՝ հերթական պատվիրատուի միջոցների հաշվին: Տեխնոլոգիական շղթայում բազմաթիվ սպառողների աննշան ֆինանսական հզորությունը և վճարումների քայքայիչ ձգնաժամն ամբողջ տնտեսությունում, տեխնոլոգիական նորացումների փոխհատուցված իրացման շանսերը ներքին շուկայում ներկայումս աննշան է: Այստեղից առաջանում է տեխնոլոգիական անվտանգության հիմնական սպառնալիքը: Կորցնելով ներքին շուկայում սեփական մշակումների իրացման հույսերը՝ պաշտպանական ինստիտուտները տեխնոլոգիաների, know-how և նոր արտադրանքի վաճառքի հնարավորություններ են փնտրում արտաքին շուկաներում: Հասկանալի է, որ արտահանող երկրի տեխնոլոգիաների արտահանումը սպառնալիք չի ներկայացնում արդյունաբերական բազայի համար, եթե այդ բազան բավարար չափով ամուր է: Ամերիկյան տեխնոլոգիական գիտական կորպորացիաները տեխնոլոգիայի արտահանումը սկսում են միայն նոր արտադրանքի ներքին արտադրության յուրացումից հետո: Քանի որ մեր երկրում նման կառույցներ չկան, և բարձր տեխնոլոգիաների իրացման համար բացակայում է կայուն արդյունաբերական բազան, կառավարությունը և Հայաստանի ազգային մրցունակության խորհուրդը լավագույն դեպքում կարող էին սատարել նոր տեխնոլոգիաների զարգացումը մինչև կիրառական և փորձնական արտադրության փուլը[7]: Միևնույն ժամանակ երկրում պայմաններ չապահովելով այդպիսի տեխնոլոգիաների զանգվածային արդյունաբերական իրականացման համար, պետությունը փաստորեն օժանդակում է գիտատար արտադրանքի արտասահմանյան արտադրողներին՝ տարբեր ծրագրերին հատկացվող ծախսերի մասով: Քիչ չեն դեպքերը, երբ գնելով տեղական մասնագետներից նորագույն տեխնոլոգիաներ, որոնք օգտագործվում են միջանկյալ արտադրանքի արտադրության մեջ, արտերկրի ընկերությունները այնուհետև արտահանում են պատրաստի ապրանքներ համաշխարհային շուկաներ, այդ թվում նաև՝ Հայաստան:

Հայաստանի Ազգային անվտանգության ռազմավարությունում հայտարարված երկրի տնտեսական և տեխնոլոգիական անվտանգության ապահովմանը վերաբերող և գիտատար տեխնոլոգիաներ արտադրողների և սպառողների միջև կայուն ներքին կապերի ստեղծման անհրաժեշտության մասին[8]: Բարձր տեխնոլոգիաների զարգացման առումով խիստ կարևոր է նաև երկրի գիտական ներուժի և առաջատար գիտական դպրոցների պահպանումը, որոնք ընդունակ են ապահովելու Հայաստանի մտավոր և տեխնոլոգիական անկախությունը:

Միաժամանակ կարևոր է հիշել, որ տեխնոլոգիական անվտանգության ապահովման առումով պետության հնարավորություններն անսահմանափակ չեն ոչ միայն ֆինանսական, այլև իրավա-օրենսդրական հիմքերի ապահովման առումով: 2011թ. սեպտեմբերի 11-ի ահաբեկչությունից հետո ԱՄՆ-ի հորդորով աշխարհի բազմաթիվ երկրներ միացան հակաահաբեկչական միությանը և, ի թիվս այլ փաստաթղթերի, ազգային օրենսդիր մարմինների կողմից ընդունեցին նաև «Երկակի տեխնոլոգիաների» գործածության սահմանափակմանն ուղղված օրենքներ: ՀՀ Ազգային ժողովը, մասնավորապես, 2010թ. ապրիլի 8-ին ընդունել է «Երկակի նշանակության ապրանքների արտահանման, ՀՀ տարածքով դրանց տարանցիկ փոխադրման, ինչպես նաև երկակի նշանակության տեղեկատվության և մտավոր գործունեության արդյունքների փոխանցման նկատմամբ հսկողության մասին» ՀՀ օրենքը[9]: Տվյալ պարագայում օրենքի վերնագիրն ինքնին խոսում է դրա բովանդակության ու մեր երկրում ոչ միայն «Երկակի տեխնոլոգիաների», այլև ընդհանուր առմամբ, բարձր տեխնոլոգիաների զարգացման ասպարեզում առկա սահմանափակումների մասին: Այնուամենայնիվ անհրաժեշտ է վերալուծել և իրատեսորեն գնահատել բարձր տեխնոլոգիաների բնագավառում ստեղծված ներկայիս վիճակը, որը թույլ կտա նաև որոշակի եզրակացությունների հանգել դրանց արտահանման հեռանկարների վերաբերյալ:

