ՀՀ ԿՐԹՈՒԹՅԱՆ, ԳԻՏՈՒԹՅԱՆ, ՄՇԱԿՈՒՅԹԻ ԵՎ ՍՊՈՐՏԻ
ՆԱԽԱՐԱՐՈՒԹՅՈՒՆ
ԽԱՉԱՏՈՒՐ ԱԲՈՎՅԱՆԻ ԱՆՎԱՆ ՀԱՅԿԱԿԱՆ ՊԵՏԱԿԱՆ ՄԱՆԿԱՎԱՐԺԱԿԱՆ
ՀԱՄԱԼՍԱՐԱՆ

ՇԱՀԲԱԶՅԱՆ ՄԱՐԻՆԵ ԿԱՐԱՊԵՏԻ

ԱՐԴԻ ՀԱՍԱՐԱԿՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱՅՆԱՑՄԱՆ ՇԱՐԺԻՉ ՈՒԺԵՐԸ ԵՎ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀԻՄՆԱԽՆԴԻՐԸ. ՍՈՑԻԱԼ-ՓԻԼԻՍՈՓԱՅԱԿԱՆ ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ

Թ. 00.01 - Փիլիսոփայական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության

ՍԵՂՄԱԳԻՐ

ԵՐԵՎԱՆ 2020

Ատենախոսության թեման հաստատվել է ՀՀ ԳԱԱ Փիլիսոփայության, սոցիոլոգիայի և իրավունքի ինստիտուտի գիտական խորհրդում:

Գիտական ղեկավար՝ փիլիսոփայական գիտությունների դոկտոր, պրոֆեսոր Մանուկ Արսենի Հարությունյան

Պաշտոնական ընդդիմախոսներ՝ փիլիսոփայական գիտությունների դոկտոր, պրոֆեսոր Էռնեստ Ռուբենի Գրիգորյան

փիլիսոփայական գիտությունների թեկնածու, դոցենտ Աշոտ Արամայիսի Գևորգյան

Առաջատար կազմակերպություն՝ Հայ-ռուսական համալսարանի փիլիսոփայության ամբիոն

Ատենախոսության պաշտպանությունը կայանալու է 2020 թ. հուլիսի 03-ին ժամը 12:00-ին Խաչատուր Աբովյանի անվան հայկական պետական մանկավարժական համալսարանում գործող՝ ԲՈԿ-ի Փիլիսոփայության 062 մասնագիտական խորհրդի նիստում:

Մասնագիտական խորհրդի հասցեն՝ 3750010, ք. Երևան, Տիգրան Մեծի 17, Խաչատուր Աբովյանի անվան հայկական պետական մանկավարժական համալսարան, գիտխորհրդի (կարմիր) դահլիճ:

Ատենախոսությանը կարելի է ծանոթանալ Խաչատուր Աբովյանի անվան հայկական պետական մանկավարժական համալսարանի գրադարանում:

Սեղմագիրն առաքված է 2020թ. մայիսի 23-ին:

Մասնագիտական խորհրդի գիտական քարտուղար՝ փիլիսոփայական գիտությունների թեկնածու, դոցենտ Հովհաննես Օնիկի Հովհաննիսյան

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Թեմայի արդիականությունը: Հետազոտության արդիականությունն ու կարևորությունը պայմանավորված է նախ՝ տեղեկատվական-տեխնոլոգիական հեղափոխությամբ, որն ուղենշում է մարդկության զարգացումը դեպի սկզբունքորեն նոր՝ տեղեկատվական, գիտելիքահեն հասարակություն: Այստեղ կարևորագույն գործոնը ժամանակն է՝ հետ մնալը հղի է բազմաբնույթ ռիսկերով, որոնց հետևանքները կործանարար կլինեն անմրցունակ ազգային պետությունների տնտեսության, սոցիալական ոլորտի, գիտության, կրթության և մշակույթի համար:

Երկրորդ՝ հետազոտության թեմայի արդիականությունը պայմանավորված է նաև անձի, հասարակության և պետության (ազգի) անվտանգության առաջ ծառացած նոր մարտահրավերների և վտանգների տրամաբանությամբ: Դրանք այսօր սերտորեն կապված են տեղեկատվական հակամարտությունների նոր ձևերի՝ կիբեռհանցագործությունների, կիբեռպատերազմների բնույթի և առանձնահատկությունների հետ: Ազգային անվտանգությունն այսօր էապես կախված է տեղեկատվական անվտանգությունից: Ընդ որում, գիտատեխնոլոգիական վերափոխումներին համընթաց այդ կախվածությունը գնալով էլ ավելի է աճելու[1]:

Երրորդ՝ պայմանավորված է նաև «տեղեկատվական սպառնալիք», «տեղեկատվական պատերազմ», «կիբեռպատերազմ» և այլ հասկացությունների հստակեցման անհրաժեշտությամբ:

Չորրորդ՝ տեղեկատվական անվտանգության խնդրակարգի արդիականությունը պայմանավորված է տեղեկատվական անվտանգության քաղաքականության ռազմավարության և մարտավարության հստակեցման անհրաժեշտությամբ:

Հինգերորդ՝ խնդրո առարկայի փիլիսոփայական ուսումնասիրության արժեքավորությունը պայմանավորված է նաև տեղեկատվական անվտանգության տարբեր հայեցակարգերի համակարգման պահանջով:

Հետազոտության գիտական աղբյուրները և մշակվածության աստիճանը: Կարելի է առանձնացնել աղբյուրների երեք խումբ: Աղբյուրների առաջին խումբը կազմում են տեղեկատվական հասարակության դասական տեսաբանների՝ Դ. Բելի, Է. Թոֆլերի, Մ. Կաստելսի, Մ. Պոստերի, Ֆ. Ուեբստերի, Մ. Մաքլյուենի և ուրիշների աշխատանքները: Դրանցում քննարկվում են համաշխարհային տեղեկատվական հասարակության առաջ ծառացած մարտահրավերների ուսումնասիրության, ինչպես նաև տեղեկատվական անվտանգության ապահովման ոլորտում առկա հիմնահարցերը:

Աղբյուրների երկրորդ խումբը կազմում են հետխորհրդային փիլիսոփաներ՝ Ա. Դ. Ուրսուլի, Ի. Ս. Մելյուխինի, Վ. Ե. Լեպսկու, Ն. Պ. Վաշեկինի, Կ. Կ. Կոլինի և ուրիշների աշխատությունները՝ նվիրված ժամանակակից հասարակության տեղեկատվական զարգացման համաշխարհայնացման հարցերին:

---

[1] ՀՀ նախագահի կարգադրությունը՝ «Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգը հաստատելու մասին», ՀՀ ՊՏ 2009/35 15.07.2009:

Աղբյուրների երրորդ խումբը տեղեկատվական անվտանգության հիմնախնդիրներին նվիրված ուսումնասիրություններն են, որոնցում տեղեկատվական անվտանգությունը դիտվում է որպես բազմագործոն և բազմաչափ երևույթ: Տեղեկատվական անվտանգության խնդրակարգի սոցիալ-փիլիսոփայական տեսանկյունները շեշտադրված են Վ. Ի. Յառոչկինի, Ա. Ի. Պոզդնյակովի, Ա. Կ. Շավանի, Կ. Կ. Կոլինի, Ի. Ա. Լազարևի, Մ. Ի. Դզիլևի, Ա. Ա. Պռոխոժեի և ուրիշների աշխատություններում: Տեղեկատվական անվտանգության ապահովման գործում պետության, նրա տեղեկատվական քաղաքականության դերի հետ կապված հրատապ հարցերը քննարկվել են Օ. Ն. Նովիկովի, Վ. Լ. Մանիլովի, Վ. Ի. Ցիմբալի, Վ. Գ. Գրաֆսկու աշխատանքներում: Մի շարք աշխատանքներ նվիրված են տեղեկատվական անվտանգության կառավարչական հիմնահարցերին: Խոսքն առաջին հերթին, Ն. Ի. Զինչենկոյի, Լ. Մ. Զեմլյանովայի, Ի. Ա. Լազարևի, Ա. Կ. Շավանի և ուրիշների հրապարակումների մասին է:

Տեղեկատվական պատերազմների խնդրակարգին անդրադարձել են ռուս հետազոտողներ Ս. Ն. Գրինյաևը, Դ. Բ. Ֆրոլովը, Ա. Վ. Մանոյլոն, Յու. Ա. Եռմակովը, Ի. Ն. Պանարինը, Վ. Ֆ. Պետրենկոն, Ս. Պ. Ռաստորգուևը: Այդ խնդիրների արծարծմանն են նվիրված նաև՝ հայ հետազոտողներ Գ. Հարությունյանի, Ս. Գրինյանի և Հ. Արզումանյանի, Ս. Մարտիրոսյանի գիտավերլուծական հոդվածները:

Չնայած հետխորհրդային երկրներում, այդ թվում Հայաստանում տեղեկատվայնացման, տեղեկատվական հասարակության կազմավորման, տեղեկատվական անվտանգության հիմնախնդիրների նկատմամբ աճող հետաքրքրությանը և այդ ասպարեզում հայ փիլիսոփաների որոշակի ձեռքբերումներին, այնուամենայնիվ, պետք է նկատել, որ տեղեկատվական անվտանգության հիմնախնդիրը այդպես էլ չի դարձել միջգիտակարգային, փիլիսոփայական համալիր ուսումնասիրության առարկա: Գործնականում ողջ հետխորհրդային տարածքում սակավ են աշխատանքները, որոնք նվիրված են հասարակական կյանքի տեղեկատվայնացման և տեղեկատվական անվտանգության հիմնախնդիրների փիլիսոփայական վերլուծությանը:

Հետազոտության օբյեկտը՝ տեղեկատվական անվտանգությունն է: **Հետազոտության առարկան՝** հասարակական կյանքի տեղեկատվայնացման պայմաններում տեղեկատվական անվտանգության ապահովման գործոններն ու դրանց առանձնահատկությունները:

Հետազոտության նպատակն ու խնդիրները: Ատենախոսության նպատակը հետխորհրդային հասարակություններում տեղեկատվական անվտանգության համակարգի գործոնների ձևավորման և զարգացման օրինաչափությունների բացահայտումն է և այդ առումով երաշխավորությունների մշակումը: Նպատակի իրականացումը ենթադրում է մի շարք խնդիրների լուծում, որոնցից հիմնականներն են.

- բացահայտել տեղեկատվական հասարակության հայեցակարգերի դերը տեղեկատվական անվտանգության խնդրակարգի ձևակերպման և կառուցակարգերի մշակման գործում,
- հստակեցնել տեղեկատվական անվտանգության սոցիալ-փիլիսոփայական ուսումնասիրության հասկացական ապարատը և վերհանել բովանդակային բեռնվածքը,
- վերլուծել և համակարգել տեղեկատվական ռիսկերի ու սպառնալիքների հիմնական տեսակները, դրանց գործառնության մեխանիզմները,
- վերլուծել ՀՀ տեղեկատվական անվտանգության քաղաքականության ձևավորման ու գործառնության, դրա ռազմավարական նպատակների առանձնահատկությունները:

Հետազոտության տեսական-մեթոդաբանական հիմքը կազմում են սոցիալական իմացության դիալեկտիկական մեթոդը, զարգացման և դետերմինիզմի սկզբունքները, տրամաբանական, պատմահամեմատական և համակարգային վերլուծության մեթոդները: Կիրառվել են ընդհանուր և հատուկ գիտական մեթոդներ՝ համանմանության, համեմատական վերլուծության, համադրման, ինչպես նաև փաստերի ու տվյալների հավաքագրման և վերլուծության սոցիոլոգիական մեթոդները: Ատենախոսն առաջնորդվել է փիլիսոփայական մեթոդաբանության, գիտության և տեխնիկայի ձեռքբերումների համադրման սկզբունքով՝ հենվելով ժամանակակից փիլիսոփայական-մեթոդաբանական, տեխնիկական, տեղեկատվական և քաղաքագիտական հետազոտությունների վրա, որոնցում վերլուծվում են տեղեկատվական անվտանգության հարցերը:

Հետազոտության գիտական նորույթը

Ատենախոսության առջև դրված խնդիրների լուծման արդյունքում ձեռք են բերվել և մշակվել գիտական նորույթ բովանդակող, տեսական և գործնական կարևորություն ունեցող որոշակի արդյունքներ, դրույթներ ու եզրահանգումներ: Մասնավորապես.

1. Հասարակական կյանքի տեղեկատվայնացման գործընթացների համալիր ուսումնասիրության միջոցով վերհանվել են տեղեկատվական անվտանգության հիմնային առանձնահատկությունները, բացահայտվել են դրա ապահովման հիմնարար սկզբունքները, տեղեկատվական անվտանգության հայեցակարգի և գործիքակազմի ազդեցության հնարավորություններն ու սահմանները:

2. Տեղեկատվական հասարակության դիսկուրսի շրջանակներում հստակեցվել է տեղեկատվական անվտանգության հիմնախնդիրների ուսումնասիրության հասկացական ապարատը:

3. Վերլուծվել և համակարգվել են տեղեկատվական սպառնալիքների հիմնական տեսակները, մասնավորապես տեղեկատվական պատերազմների, կամ, որ նույնն է՝ կիբեռպատերազմների («ցանցային» պատերազմների) առանձնահատկությունները:

4. Հիմնավորվել է տեղեկատվական անվտանգության քաղաքականության հայաստանյան մոդելի մշակման անհրաժեշտությունը՝ որպես Հայաստանի Հանրապետության առաջ ծառացած տեղեկատվական սպառնալիքների հաղթահարման առաջատար գործոն և գործողության ռազմավարական ծրագիր:

5. Հստակեցվել են Հայաստանի Հանրապետության տեղեկատվական անվտանգության քաղաքականության առաջնահերթությունները, ձևակերպվել են դրանց ուսումնասիրության գործնական ուղիներ և երաշխավորություններ:

Պաշտպանության ներկայացված հիմնական դրույթները

1. Տեղեկատվական տեխնոլոգիաների ոլորտն այսօր դարձել է հասարակական կյանքի արդիականացման կարևորագույն գործոն: Այն մեծապես ազդում է պետությունների, ազգերի և միջանձնային մակարդակներում տեղի ունեցող կոմունիկացիոն գործընթացների, տեղեկատվական անվտանգության ընդհանուր վիճակի և դրա բաղադրիչների վրա՝ ավելի ու ավելի կարևորելով տեղեկատվական անվտանգության դերն ու նշանակությունն ազգային շահերի պաշտպանության մշակման գործում:

2. Հասարակության զարգացման ներկայիս փուլում մարդկանց միջև տեղեկատվական փոխգործակցությունն իրականացվում է տեղեկատվական պաշարներների օգնությամբ: «Տեղեկատվական պաշար» հասկացությունը կիրառելի է գիտական գիտելիքի և հասարակական կյանքի բոլոր բնագավառներում՝ «տեղեկատվություն» հասկացությունից հետո այն ևս հավակնում է դառնալ է ոչ միայն միջառարկայական, այլ նաև համագիտական կատեգորիա: Դա նշանակում է, որ «տեղեկատվություն», «տեղեկատվայնացում» և «տեղեկատվական պաշար» հասկացությունների օգնությանբ նորովի են իմաստավորվում քաղաքական հաղորդակցության և քաղաքական տեղեկատվական տարածության հասկացությունները: Պետական կառավարման ամբողջ համակարգը ենթարկվում է էական փոխակերպումների, որի վկայությունը աշխարհի բազմաթիվ երկրներում էլեկտրոնային կառավարման, դրա անվտանգության հուսալի պաշտպանվածության հիմնախնդրի ակտիվ քննարկումն է և նոր տեխնոլոգիաների ներդրումը կառավարչական պրակտիկայում: Հասարակության կյանքում տեղեկատվական տեխնոլոգիաների կիրառության ոլորտների ընդլայնմանը համընթաց, իրական հնարավորություններ են ստեղծվում ոչ միայն ժողովրդավարության գործընթացների խորացման, այլ նաև անձնական կյանքի լիակատար վերահսկողության և անհատի վրա ձեռնածուական (մանիպուլյատիվ) ներգործության համար:

3. Տեղեկատվայնացման գործընթացի դրական արդյունքների հետ միասին ի հայտ են եկել տեղեկատվական նոր վտանգներ և սպառնալիքներ՝ «տեղեկատվական աղքատությունը», «թվային անհավասարությունը», «կիբեռհանցագործությունները», «կիբեռ և տեղեկատվական պատերազմները», «ցանցային պատերազմները»՝ «ֆեյքային» ռեսուրսի գործադրմամբ: Տեղեկատվական հակամարտության ժամանակակից ձևերը ավելի ու ավելի մեծ չափով դրսևորվում են կիբեռպատերազմի բաղադրիչների՝ «ֆեյքային» քարոզչության,

լրտեսության, համակարգչային սերվերների վրա գրոհների և այլ ոչ օրինավոր եղանակներով:

4. ՀՀ տեղեկատվական անվտանգության պաշտոնական հայեցակարգը լրամշակման կարիք ունի՝ հաշվի առնելով համաշխարհայնացման գործընթացների ինտենսիվացումը, ահաբեկչական կազմակերպությունների աճը, Թուրքիայի և Ադրբեջանի կողմից սանձազերծված հակահայկական քարոզչության ակտիվացումը:

5. Հայաստանի Հանրապետության տեղեկատվական անվտանգության քաղաքականությունը ևս նորացման կարիք ունի: Այդ կապակցությամբ անհրաժեշտ է զարգացնել և կատարելագործել Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման համակարգը, այդ բնագավառում իրականացվող միասնական պետական քաղաքականությունը: Հարկավոր է նաև կատարելագործել ՀՀ տեղեկատվական անվտանգության առջև ծառացած սպառնալիքների բացահայտման, գնահատման և կանխատեսման ձևերը, մեթոդները և միջոցները, ինչպես նաև այդ սպառնալիքների հակազդման արդյունավետ կառուցակարգերը:

Ատենախոսության տեսական և գործնական նշանակությունը: Ատենախոսությունը, կատարված վերլուծություններն ու եզրահանգումները կարող են տեսական-մեթոդաբանական հիմք ծառայել Հայաստանի Հանրապետության տեղեկատվական անվտանգության ոլորտում արդիականացման գործընթացների կառավարման հրատապ խնդիրների հետագա ուսումնասիրության համար:

Տեղեկատվայնացման և տեղեկատվական անվտանգության հայեցակարգի վերլուծությունը կարող է օգտագործվել Հայաստանի Հանրապետության առաջ ծառացած նոր մարտահրավերներին և սպառնալիքներին հակազդող ազգային տեղեկատվական քաղաքականության ռազմավարության ուղենիշների հստակեցման, դրանց իրականացմանը հետամուտ գործնական ծրագրերի մշակման համար:

Ատենախոսության նյութերը կարող են օգտագործվել գիտության և տեխնիկայի փիլիսոփայության, սոցիալական էկոլոգիայի և սոցիալական ինֆորմատիկայի դասընթացների, ինչպես նաև անվտանգության և կայուն զարգացման փիլիսոփայական հիմնախնդիրներին նվիրված հատուկ դասընթացների մշակման համար:

Ատենախոսության փորձաքննությունը: Ատենախոսության հիմնական դրույթները և հետևությունները ներկայացվել և քննարկվել են «Կյանքը և փիլիսոփայությունը» միջազգային գիտաժողովում, Երևանի Կոմիտասի անվ. Կոնսերվատորիայի հումանիտար գիտությունների ամբիոնի մեթոդաբանական սեմինարում, ՀՀԳԱ փիլիսոփայության, սոցիոլոգիայի և իրավունքի ինստիտուտի սոցիալական փիլիսոփայության բաժնում, հեղինակի 8 գիտական հոդվածներում և 2 ուսումնական թեմատիկ ձեռնարկներում:

Ատենախոսության կառուցվածքն ու ծավալը: Ատենախոսությունը բաղկացած է ներածությունից, երկու գլուխներից, եզրակացությունից և գրականության ցանկից: Աշխատության ծավալը 157 էջ է:

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ՀԱՄԱՌՈՏ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածությունում հիմնավորվել է թեմայի արդիականությունը, ներկայացվել է գիտական մշակվածության աստիճանը, ձևակերպվել են հետազոտության նպատակները, խնդիրներն ու մեթոդաբանական սկզբունքները: Ներկայացվել են ատենախոսության գիտական նորույթ պարունակող դրույթները, տեսական ու գործնական նշանակությունը:

Առաջին գլուխը՝ «Անվտանգությունը որպես սոցիալ-փիլիսոփայական վերլուծության օբյեկտ» նվիրված է «անվտանգություն», «տեղեկատվայնացում» և «տեղեկատվական հասարակություն» հասկացությունների բովանդակային ծանրաբեռնվածության պարզաբանմանն ու սոցիալ-փիլիսոփայական բնութագրությանը: Բացահայտվել են դրանց փոխհարաբերության առանձնահատկություններն ու գործառնական նշանակությունը տեղեկատվական անվտանգության ապահովման գործընթացներում:

Առաջին՝ «Անվտանգության հասկացության սոցիալ-փիլիսոփայական բնութագրությունը» ենթագլխում մեկնաբանվում է հետազոտության հիմնային հասկացություններից մեկը՝ «անվտանգությունը»: Ներկայացվել է հասարակական անվտանգության ըմբռնման հայեցակարգային էվոլյուցիան, ինչը թույլ է տվել հասկանալ, որ «անվտանգություն» հասկացությունը պատմականորեն փոխակերպվել և զարգացում է ապրել, սակայն անվտանգության երևույթի ընկալումը սկզբունքորեն մնացել է նույնը՝ ինքնապահպանում և սպառնալիքի բացակայություն: Առանձնացվել և վերլուծվել են «ազգային անվտանգություն» հասկացության իմաստավորման հիմնական մեթոդաբանական մոտեցումները: Հիմնավորվել է տեսակետ, որ համակարգային մոտեցման տեսանկյունից՝ անվտանգության ապահովումը գոյության պայմաններին տիրապետելու և, միաժամանակ, սուբյեկտի ազատության՝ որպես սեփական գոյության պայմանները վերահսկելու ունակության հաստատման համալիր գործընթաց է:

Այս և մյուս մոտեցումների սոցիալ-փիլիսոփայական վերլուծությունը հնարավորություն է տվել համակողմանիորեն ուսումնասիրել անվտանգության ֆենոմենը, ըմբռնել ազգային անվտանգության էությունը և այն սահմանել անվտանգության ապահովման օբյեկտիվ և սուբյեկտիվ կողմերի միասնության միջոցով, բացահայտել անվտանգություն կատեգորիայի բովանդակությունն ու նշանակությունը սոցիալական փիլիսոփայության այնպիսի հիմնարար հասկացությունների հետ դրա հարաբերակցության մեջ, ինչպիսիք են հասարակության քաղաքական, սոցիալ-տնտեսական, մշակութային համակարգերը, ազգային համակարգն ու ազգային շահերը:

Ըստ Վ. Մանիլովի՝ ազգային անվտանգությունը մի համակարգ է, որի բաղկացուցիչ տարրերն են սպառնալիքները, շահերը և դրանց վրա ազդելու գործոնները, ինչպես նաև ազգային անվտանգությունն ապահովելու եղանակները[2]:

---

[2] *Манилов В.Л.*, Угрозы национальной безопасности России, «Военная мысль»,1996, №1, с. 7-18.

Ազգային շահերը, ռեսուրսները, արժեքները և դրանց համապատասխան ինստիտուտները նշանակալից չափով որոշում են ազգային անվտանգության ապահովվածության իրական մակարդակը: Այս մեթոդաբանական դիրքորոշման շրջանակներում հստակորեն ուրվագծվում է ազգային անվտանգության սոցիալ-փիլիսոփայական վերլուծության ելակետային տեսական նախադրյալը, պատկերացումը անձի, հասարակության և պետության շահերի, արժեքների, ռեսուրսների և ազգային անվտանգության բնականոն կապի մասին:

Ազգային անվտանգությունը, լինելով բարդ, բազմատեսակ գործառութային համակարգ, ներառում է բազմաթիվ բաղադրիչներ: Առանձնացվել են այդ բաղադրիչները՝ ռազմական, քաղաքական, տնտեսական, սոցիալական, սոցիոմշակութային, էկոլոգիական և տեղեկատվական: Այս բաղադրիչների սոցիալ–փիլիսոփայական վերլուծությունը հնարավորություն է տվել անվտանգությունը կենսագործունեության այս կամ այն կողմի հետ նույնացման հարթությունից փոխադրել ազգային անվտանգության փիլիսփայական բնութագրման հարթության վրա:

Երկրորդ՝ «Տեղեկատվական գործընթացները բնութագրող հասկացությունների հայեցակարգային վերլուծությունը» ենթագլխում ուսումնասիրվում են «տեղեկատվություն», «տեղեկատվական պաշար» և «տեղեկատվայնացում» հասկացությունների փիլիսոփայական և համագիտական տեսանկյունները տեղեկատվական զարգացումների համատեքստում: Միանգամայն ակներև է, որ սկզբունքորեն նոր տեղեկատվական իրադրությունը պահանջում է մշակել տեղեկատվական զարգացման միտումների ուսումնասիրության ավելի լայն կոնցեպտուալ ցանց: Տեղեկատվությունը՝ «տեղեկատվական պաշարներ» եզրույթի վերլուծության ելակետային մեկնակետն է: Դա նշանակում է, որ անհնար է վերլուծել «տեղեկատվական պաշար» հասկացությունն առանց «տեղեկատվություն» հասկացության նախնական քննարկման: Տեղեկատվություն հասկացության բազմաթիվ սահմանումների վերլուծությունն ու հիմնային առանձնահատկությունների բացահայտումը թույլ է տալիս եզրակացնել, որ տեղեկատվությունն ամենևին էլ ինչ-որ պարզ «տվյալների» համախումբ չէ: Իրականում այդ «տվյալները» հասկացման, իմաստավորման արդյունք են: Տեղեկատվության, որպես հասարակության հիմնային ռեսուրսի, օգտագործումը պահանջում է, նախևառաջ, բարձրացնել առանձին մարդու մտավոր և սոցիոմշակութային հասունության, իրազեկվածության մակարդակը: Առանձին անհատի մտավոր մակարդակի բարձրացումը հանգեցնում է, ի վերջո, ողջ հասարակության ինտելեկտուալացմանը, ինչը՝ տեղեկատվայնացման համալիր գործընթացի անհրաժեշտ բաղադրիչն է:

Փոփոխվող տեղեկատվական իրականության փիլիսոփայական իմաստավորումն «տեղեկատվայնացում» հասկացության միջոցով թույլ է տվել հստակեցնել մեր պատկերացումները տեղեկատվական փոխակերպումների էության, վտանգների և սպառնալիքների բնույթի ու հեռանկարների մասին: Սոցիալ-փիլիսոփայական իմաստով՝ դինամիկորեն զարգացող ժամանակակից հասարակության տեղեկատվայնացումը տեխնոլոգիական, քաղաքական և սոցիոմշակութային գործունեության

առանձնահատուկ մի տեսակ է, որը նպատակաուղղված է տեղեկատվական հասարակության, տեղեկատվական քաղաքակրթության կազմավորմանը:

Երրորդ՝ «Տեղեկատվական հասարակություն. տեսական մեկնությունների յուրահատկությունները» ենթագլխում վերլուծվում են «տեղեկատվական հասարակության» տարբեր հայեցակարգեր, որոնք հնարավորություն են տվել բացահայտել տեղեկատվական հասարակության կառուցվածքն ու առանձնահատկությունները և պարզել տեղեկատական զարգացման նոր ձևերն ու տեղեկատվական անվտանգության հիմնահարցերի կոորդինատները:

Այսօր փիլիսոփաների և սոցիոլոգների շրջանակներում ընդհանուր համաձայնություն կա այն հարցում, որ ժամանակակից հասարակության վիճակը սկզբունքորեն տարբերվում է զարգացման նախորդ փուլերից, տեսաբանները տարբեր կերպ են անվանում նոր հասարակությունը. «հետարդյունաբերական» (Դ. Բել), «հետկապիտալիստական» (Ռ. Դարենդորֆ), «էլեկտրոնային հասարակություն» (Մ. Մաքլուեն), «ցանցային հասարակություն» (Մ. Կաստելս), «գերարդյունաբերական» (Է. Թոֆլեր), «տեխնոտրոն» (Զ. Բժեզինսկի) և այլն:

Տեղեկատվական հասարակության որպես հետարդյունաբերական հասարակության առավել հետաքրքիր և հիմնավորված սոցիալ-փիլիսոփայական հայեցակարգերից մեկը մշակել է հայտնի ամերիկացի սոցիոլոգ և փիլիսոփա Դանիել Բելը: Դ. Բելը շեշտադրում է հեռահաղորդակցության դերը, որպես նոր կենսաձևի հաստատման հիմք: Հետարդյունաբերական հասարակության կազմավորման և զարգացման հիմնական գործոն և ռազմավարական պաշար է համարում ինտելեկտուալ տեխնոլոգիաները: Է. Թոֆլերը ուշադրությունը կենտրոնացնում է գիտելիքի ու տեղեկատվության ձեռք բերման, մշակման, պահպանման, փոխանցման, տարածման և օգտագործման հրատապ հիմնախնդիրների վրա: Համընդհանուր էլեկտրոնային փոխկապակցվածությունը, ըստ Մարշալ Մաքլուենի, ի վերջո, երկրագունդը կվերածի մեկ «գլոբալ համայնքի»: Մանուել Կաստելսը ձևակերպել է մի ամբողջական հիմնավորված սոցիալական տեսություն, որը թույլ է տալիս գնահատել տեղեկատվական տեխնոլոգիաների մեջ տեղի ունեցող հեղափոխական վերափոխումները, որոնք ընդգրկել են մարդկային գործունեության բոլոր բնագավառները: Նա ուրվագծել է տեղեկատվական-տեխնոլոգիական հարացույցի սահմանները՝ իրենց բնութագծերով: «Ցանցային հասարակություն» եզրույթը սոցիոլոգիական գրականության մեջ ներմուծել է Մ. Կաստելսն իր «Ցանցային հասարակության առաջացումը» գրքում:

Տեղեկատվական հասարակության տեսական ըմբռնման մեկնաբանության առանձին նրբերանգները, որոնք առկա են տարբեր հետազոտողների մոտ, չեն փոխում տեղեկությունների և տեղեկատվական տեխնոլոգիաների դերի վերաբերյալ նրանց տեսակետների ընդհանրությունը: Ժամանակակից տեղեկատվական (ցանցային) տեխնոլոգիաները առօրյա կյանքում իրենց գործածության ոլորտների ընդլայնմանը զուգահեռ.

- հասարակությունը դարձրել են ավելի խոցելի՝ ուժեղացող քաղաքական վերահսկողության տեսանկյունից,

- ստեղծել են անձի, սոցիալական խմբերի և հասարակությունների վրա ձեռնածուական (մանիպուլյատիվ) ներգործության տեղեկատվական նոր տեխնոլոգիաների առաջացման իրական հնարավորություն,
- ստեղծել են հասարակական և անհատական անվտանգությանը սպառնացող նոր մարտահրավերներ և սպառնալիքներ:

Երկրորդ՝ «Տեղեկատվական անվտանգությունը որպես հասարակության կայուն զարգացման չափանիշ» գլխում ներկայացվում է տեղեկատվական անվտանգության ընդհանուր բնութագիրը, դրսևորման ձևերը համաշխարհային տեղեկատվական հասարակության կազմավորման պայմաններում, վերլուծվում են տեղեկատվական ռիսկերի և սպառնալիքների նոր իրադրությունը, Հայաստանի Հանրապետության տեղեկատվական անվտանգության ռազմավարության լրամշակման հրատապ խնդիրները:

Առաջին՝ «Տեղեկատվական անվտանգություն հասկացության ընդհանուր բնութագիրը» ենթագլխում վերլուծվում են «տեղեկատվական անվտանգություն» հասկացության բնորոշման մեթոդաբանական չափանիշները, բացահայտվում է տեղեկատվական անվտանգության էությունն ու կառուցվածքային բովանդակությունը: Տեղեկատվության անվտանգությունը՝ ազգային սոցիումի այնպիսի վիճակն է, որի դեպքում անձի, հասարակության և պետության հուսալի և համակողմանի պաշտպանությունն ապահովված է՝ ամեն տեսակի տեղեկատվական վտանգներից և սպառնալիքներից, ծայրահեղականորեն տրամադրված քաղաքական և սոցիալական ուժերից[3]: Հետևաբար, տեղեկատվական անվտանգությունը ցանկացած տեղեկատվական վտանգի հաղթահարման համալիր գործընթաց է, որի սոցիալ-փիլիսոփայական ըմբռնումը բնութագրում է տեղեկատվության, դրա արտադրության, մշակման և պահպանման միջոցների, տեղեկատվական ենթակառուցվածքի, տեղեկատվության հավաքմամբ, ձևավորմամբ, տարածմամբ ու օգտագործմամբ զբաղվող սուբյեկտների, ինչպես նաև այդ ոլորտում հասարակական հարաբերությունները կարգավորող համակարգի ամբողջականությունը:

Տեղեկատվական անվտանգության հայեցակարգային ըմբռնման համար պահանջվում է տեղեկատվական հարաբերությունների սուբյեկտների, նրանց շահերի և պահանջմունքների համակարգային վերլուծություն, որոշվում են տեղեկատվական անվտանգության օբյեկտը և սուբյեկտը, հետազոտման առավել հեռանկարային ուղղությունները:

Առանձնացվում և մեկնաբանվում է տեղեկատվական անվտանգությունը որպես ազգային անվտանգության կարևոր բաղադրիչ, վերլուծվում են ազգային անվտանգության ապահովման համակարգում տեղեկատվական անվտանգության դերի ուժեղացման միտումները: Անվտանգության այս կամ այն տեսակի առաջնահերթությունը որոշվում է՝

---

[3]Տես՝ ***Иващенко Г. В.***, Доктрина информационной безопасности и методические проблемы теории безопасности. Материалы круглого стола''Глобальная информатизация и социально-гуманитарные проблемы человека, культуры, общества'', МГУ, окрябрь, 2000, էջ 56-58:

- քաղաքացիների, հասարակության, պետության և միջազգային հանրության գործառության և զարգացման պահանջմունքներով,
- մարդկանց և պետության կենսականորեն կարևոր քաղաքական և մշակութային օբյեկտների աճող խոցելիությամբ,
- վտանգների և սպառնալիքների լայն շրջանակով, որոնց կոչված է դիմակայելու և հակազդելու անվտանգության կոնկրետ համակարգը:

Ակներև է, որ նշված բոլոր գործոնները կիրառելի են նաև տեղեկատվական անվտանգության նկատմամբ:

Տեղեկատվական անվտանգության երևույթը իմաստավորելիս կարևորվել են ոչ թե մասնավոր իմացաբանական խնդիրները, այլ տեղեկատվական անվտանգության՝ որպես սոցիալ-քաղաքական համակրգի յուրօրինակ բաղադրիչի բնութագրումը, ինչը հնարավորություն է ստեղծել տալ «տեղեկատվական անվտանգության» ֆենոմենի ամբողջական նկարագիրը:

Երկրորդ՝ «Ժամանակակից տեղեկատվական սպառնալիքների և վտանգների կառուցվածքային վերլուծությունը» ենթագլուխում պարզաբանվում են տեղեկատվական ոլորտում հասարակության և պետության շահերին սպառնացող վտանգներն ու սպառնալիքները, որոշվում է դրանց բնույթը, տեսակը, աղբյուրը և ուղղությունը: Տեղեկատվական սպառնալիքների նոր իրադրությունը պահանջում է մշակել դրանց բացահայտման ավելի լայն կոնցեպտուալ ցանց: Դրանց թվում առանձնացվել են «տեղեկատվական պայքար», «տեղեկատվական հակամարտություն», «տեղեկատվական պատերազմ», «տեղեկատվական կեղծիք» (ֆեյք), «տեղեկատվական մանիպուլյացիա» և այլ հասկացությունները:

Հետազոտվում են տեղեկատվական պայքարի ձևերը՝ տեղեկատվական հակամարտություն և տեղեկատվական պատերազմ: Տեղեկատվական պայքարը տեղեկատվական հարաբերությունների առանձնահատուկ ձև է, որն ըստ էության հակադիր կողմի տեղեկատվական միջավայրի վրա ներգործության քաղաքական, տնտեսական, դիվանագիտական, ռազմական և այլ եղանակների և միջոցների ամբողջություն է: Տեղեկատվական պայքարի ձևերի համակարգում հատուկ տեղ է զբաղեցնում տեղեկատվական հակամարտությունը, որն իրականացվում է տեղեկատվական անվտանգության պետական մարմինների կողմից ընդդեմ այն ուժերի, որոնք կանխամտածված կերպով ստեղծում են տեղեկատվական սպառնալիքներ՝ անձի, հասարակության և պետության կենսականորեն կարևոր շահերի համար: Տեղեկատվական հակամարտության բովանդակության մեջ, բացի տեղեկատվական ապահովումից և տեղեկատվական պաշտպանությունից, մտնում է տեղեկատվական հակազդեցությանն ուղղված միջոցառումների ողջ համալիրը: Տեղեկատվական հակամարտության ձևերից են տեղեկատվական մանիպուլյացիան և տեղեկատվական կեղծիքը (ֆեյք): Առանձնացվել և մեկնաբանվել են տեղեկատվական մանիպուլյացիայի և ֆեյքերի տեսակներն ու գործարկման մեխանիզմները:

Այսօր տեղեկատվական պայքարը և դիմակայությունը շարունակվում է համացանցում՝ կիբեռպատերազմի, ցանցային պատերազմի և դրանց բաղադրիչների տեսքով: Այդ կապակցությամբ հատկապես կարևորվել է

«տեղեկատվական պատերազմ», «կիբեռպատերազմ», «ցանցային պատերազմ» հասկացությունների հարաբերակցության համալիր վերլուծությունը: Համացանցը ստեղծում է հասարակական գիտակցության և վարքի վրա մանիպուլյատիվ (ձեռնածուական) ներգործության հսկայական հնարավորություններ: Խոսքն, ըստ էության, հասարակական գիտակցության միտումնավոր փոխակերպման-աղավաղման, ինչպես նաև սոցիալական վարքի կազմալուծման-քայքայման մասին է: Հայաստանը, Արցախը, առհասարակ համայն հայությունը՝ անկախ իր բնակությաան վայրից, այսօր դարձել են ադրբեջանական և թուրքական հաքերային խմբերի տեղեկատվական հարձակումների հիմնական թիրախները:

Երրորդ՝ «Տեղեկատվական հակամարտությունների կառուցվածքը և անվտանգության հիմնախնդիրները» ենթագլխում առանձնացվել և մեկնաբանվել են տեղեկատվական մանիպուլյացիայի տեսակներն ու կիրարկման մեխանիզմները: Ժամանակակից հետխորհրդային հասարակություններում քաղաքացիների վարքի և գիտակցության վրա մանիպուլյատիվ ներգործությունը հասել է այնպիսի մասշտաբների, որ լուրջ սպառնալիք է ստեղծել անձանց և այդ հասարակությունների տեղեկատվական-հոգեբանական անվտանգության համար: Այսօր մարդկությունը թևակոխել է «տեղեկատվական պայթյունի» դարաշրջանը, որտեղ մեծ տարածում են ստացել տեղեկատվական մանիպուլյացիայի նոր տեխնոլոգիաները: Ցանկացած ժամանակակից ռազմական գործողություն՝ ուժի ցուցադրումից սկսած, ուղեկցվում է դրա տեղեկատվական ապահովմանն ուղղված որոշակի քայլերով: Տեղի է ունենում ռազմական քաղաքականության յուրօրինակ վիրտուալացում: Դա նշանակում է, որ ռազմական քաղաքականության գործադրման հիմնական դաշտը փոխադրվում է կիբեռտարածք: Այստեղ տեղեկատվության՝ որպես ռազմավարական ռեսուրսի համար մղվող դաժան պայքարն ավելի ու ավելի մեծ չափերով սկսում է ենթարկվել համացանցի տրամաբանությանը, դրա պահանջներին: Այս տեսանկյունից համացանցը ստեղծում է հասարակական գիտակցության և վարքի վրա մանիպուլյատիվ ներգործության հսկայական հնարավորություններ:

Արդի աշխարհում տեղեկատվական պայքարը և դիմակայությունը շարունակվում է համացանցում՝ կիբեռպատերազմի, ցանցային պատերազմի և դրանց բաղադրիչների տեսքով: Այդ կապակցությամբ հատկապես կարևորվել է «տեղեկատվական պատերազմ», «կիբեռպատերազմ», «ցանցային պատերազմ» հասկացությունների հարաբերակցության համալիր վերլուծությունը: «Ցանցային պատերազմ», «կիբեռպատերազմ», հասկացությունները՝ ժամանակակից պատերազմի, ռազմական կոնֆլիկտների նպատակների և խնդիրների ըմբռնման նոր որակական մակարդակ են: Դա նշանակում է, որ տեղեկատվական դարաշրջանում արմատապես փոխվում է պատերազմի փիլիսոփայությունը:

Չորրորդ՝ «Հայաստանի տեղեկատվական անվտանգության ռազմավարության առաջնահերթութերը» ենթագլխում քննարկվում են Հայաստանի տեղեկատվական անվտանգության ապահովման ռազմավարության իրականացման առաջնային խնդիրները: Ռազմավարությունն անհրաժեշտ է որպես Հայաստանում

տեղեկատվական հասարակության, կամ, որ նույնն է՝ «գիտելիքների հասարակության» հիմնապայման:

Հայաստանի պետական տեղեկատվական քաղաքականության հայեցակարգը մշակելիս հարկավոր է հաշվի առնել երկու հիմնարար սկզբունքներ. 1. տեխնիկատեխնոլոգիական՝ կապված Հայաստանում տեղեկատվական հասարակության անցման տեխնիկատեխնոլոգիական հենարանի ստեղծման հիմնախնդրի հետ: 2. Սոցիալ-քաղաքական, որը պետք է նպաստի տեղեկատվական հասարակության պայմաններում հայ հասարակության այդ կենսաձևի նախապատրաստելու սոցիալական, օրենսդրական, բարոյահոգեբանական խնդիրների լուծմանը:

Ժամանակակից հայ հասարակությունը տեղեկատվական անվտանգության ապահովման կազմակերպական միջոցների գործուն համակարգի կարիքն ունի, որը ունակ կլինի ոչ միայն արագ և արդյունավետորեն հակազդելու առաջացող տեղեկատվական սպառնալիքներին, այլև կանխելու և կասեցնելու դրանց առաջացումը: Դրանք լրջորեն խոչընդոտում են ՀՀ տեղեկատվական անվտանգության ապահովման համակարգի կազմավորման գործընթացների արդյունավետ կառավարումն ու երկրի հետագա կայուն զարգացումը: Պահանջվում է, մի կողմից, մշակել ՀՀ տեղեկատվական անվտանգության համալիր ծրագիր, իսկ մյուս կողմից՝ էլ ավելի հստակեցնել Հայաստանի տեղեկատվական անվտանգության քաղաքականության առաջնահերթությունները: Դրա համար կպահանջվի հայկական պետության և քաղաքացիական հասարակության լայն համագործակցությունը՝ հայ ժողովրդի առաջ ծառացած տեղեկատվական մարտահրավերների և սպառնալիքների վերլուծության-պարզեցման նպատակով: Միայն այդ դեպքում հնարավոր կլինի մշակել տեղեկատվական անվտանգության քաղաքականության առաջնահերթությունների հանարայնորեն արժևորված համակարգ: Դրա կարևոր մասը պետք է կազմի Հայաստանի տեղեկատվական անվտանգության առաջ ծառացած վտանգների և սպառնալիքների ազգային մշտադիտարկման համակարգը: Վերջինիս կարևորագույն գործառույթն է՝ գնահատել իրականացվող տեղեկատվական անվտանգության քաղաքականությունը այն տեսանկյունից, թե որքանով է դա համապատասխանում Հայաստանի ազգային անվտանգության ամրապնդման շահերին, ինչը կարող է լինել տեղեկատվական անվտանգության ապահովման ընտրված միջոցների քաղաքական արդյունավետության կարևոր ցուցանիշը: Տեղեկատվական քաղաքականության արդյունավետությունը հնարավոր է միայն այն դեպքում, երբ հասարակության տեխնիկական-տեխնոլոգիական, սոցիալ-տնտեսական, քաղաքական և կրթամշակութային անվտանգության ապահովման հիմնախնդիրներն օրգանապես միահյուսված կլինեն մեկ միասնական տեղեկատվական անվտանգության համակարգի կազմավորման ռազմավարության մեջ:

Պետական տեղեկատվական քաղաքականության ընդհանուր հայեցակարգը պետք է դառնա մեթոդաբանական հիմք Հայաստանի տեղեկատվական անվտանգության հայեցակարգի ձևավորման համար: Տեղեկատվական

անվտանգության հայեցակարգի ձևավորման մյուս աղբյուրը պետք է դառնա Հայաստանի ազգային անվտանգության՝ արդեն մշակված և ընդունված դոկտրինը:

Եզրակացությունում ամփոփվել են հետազոտության արդյունքները և ձևակերպվել են մի շարք հիմնարար եզրահանգումներ:

Տեղեկատվական հասարակության հայեցակարգերի մեթոդաբանական վերլուծությունը հնարավոր է դարձրել Հայաստանում տեղեկատվայնացման դրսևորումների սոցիալ-տեխնոլոգիական մակարդակից անցում կատարել տեղեկատվական գործընթացների զարգացումների սոցիալ-փիլիսոփայական իմաստավորման մակարդակ և բացահայտել այն ուղենիշերը, որոնց վրա պետք է հիմնվի տեղեկատվական անվտանգության արդյունավետ քաղաքականությունը:

Տեղեկատվության շրջանառության ծավալների ու արագության ընդլայնումը մերօրյա աշխարհում տեղեկատվական զարգացվածության գլխավոր չափանիշներից է: Ուսումնասիրությունները ցույց են տալիս, որ «տեղեկատվական պաշար» հասկացությունը կարող է կիրառվել գիտական գիտելիքի և սոցիալական կյանքի բոլոր բնագավառներում՝ «տեղեկատվություն» հասկացությունից հետո այն ևս դարձել է ոչ միայն միջառարկայական, այլ նաև համագիտական կատեգորիա: Դա նշանակում է, որ «տեղեկատվություն», «տեղեկատվայնացում» և «տեղեկատվական պաշար» հասկացությունները ներառում են մի շարք տեսանկյուններներ, որոնք սերտորեն կապված են տեղեկատվական անվտանգության ուսումնասիրության խնդրակարգի հետ:

Քննարկելով հայ հասարակության և պետության առաջ ծառացած տեղեկատվական սպառնալիքների և տեղեկատվական անվտանգության խնդրակարգի սոցիալ-փիլիսոփայական վերլուծության հարցերը՝ հետազոտության մեջ հիմնավորվում է Հայաստանի տեղեկատվական հայեցակարգի համալիր հետազոտության և լրամշակման անհրաժեշտությունը: Պետական տեղեկատվական քաղաքականության ընդհանուր հայեցակարգը պետք է մեթոդաբանական հիմք ծառայի Հայաստանի տեղեկատվական անվտանգության հայեցակարգի ձևավորման համար: Մեկ այլ աղբյուր պետք է դառնա արդեն մշակված և ընդունված՝ Հայաստանի ազգային անվտանգության դոկտրինը:

Հետազոտության շրջանակներում կատարված ուսումնասիրությունները վկայում են, որ Հայաստանում տեղեկատվայնացման գործընթացների ներազդեցության շնորհիվ հասարակական և ազգային կյանքի բոլոր ոլորտները աստիճանաբար ձեռք են բերում ճկունության և շարժունակության նոր որակներ: Սակայն միաժամանակ աճել են անձի, հասարակության և պետության խոցելիության աստիճանն ու հնարավորությունները, որոնք կապված են տեղեկատվական սպառնալիքների նոր ձևերի ակտիվացման հետ: Դրանք պահանջում են մշակել այդ սպառնալիքներին հակադարձելու համարժեք և արդյունավետ միջոցներ:

Լուրջ թերություն է մշակված և հստակ ձևակերպված տեղեկատվական անվտանգության քաղաքականության ռազմավարության բացակայությունը, որի առկայության դեպքում բազմաթիվ սխալներ կարող էին ժամանակին կանխարգելվել: Արդի փուլում անհրաժեշտ է մշակել տեղեկատվական անվտանգության ապահովման դինամիկ մոդելներ: Այդպիսիք մշակվել են