Մտավոր արժեքները շուկայում հանդես են գալիս որոշակի ապրանքների ձևով ուրոնք «արտաքուստ նյութական չլինելով» մնացած բոլոր հատկանիշներով լիովին համապատասխանում են «ապրանք» հասկացությանը «Միջազգային շուկայում այդ ապրանքի համար մղվում է եռանդուն և կոշտ պայքար և այդ ոլորտի զարգացման հարցերը չափազանց արդիական են»:

Միջազգային տնտեսական համագործակցությանը Հայաստանի մասնակցությունը ռազմավարական առաջնահերթ խնդիրներից է ինչն արտահայտվում է մի շարք գործոններով.

- մտավոր սեփականության օբյեկտների պաշտպանության ապահովումը Հայաստանում՝ չսահմանափակելով հայրենական հայտատուների շահերը,
- հայրենական հայտատուների կողմից ստեղծված օբյեկտների պաշտպանության ապահովումն արտասահմանում, ինչպես նաև պաշտպանված օբյեկտների լայնատարած օգտագործումը տնտեսությունում:

1993թ. ապրիլին Հայաստանը դարձավ Մտավոր սեփականության պաշտպանության համաշխարհային կազմակերպության «WIPO» 1994թ. մայիսին՝ Արդյունաբերական սեփականության պաշտպանության փարիզյան կոնվենցիայի «Նշանների միջազգային գրանցման» մադրիդյան համաձայնագրի, ինչպես նաև Արտոնագրային համագործակցության մասին պայմանագրի «PCT» անդամ: 2003թ.-ից Հայաստանի Հանրապետությունն անդամակցում է Առևտրի համաշխարհային կազմակերպությանը «ԱՀԿ-WTO» ԱՀԿ-ի հետ բանակցությունների ընթացքում Հայաստանը ստանձնել է մտավոր սեփականության ոլորտի օրենսդրական դաշտի ստեղծման և փոփոխման մի շարք պարտավորություններ: Սակայն այդ աշխատանքը պատշաճ ձևով չի համակարգվում, և դեռևս մշակված չէ արտաքին տնտեսական կապերի զարգացման և ներքին շուկայի պաշտպանվածության ներդաշնակության պետական հայեցակարգը:

Նման չհամաձայնեցված գործունեության հետևանքով ընդունվում են օրենսդրական փաստաթղթեր, որոնք կամ չեն համապատասխանում միջազգային որոշակի պահանջներին, կամ էլ հապճեպ ընդունվելով և համապատասխանեցվելով դրանց՝ կարող են խոչընդոտել հանրապետության տնտեսական զարգացումը. այդպիսի իրավիճակ ստեղծվեց, երբ հայրենական և օտարերկրյա հայտատուներից սկսեցին գանձել միևնույն չափի տուրքեր:

Այսպիսով՝ մտավոր սեփականության օբյեկտների ստեղծումը, պաշտպանությունը և տնտեսությունում օգտագործումը խթանելու խնդիրը պետք է համարել հանրապետության արտաքին տնտեսական կապերի քաղաքականության բաղկացուցիչ ուղղություններից մեկը:

Կնքվել են համագործակցության մի շարք պայմանագրեր և փոխըմբռնման հուշագրեր ինչպես այլ պետությունների՝ Հնդկաստանի Հանրապետության, Եգիպտոսի Արաբական Հանրապետության և այլն, այնպես էլ համաշխարհային ծանաչում ունեցող այնպիսի ընկերությունների հետ, ինչպիսիք են Մայքրոսոֆթը, Ալկատելը, Հյուլեթ Փակարդը, Սան Մայքրոսիսթենսը, Նելսոն Ինսթրումենթսը, Սենթոր Գրաֆիքսը և այլն, որոնց շրջանակներում իրավաբանորեն կանոնակարգվում են նաև բարձր տեխնոլոգիաների անվտանգությանն առնչվող խնդիրները:

Բարձր տեխնոլոգիաների բնագավառի վերջին նվաճումները թույլ են տալիս տեղեկություններ ստանալ նաև կանխամտածված կերպով թաքցվող տնտեսական գործունեության ամենատարբեր կողմերի ու ոլորտների վերաբերյալ: Տեղեկատվությունն արտադրական գաղտնիք է, եթե ունի իրական կամ պոտենցիալ արտադրական արժեք երրորդ դեմքին անհայտ լինելու պատճառով՝ նրանց անհասանելի լինելու շնորհիվ և գաղտնիության պահպանման չափերի ընդունմամբ: Դրա դրսևորման ձևերն են փաստաթղթերը, սխեմաները, արտադրությունը, որոնք ապահովագրված են կողոպուտից ու բացահայտումից:

Արտադրական գաղտնիքները բաժանվում են տեխնոլոգիական, արտադրական, կազմակերպչական, մտավոր, շուկայական, գովազդային և այլ խմբերի: Դրանց կարելի է հասնել ինչպես օրինական ձանապարհով, այնպես էլ անօրինական՝ կիրառելով կաշառք, շանտաժ և այլն: Համացանցը դրա համար բացում է լրացուցիչ հնարավորություններ: Գաղտնի տեղեկատվությունը բաժանում է գործնականի ու տեխնիկականի: Տեղեկատվությունը դադարում է լինել գաղտնի, հենց որ դառնում է հանրությանը հայտնի: Բայց մեղավոր չի համարվում նա, ով այդ տեղեկատվությունը ստանում է հանրամատչելի միջոցներով: Բարձր տեխնոլոգիաների դարաշրջանում տեղեկատվական անվտանգության համակարգի ստեղծման համար ընդունվում են չափեր, որոնք ներառում են կադրային ծրագիրը, գաղտնի տվյալներին հասու լինելու սահմանափակությունը, տեղեկատվությունը կրողների հետ աշխատանքի կարգավորում, փաստաթղթեր, տարբեր տեխնիկական կրիչներ և համաձայնությունների ճիշտ կայացում: Գաղտնի տվյալների արտահոսքի կանխումը ենթադրում է ընկերության գաղտնիքների սահմանի որոշում և նրանց կուտակման տեղի որոշում, խոցելի ալիքների պրոտենցիալի որոշում ու դրանց փակման միջոցների մշակում, գործերի վիճակի ստուգման գրաֆիկի առկայությունը^[10]: Տեղեկատվական անվտանգության համակարգի իրականացումը ներառում է աշխատանքի ընդունման և ազատման ժամանակ անհատի հետ զրույցներ, կազմակերպված աշխատանք գաղտնի փաստաթղթերի հետ (արտադրության կարգուկանոնի հաստատում, գաղտնիքների բացահայտում ու ոչնչացում, այլ ֆիրմաներից գաղտնիքի պահպանում), թվային ու պատճենահանող տեխնիկայի նկատմամբ վերահսկողություն, արտադրական գաղտնիքի պահպանում այլ կազմակերպությունների հետ համաձայնության գալիս և այլն:

Համացանցի զարգացումը, լայնացնելով հաղորդակցման հնարավորությունները, նոր խնդիրներ է առաջ քաշում ինֆորմացիայի պահպանման հետ կապված: ՀՀ և ԱՀ գոյություն ունեցող օրենսդրությունները չեն գործում այն ընկերությունների նկատմամբ, որոնք կապված են Internet-ի հետ: Այդ պատճառով էլ այդ հարցի շուրջ քննարկումները բացահայտել են հասարակության ուշադրությունն այդ հարցի հետ կապված: Անհրաժեշտ է մշակել «առևտրական գաղտնիքի մասին» նոր օրենք, ուր կներառվեն միջազգային տեղեկատվության փոխանակման մասնակցության մասին համապատասխան դրույթներ:

Նման գործունեությունն ուղղված է այն բանին, որ մի կողմից տեղեկատվությունն ազատ հասնի քաղաքացիներին, իսկ մյուս կողմից՝ տեղեկատվությունը պահպանվի հեռահաղորդակցման ցանցերում, պահպանվեն բիզնեսն ու իրավունքները, ինչպես նաև քաղաքացիների կյանքին առնչվող տվյալների անմատչելիությունը: Տեղեկատվության պահպանման պահանջով կատարվող վերահսկումը պետք է իրականացվի պետական իշխանության մարմինների կողմից: Կազմակերպությունները կարող են ստեղծել հատուկ ծառայություններ՝ տեղեկատվությունը պաշտպանելու համար: Տեղեկատվական ռեսուրսների սեփականատերը իրավունք ունի իրականացնելու վերահսկումը և արգելելու տեղեկատվության վերամշակումը՝ այդ պահանջները չկատարելու դեպքում: Փաստաթղթավորված տեղեկատվության սեփականատերը իրավունք ունի նաև դիմելու պետական իշխանության մարմիններին՝ նորմերի կատարման ճիշտ գնահատման համար: Փաստաթղթերի սեփականատերը կարգ ու կանոն պետք է հաստատի տեղեկատվությունը օգտագործողի համար նշված տեղով, ժամանակով ինչպես նաև անհրաժեշտ գործընթացով և ապահովի հասանելիության պայմանը տեղեկատվությունից օգտվողի համար: Բացի այդ՝ նա գործող օրենսդրությամբ կարող է նաև ապահովել տեղեկատվության պաշտպանության մակարդակը: Փաստաթղթերի սեփականատերը կարող է դիմել այն կազմակերպությանը, որն իրականացնում է տեղեկատվական համակարգի պաշտպանության միջոցները և տեղեկատվական ռեսուրսները:

Վիճակագրությունը վկայում է, որ մտավոր սեփականության օբյեկտների պաշտպանության բնագավառների հիմնական ցուցանիշները աճի միտում ունեն: Սակայն դրանց կանխատեսումը չի կարող բնութագրել ամբողջ ոլորտի իրավիճակը, քանզի այն պայմանավորվում է ոչ թե արտոնագրերի կամ վկայականների քանակով, այլ պաշտպանվող օբյեկտների ստեղծագործական պատշաճ մակարդակով և դրանց կիրառումամբ, ինչի ապահովումը այս ոլորտի պետական ծրագրի հիմնական նպատակներից մեկը պետք է լինի:

Այսպիսով՝ կարևոր է առանձնահատուկ ուշադրություն դարձնել տեղեկատվական տեխնոլոգիաների բնագավառի առավել հրատապ հիմնահարցերին, որոնց աստիճանական լուծումը կարող է ապահովել երկրի տեղեկատվական անվտանգությունը: Տեղեկատվական տեխնոլոգիաների անվտանգությունը մասնագետների կողմից տարբեր ձևով է հասկացվում, ընդ որում՝ նկատի են ունենում այդ խնդրի որևէ կոնկրետ մի բնագավառ: Օրինակ՝ անընդհատ սնուցման աղբյուրների արտադրողների տեսակետից կարևոր վտանգ է հանդիսանում էներգացանցի անկայունությունը, իսկ հակավիրուսների աշխատողի տեսակետից՝ արժեքավոր տվյալների ոչնչացման ռիսկը: Այս բնագավառներից յուրաքանչյուրը, անշուշտ, կարիք ունի առանձին ուսուցման: Բայց սպառողի համար կարևոր է ապահովել անվտանգությունն ընդհանրապես: Սպառողների առջև կան հստակ առաջադրանքներ. հարթել արտադրական գործընթացը, հաշվապահական հաշվառումը, ֆինանսների և կադրերի ղեկավարումը, այսինքն՝ ապահովել գործարարության համար նպաստավոր գործընթաց: Եվ եթե տեղեկատվական տեխնոլոգիաների օգտագործումը հնարավորություն է տալիս արդյունավետ լուծել այդ խնդիրը, ապա սպառողը ժամանակ և փող է տրամադրում դրա ներդրման համար: Բայց վստահելով գործարարությունը տեղեկատվական համակարգին՝ այն կախվածության մեջ են գցում դրա աշխատանքային հնարավորություններից: Այդ անկախությունը այնքան կարևոր է, որքան կարևոր է համապատասխան գործարար գործընթացը կազմակերպության համար: Այլ խոսքով՝ այդ գործընթացի համար պատասխանատու յուրաքանչյուր չհաջողված համակարգ վտանգի է ենթարկում ամբողջ ձեռնարկությունը: Ի վերջո, մարդկանց և կազմակերպությունների համար համար ներդրված տեղեկատվական տեխնոլոգիայի անվտանգությունը դժվարին խնդիր է՝ կապված նրանց ճիշտ և անընդհատ գործածության հետ:

ԾԱՆՈԹԱԳՐՈՒԹՅՈՒՆՆԵՐ

1. Asia-Pacific Security Asia-Pacific Security Studies Civil-Milit Civil-Military Integration and ary Integration and Chinese Milit Chinese Military Modernization ary Modernization Asia-Pacific Center f ic Center for Security Studies Volume 3 - Number 9, December 2004, p. 1-4.
2. Douglas A. Irwin (PIIE), MEMORANDUM ON Rethinking Industrial Policy Office of Trade and Manufacturing Policy, October 20, 2020, Part of a special PIIE series Rebuilding the Global Economy outlining policy priorities and solutions heading into 2021, available at: <https://www.piie.com/blogs/trade-and-investment-policy-watch/memo-biden-administration-how-rethink-industrial-policy>.
3. W. Clark McFadden, Dewey Ballantine, Dual-Use Technologies and National Security, International Friction and Cooperation in High-Technology Development and Trade: Papers and Proceedings (1997), **Chapter: Dual-Use Technologies and National Security**, pp. 130-152, available at: <https://www.nap.edu/read/5902/chapter/16#151>.
4. Promoting technological civil-military synergies, European defence agency, 04 MARCH 2021, AVAILABLE AT: [HTTPS://EDA.EUROPA.EU/NEWS-AND-](https://eda.europa.eu/news-and-)

EVENTS/NEWS/2021/03/04/PROMOTING-TECHNOLOGICAL-CIVIL-MILITARY-SYNERGIES

5. Certain issues about foreign investment in dual-use technology in Spain Richard A. Silberstein Partner of the Corporate Area, G A _ P Pol Rubio Lawyer of the Corporate Area, G A _ P, June, 2017, available at: <https://www.ga-p.com/wp-content/uploads/2018/07/certain-issues-about-foreign-investment-in-dual-use-technology-in-spain-2.pdf>
6. Lucia Waldner, Investment Trends Beyond 2021: Nearshoring Of Tech Talent, Forbes Finance Council, Money, January 20, 2021, available at: <https://www.forbes.com/sites/forbesfinancecouncil/2021/01/20/investment-trends-beyond-2021-nearshoring-of-tech-talent/?sh=241b21531ee0>
7. Հայաստանի ազգային մրցունակության հիմնադրամը (ՀԱՄՀ) հիմնադրամ է, որը ստեղծվել է 2008 թվականին՝ Հայաստանի տնտեսական մրցունակության զարգացման նպատակով: Հիմնադրամի հիմնական աշխատողական ոլորտներն էին կրթությունը, առողջապահությունը, գրոսաշրջությունը և ցանցերի ու տեղեկատվության հասանելիությունը: Ներկայումս այս կառույցը դադարեցրել է իր գործունեությունը:
8. Հայաստանի Ազգային անվտանգության ռազմավարություն, https://www.primeminister.am/u_files/file/Different/AA-Razmavarutyun-Final.pdf
9. «Երկակի նշանակության ապրանքների արտահանման, ՀՀ տարածքով դրանց տարանցիկ փոխադրման, ինչպես նաև երկակի նշանակության տեղեկատվության և մտավոր գործունեության արդյունքների փոխանցման նկատմամբ հսկողության մասին» ՀՀ օրենքը, www.parliament.am
10. M.R. Fazlida, Jamaliah Said, Information Security: Risk, Governance and Implementation Setback, Procedia Economics and Finance, Volume 28, 2015, pp. 243-248.