Արևմուտքի երկրներում, որոնք ունակ են արագ ընկալելու և յուրացնելու իրենց փոխակերպող ներքին և արտաքին ազդակները, սպառնալիքների կանխարգելման, ինչպես նաև դրանց չեզոքացման տեղեկատվական մեխանիզմները:

Քանի որ բացասական տեղեկատվական ներգործությունը շոշափում է հայ հասարակության և անհատի շահերը, տեղեկատվական անվտանգության քաղաքականության ըմբռնումը զուտ տեխնոլոգիականից պետք է շրջվի դեպի հումանիտար ըմբռնումը: Խնդիրն այն է, որ մեզանում արդյունավետ տեղեկատվական քաղաքականության մշակման թերագնահատումը կապված է կառավարող ընտրանու միակողմանի տեխնոկրատական մտածողության հետ: Միայն այն դեպքում, երբ Հայաստանում սոցիալական առաջընթացի տեխնիկա-տեխնոլոգիական, սոցիալ-տնտեսական և հումանիտար հարցերը փոխկապակցված կլինեն միասնական տեղեկատվական քաղաքականության մեջ, երկիրը կունենա արդյունավետ տեղեկատվական անվտանգության քաղաքականություն մշակելու և իրականացնելու ռեալ հնարավորություն: Այդ փոխակերպման կառավարումը և կարգավորումը պետք է իրականացնի Հայաստանի իրավաքաղաքական համակարգի գլխավոր սուբյեկտը՝ ազգային պետությունը: Ընդ որում, կառավարումը պետք է իրականացվի լրամշակված պետական տեղեկատվական քաղաքականության հայեցակարգի հիման վրա:

Ատենախոսության մեջ առանձնահատուկ ուշադրության է արժանացել այն հանգամանքը, որ Հայաստանում տեղեկատվայնացման գործընթացի դրական արդյունքների հետ մեկտեղ արդեն դրսևորվել են նաև դրա բացասական ազդեցությունները, որոնք կապված են այնպիսի տարատեսակ վտանգների և սպառնալիքների հետ, ինչպիսիք են՝ թվային անհավասարությունը, կիբեռհանցագործությունները, համակարգչամոլությունը, անձնական կյանքի լիակատար վերահսկողության և անհատի վրա մանիպուլյատիվ ներգործության հնարավորությունները: Դրանք կապված են տեղեկատվական հակամարտության և տեղեկատվական, ցանցային և, այսպես կոչված, «ֆեյքային» պատերազմների նոր ձևերի և տարատեսակությունների հետ: Վերլուծելով այս երևույթները, հետևություն է արվում, որ անհրաժեշտ է Հայաստանում մշակել տեղեկատվական հակամարտությունների դրսևորումների և մեխանիզմների բացահայտման ավելի լայն «կոնցեպտուալ ցանց», երբ «տեղեկատվական հակամարտություն» հասկացությունը հարստացվում է մի շարք լրացուցիչ բնութագրիչներով: Այդ նպատակով վերլուծության են ենթարկվել «ցանցային պատերազմ», «ֆեյք», «ֆեյքային պատերազմ», «կիբեռպատերազմ», «մանիպուլյատիվ գիտակցություն», «հոգեբանական անվտանգություն» հասկացությունները:

Կատարված հետազոտությունների արդյունքում կարելի է պնդել, որ այսօր տեղեկատվական պատերազմներն՝ իրենց տեղեկատվական-հոգեբանական և տեխնիկական բաղադրիչներով, Հայաստանի ազգային անվտանգության հիմնական սպառնալիքներից մեկն են դարձել:

Օրենսդրական մակարդակում բավարար հստակեցված չեն տեղեկատվական սպառնալիքներից ՀՀ քաղաքացիների գործուն պաշտպանության երաշխիքները, որոնք կապված են բացասական տեղեկատվական ներգործությունների հետ: Դա

վկայում է ազգային օրենսդրության՝ միջազգային իրավունքի նորմերի տեսանկյունից, հետագա լրամշակման անհրաժեշտության մասին:

Ժամանակակից Հայաստանում կազմավորված տեղեկատվական անվտանգության ապահովման համակարգը դեռևս չի կարողանում ժամանակին և արդյունավետորեն դիմակայել նոր տեղեկատվական սպառնալիքներին և մարտահրավերներին: Դրա համար պահանջվում է, **նախ,** մշակել և ընդունել օրենք «Տեղեկատվական-հոգեբանական անվտանգության մասին»: Կարևոր հետևություններից մեկն էլ այն է, որ անձի, հասարակության և պետության տեղեկատվական-հոգեբանական անվտանգության ապահովման իրավական, սոցիալ-կառուցվածքային մեխանիզմների համակողմանի վերլուծությամբ, հստակեցմամբ, դրանց արդյունավետ գործառնությամբ է պայմանավորված անձի, հասարակության և պետության պաշտպանվածության մակարդակը:

Հայեցակարգային և գործնական առումներով անհրաժեշտ է մշակել Հայաստանի սկզբունքորեն նոր տեղեկատվական անվտանգության քաղաքականություն, որը կոչված կլինի առավել արդյունավետորեն պաշտպանելու պետության շահերը, ինչպես նաև ստեղծելու բարենպաստ պայմաններ տեղեկատվական անվտանգության ողջ համակարգի արդյունավետ գործառնության համար և առաջին հերթին ապահովելու պետական, քաղաքական, տնտեսական և հոգևոր շահերի պաշտպանությունը տեղեկատվության ոլորտում: Հայսատանի Հանրապետության համար անհրաժեշտություն է նոր մարտահրավերներին և սպառնալիքներին հակազդելու ունակ, հստակ մշակված տեղեկատվական անվտանգության ռազմավարություն ունենալը: Ատենախոսության շրջանակներում իրականացված ուսումնասիրությունները թույլ են տալիս նկատել, որ ներկայիս ռազմավարությունն իրագործվում է թույլ, անհետևողական կերպով: Այն լուրջ ճշգրտումների կարիք ունի: Դրա համար պահանջվում է Հայաստանում տեղի ունեցող տեղեկատվական փոփոխությունների և կուտակված համաշխարհային փորձի սոցիալ-փիլիսոփայական խորը իմաստավորում և համակողմանի հետազոտություն: Քանի դեռ այս ամենը չի արված, սխալները, որպես կանոն, կհայտնաբերվեն հետին թվով, երբ հայկական պետությունը կշարունակի ետ մնալ զարգացման տեմպերով:

Երկրորդ՝ հստակեցման կարիք ունի ՀՀ պետական տեղեկատվական քաղաքականությունը, մասնավորապես պահանջվում է որակապես բարձրացնել պետական գերատեսչությունների և կազմակերպությունների, ինչպես նաև քաղաքացիական հասարակության ինստիտուտների գործունեության կոորդինացման և գործակցության մակարդակը:

Երրորդ՝ ժամանակակից հայ հասարակությունը կենսականորեն շահագրգռված է այնպիսի պետական տեղեկատվական կառուցվածքների գործունեությամբ, որոնց օգնությամբ կարելի կլինի արտասահմանյան լսարանում արմատավորել հայ իրականության, նրանում տեղի ունեցող իրադարձությունների, պաշտոնական և ոչ պաշտոնական կարծիքների վերաբերյալ օբյեկտիվ պատկերացումներ, հայանպաստ գնահատականներ: Այդ տեսակետից հայկական ԶԼՄ-ների գործունեությունը խորը և լուրջ կատարելագործման կարիք ունի: ԶԼՄ-ները

Հայաստանի տեղեկատվական անվտանգության ապահովման առավել կարևոր օբյեկտներից են:

Չորրորդ՝ արտերկրի հայկական դիվանագիտական ներկայացուցչություններում հարկավոր է ստեղծել հատուկ ծառայություններ՝ Թուրքիայի և Ադրբեջանի կողմից ՀՀ արտաքին քաղաքականության մասին ապատեղեկատվական, ստահոդ հերհյուրանքների տարածման հակազդմանն ու չեզոքացմանն ուղղված արդյունավետ աշխատանքի համար: Մեր հետազոտությունը ցույց է տալիս, որ այսօր, ինչպես երբեք, անհրաժեշտ է որակապես նորացնել արտերկրներում ՀՀ քաղաքացիների և իրավաբանական անձանց իրավունքների և ազատությունների խախտումների հակազդման տեղեկատվական ապահովումը:

Հինգերորդ՝ աշխարհում ընդհանրապես, և Սփյուռքում հատկապես, Հայաստանի տեղեկատվական ազդեցության արդյունավետության ամրապնդումը անհրաժեշտ է դիտել որպես ոչ միայն ՀՀ տեղեկատվական քաղաքականության ռազմավարական կարևորագույն ռեսուրս, այլև ազգաշահ գործընկերության հիմունքներով համահայկական ջանքերի կորդինացման ու համախմբման կարևորագույն գործոն:

Ատենախոսության հիմնական դրույթներն արտացոլվել են հեղինակի հետևյալ հրապարակումներում.

1. Ինֆորմացիոն անվտանգության ֆունկցիոնալ վերլուծությունը: «Գարուն», N7-8, Երևան, 2008, էջ 46-51:
2. Ինֆորմացիոն հակամարտությունը նոր դարաշրջանում: «Կանթեղ», գիտական հոդվածների ժողովածու, Երևան, 2008, էջ 137-143:
3. Տեղեկատվական վերազինում, գլոբալացում և ազգային անվտանգություն: «Լրաբեր – 75», գիտական և մեթոդական հոդվածների ժողովածու, ԵՊՃՀ, Երևան, 2008, էջ 896-899:
4. Տեղեկատվական տեխնոլոգիաների զարգացման սոցիոմշակութային որոշ հիմնախնդիրներ: «Կանթեղ», գիտական հոդվածների ժողովածու, Երևան, 2014, էջ 321-328:
5. Տեղեկատվական անվտանգության դերը ժամանակակից մարտահրավերների հաղթահարման գործում (ուսումնական թեմատիկ ձեռնարկ), Նաիրի, Երևան, 2014, 119 էջ:
6. Զանգվածային տեղեկատվական միջոցները որպես մանիպուլյացիոն հզոր զենք: «Կանթեղ», գիտական հոդվածնեի ժողովածու, Երևան, 2015, 214-221էջ:
7. Տեղեկատվական բաղադրիչի ներառումը անվտանգության համակարգում: «Լրաբեր», գիտական հոդվածների ժողովածու, ԵՊՃՀ, Երևան, 2015, 811-816 էջ:
8. Տեղեկատվության և տեղեկատվական տեխնոլոգիաների ներդրումը կրթական համակարգի բարեփոխումների գործընթացում (ուսումնական թեմատիկ ձեռնարկ): Նաիրի, Երևան, 2015, 118 էջ:

9. Information Security in the Sistem of Ensuring National Security. «WISDOM» Scientific Journal, N 2(9), Erevan 2017, p.92-97.
10. Տեղեկատվական հասարակության հարացույցը և ընդհանուր սոցիալ-փիլիսոփայական նկարագիրը: «Կանթեղ», գիտական հոդվածների ժողովածու, 1(74), Երևան, 2018, 144-154էջ:

Шахбазян Марине Карапетовна

ДВИЖУЩИЕ СИЛЫ ИНФОРМАТИЗАЦИИ СОВРЕМЕННОГО ОБЩЕСТВА И ПРОБЛЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: СОЦИАЛЬНО-ФИЛОСОФСКИЙ АНАЛИЗ

Диссертация на соискание учёной степени кандидата философских наук по специальности 09. 00. 01
Защита состоится 3-его июля 2020 года в 12:00 на заседании специализированного совета Философии 062 ВАК в АГПУ, по адресу: 3750010, г. Ереван, проспект Тиграна Меца 17, Армянский государственный педагогический университет имени Х. Абовяна

РЕЗЮМЕ

Проблема обеспечения безопасности социума имеет фундаментальное значение для разработки национальной политики, направленной на сохранение и воспроизводство общественной системы и реализации национальных интересов. Информационная безопасность глубоко проникла во все другие виды безопасности, стала первоочередной проблемой развития остальных видов безопасности. Сегодня информатизация общества и информационная безопасность приобрели всеобъемлющие масштабы, превратились в фактор, который в условиях образования единого мирового информационного пространства сильно влияет на сложные и противоречивые процессы существования наций и народов, всего человечества.

Выбор исследовательского дискурса становления информационного общества позволил перейти от социотехнологического уровня проявлений информатизации в Армении на уровень социально-философского обобщения основных тенденций информационного развития.

Вместе с положительными результатами процесса информатизации проявлялись и его негативные влияния, которые связаны с такими разнообразными опасностями и угрозами, как “информационное оружие”, “информационная борьба”, “информационный конфликт”, “информационная война”, “информационная подделка” (фейк), “информационная манипуляция” и другие негативные явления.

Все это придало особую насущность проблематике информационной безопасности, комплексное исследование которой может довести негативные влияния, опасности и угрозы информатизации до минимума. По отношению к другим видам безопасности элементы информационной безопасности выступают в качестве системообразующего фактора.

Недооценение проблем информационной безопасности может привести к трудно предсказуемым социальным, политическим, экономическим, военным и другим негативным последствиям. Анализ проблем обеспечения информационной безопасности РА показывает, что нынешнее состояние этой системы характеризуется с одной стороны усилением уже существующих опасностей и угроз, а с другой стороны – возникновением новых угроз и вызовов. Самый главный из них – активизация информационно-психологической войны, развязанной Турцией, Азербайджаном и протурецкими силами против Армении. В этих условиях Республика Армения должна

прилагать исключительные усилия в направлении обеспечения действенной защиты своих национальных и государственных интересов, разработать национальную стратегию и новую, модернизированную концепцию информационной безопасности для эффективного противодействия новым вызовам и угрозам.

Новая политика информационной безопасности Армении должна уреголировать информационные отношение, обеспечить системную защиту интересов всех участников. Продуктивность токой политики возможна только тогда, когда проблемы обеспечения технической-технологической, социально-экономической, политической и оброзовательно-культурной безопасности общества будут органически сплетени в единую систему информационной безопасности.

Shahbazyan Marine Karapet

DRIVING FORCES OF MODERN SOCIETY INFORMATIZATION AND MAJOR INFORMATION SECURITY ISSUES: SOCIAL-PHILOSOPHICAL ANALYSIS

Thesis for Receiving Academic Degree of Candidate of Philosophical Sciences under the speciality 09.00.01

The dissertation defense will take place on 03 July 2020, at 12:00 at Kh.Abovyan Armenian State Pedagogical University at the committee meeting of Philosophy with the specialty of HCC 062.

Address: 3750010, 17 Tigran Mets Ave., Yerevan, ASPU

RESUME

The security issue of the society plays a fundamental role in the elaboration of a national policy for preservation and reproduction of the societal system and realization of national interests. The information security has deeply penetrated all other types of security and become a primary issue for the development of other kinds of security. Today the informatization of the society and the information security has reached comprehensive scales and has become a factor that under the emergence of a united world information space heavily influences the complex and contradictory processes of existence of nations and peoples, the entire humanity.

The choice of research discourse of the establishment of information society has enabled the passage from the socio-technological level of expressions of informatization in Armenia to the level of socio-philosophical generalization of main tendencies of informational development.

Together with positive results of the informatization process also negative influences have been demonstrated, which are connected with such various dangers and threats as “information arm”, “information struggle”, “information conflict”, “information war”, “information fake”, “information manipulation” and other terms.

All this has conveyed actuality to the problematics of information security, the complex study of which can minimize the negative consequences, dangers and threats of the informatization. The elements of information security act as a system-creating factor vis-à-vis other types of security.

The underestimation of information security issues may result in hardly predictable social, political, economic, military and other consequences. The analysis of the RA information security issues shows that the current state of that system is characterized on the one hand by the strengthening of already existing dangers and threats and the emergence of new threats and challenges on the other hand. Among them the most important one is the activization of information-psychological war, waged by Turkey, Azerbaijan and pro-Turkish forces against Armenia. In such conditions the Republic of Armenia should make an exclusive effort to provide an active protection to its national and state interests, elaborate a national strategy and a new, modernized concept of information security to efficiently counteract the new challenges and threats.

The new policy of information security of the Republic of Armenia is designed to regulate informational relations and provide structural protection for all the participants. The effectiveness of such policy is possible when the technical-technological, social-economical, political and educational-cultural problems of ensuring security are included in the formation of a unified information security system.