ԱՄՓՈՓԱԳԻՐ

**Տեխնոլոգիական անվտանգությունը և «երկակի նշանակության տեխնոլոգիաների» զարգացման խնդիրները
Թաթուլ Սանասերյան**

Երկրի մտավոր և տեխնոլոգիական անվտանգությունը հնարավոր չէ պատկերացնել առանց նրա ռազմա-արդյունաբերական համալիրի կայուն գործունեության: Արցախյան պատերազմն ամենայն խորությամբ բացահայտեց Հայաստանի և Արցախի տեխնոլոգիական խոցելիությունը և այս ասպարեզում համակարգված գործողությունների բացակայությունը: Ակնհայտ է, որ ռազմա-արդյունաբերական համալիրը համարվում է բարձր տեխնոլոգիաների հիմնական պատվիրատուն և ներդրումների աղբյուրը: Ետպատերազմյան շրջանում տեխնոլոգիական անվտանգության ապահովման գլխավոր ուղղությունը՝ ռազմական արդյունաբերության «երկակի» տեխնոլոգիաների առաջնահերթ զարգացումն է: Հայ և արևմտյան տնտեսագետների բազմաթիվ ուսումնասիրություններից վաղուց պարզվել է, որ նախորդ տնտեսակարգում տարբեր ոլորտների ինովացիաների փոխներթափանցման խնդիրն այն չէր, որ գինվորականները չէին ցանկանում հաղորդել իրենց տեխնոլոգիական գաղտնիքները քաղաքացիական արդյունաբերությանը: Խնդիրն այլ էր, այն է՝ վերջինիս մոտ առաջավոր նորացումների ներդրման համար արդյունավետ խթանների բացակայությունը, էժան աշխատուժը, ազատությունը ներքին և միջճյուղային մրցակցությունից, յուրաքանչյուր ձեռնարկության ներդրումային ռեսուրսների կենտրոնացված ձևավորումը, թողարկման պլանի թվային ցուցանիշների

գերակայությունը այս ամենը խորհրդային հիմնարկներին չէին մղում տեխնոլոգիական նորույթները, վերցնելու ռազմական արդյունաբերությունից:

РЕЗЮМЕ

Технологическая безопасность: проблемы развития технологий двойного назначения Татул Манасерян

Ключевые слова: Технологическая безопасность, «технологии двойного назначения», экономика, инвестиции

Нет сомнений в том, что интеллектуальную и технологическую безопасность страны невозможно представить без устойчивого функционирования ее военно-промышленного комплекса. 44-дневная арцахская война глубоко выявила отсутствие скоординированных действий в Армении и технологическую уязвимость Арцаха. Очевидно, что военно-промышленный комплекс считается основным заказчиком высоких технологий, источником инвестиций.

Основным направлением обеспечения технологической безопасности в послевоенный период является приоритетное развитие технологий «двойного назначения» в военной промышленности. Многочисленные исследования армянских экономистов уже давно показали, что проблема взаимопроникновения инноваций в различных областях в прежнюю экономику заключалась не в том, что военные не хотели делиться своими технологическими секретами с гражданской промышленностью. Проблема заключалась в другом, то есть в отсутствии эффективных стимулов для внедрения передовых инноваций. Недорогая рабочая сила, свобода от внутренней и межотраслевой конкуренции, централизованное распределение инвестиционных ресурсов каждого предприятия, преобладание цифровых показателей плана выпуска - все это не подталкивало советские институты к заимствованию технологических инноваций у военной промышленности.

SUMMARY

Technological Security: the Problems of the Development of "Dual Use" Technologies Tatul Manaseryan

Key words: Technological security, "dual-use technologies", economy, investments

There is no doubt that the intellectual and technological security of a country cannot be imagined without the sustainable operation of its military-industrial complex. The 44-day Artsakh war revealed in depth the lack of coordinated actions in Armenia and in Artsakh technological vulnerability. It is obvious that the military-industrial complex is considered to be the main customer of high technologies, the source of investments.

The main direction of technological security in the post-war period is the priority development of "dual use" technologies in the military industry. Numerous studies by Armenian economists have long revealed that the problem with the interpenetration of innovations in various fields in the previous economy was not that the military did not want to share their technological secrets with the civilian industry. The problem was different, that is, the lack of effective incentives for the introduction of advanced innovations. Inexpensive labor, freedom from internal and cross-sectoral competition, the centralized allocation of investment resources of each enterprise, the dominance of digital indicators of the output plan - all this did not push the Soviet institutions to take technological innovations from the military industry.