Բանբեր Երևանի համալսարանի. Միջազգային հարաբերություններ, Քաղաքագիտություն
2024, Vol. 15, No. 1(43), ապրիլ, 93-107
https://doi.org/10.46991/BYSU:D/2024.15.1.093

# ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅԱՆ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԱՐԴԻԱԿԱՆԱՑՄԱՆ ՀԻՄՆԱԽՆԴԻՐՆԵՐԸ

ՄԱՐԻԱՄ ԳԶՈՂՅԱՆ *
*ՀՀ ԳԱԱ փիլիսոփայության, սոցիոլոգիայի և իրավունքի ինստիտուտ*

Արդի միջազգային հարաբերություններում պետությունները մեծ կարևորություն են տալիս տեղեկատվական անվտանգության մեխանիզմների արդիականացման և պահպանման հիմնախնդիրներին: Հարկ է նկատել, որ տեղեկատվության դերի ու ծավալի աճին զուգահեռ՝ ավելացել են նաև տեղեկատվական անվտանգության սպառնալիքները, ուստի տեղեկատվության պաշտպանությունը դարձել է մի շարք պետությունների ներքին ու արտաքին քաղաքականության առաջնային ուղղություններից մեկը:

Մեր երկրի քաղաքական զարգացման բազմակողմ խնդիրների լուծումը և դրանց հետ կապված քաղաքական գործընթացների կանխատեսման կոնկրետ տեխնոլոգիաների և ընդհանուր մեթոդաբանության կատարելագործման գործուն միջոցների որոնումների արդիական հարցերն այսօր ակադեմիական և իշխանական շրջանակներում շատ են կարևորվում:

Գիտության ու քաղաքականության մեջ ներկայումս առավելապես ուշադրություն է դարձվում անվտանգության ոչ ռազմական կողմին: Այս պարագայում պետությունների ու միջազգային կազմակերպությունների համար հրամայական է դառնում համալիր անվտանգության ապահովումը բոլոր՝ քաղաքական, տնտեսական, սոցիալական, էկոլոգիական, ռազմական ուղղություններում: Ընդ որում, երկրները, ըստ իրենց ռեժիմի բնույթի, խնդիրը լուծում են տարբեր կերպ. մի մասը տեղեկատվական դաշտը փակում է՝ արգելելով նույնիսկ սոցիալական ցանցերի օգտագործումը, մյուսներն ավելի լիբերալ մեթոդներ են կիրառում[1]:

* **Մարիամ Գզողյան** – ՀՀ ԳԱԱ փիլիսոփայության, սոցիոլոգիայի և իրավունքի ինստիտուտի «Քաղաքական գործընթացներ և ինստիտուտներ» բաժնի հայցորդ, ՀՀ ԳԱԱ փիլիսոփայության, սոցիոլոգիայի և իրավունքի ինստիտուտի տնօրենի օգնական

**Мариам Гзогян –** Института Философии, социологии и права Национальной академии наук Армении, Соискатель кафедры Политических процессов и институтов, Заместитель директора Института Философии, социологии и права НАН РА

**Mariam Gzoghyan –** Institute of Philosophy, Sociology and Law of the National Academy of Sciences of Armenia, Applicant at the Chair of Political Processes and Institutions, Deputy Director of the Institute of Philosophy, Sociology and Law of the NAS of the RA.

Էլ. փոստ՝ mariam.gzoxyan.1998@gmail.com. ORCID: https://orcid.org/0009-0005-1655-9516.



Ստացվել է՝ 26.01.2024
Գրախոսվել է՝ 18.03.2024
Հաստատվել է՝ 08.04.2024


[1] Տե՛ս **Հայկուհի Մկրտչյան**, «Տեղեկատվական անվտանգություն» հասկացության զարգացումը, Եր., 2018, էջ 55, https://razmavaraget.files.wordpress.com/2018/03/haykuhi-mkrtchyan.pdf

Տեղեկատվական տեխնոլոգիաների առաջընթացը և հեռահաղորդակցության միջոցների ժամանակակից ձեռքբերումները միջազգային անցուդարձերում սեփական շահերը և նպատակներն առաջ մղելու կարևոր գործիք են դարձել, ուստի պետությունները ջանք ու եռանդ չեն խնայում ունենալու արհեստավարժ «տեղեկատվական բանակ» և տեղեկատվական պաշտպանված ենթակառուցվածքներ: Վերջին տարիների համաշխարհային փորձը վկայում է, որ հակառակորդի դեմ գործողությունների իրականացման համար տեղեկատվական հոսքերի ազդեցությունը կարող է պետությունների ձեռքում հզոր զենք լինել, իսկ այդ զենքին դիմագրավելու ներուժ չունեցող պետությունները կարող են հայտնվել պարտվողների շարքերում:
Հաշվի առնելով Հայաստանում տեղեկատվական և հաղորդակցական տեխնոլոգիաների զարգացման բարձր տեմպերը՝ հոդվածում վերլուծության է ենթարկվում այնպիսի արդիական խնդիր, ինչպիսին ենթակառուցվածքների պաշտպանությունն է, որն առանցքային նշանակություն ունի տնտեսության և պետության տարբեր բնագավառների կենսագործունեության համար:

**Բանալի բառեր** – *միջազգային հարաբերություններ, տեղեկատվական անվտանգություն, արդիականացում, հեռահաղորդակցություն, լիբերալ մեթոդներ, ազգային շահ*

## Տեղեկատվական անվտանգության ապահովման հիմնախնդիրները

Անդրադառնալով տեղեկատվական անվտանգությանը ՀՀ-ում՝ հարկ է նշել, որ հասարակության ներկայիս զարգացումները բնութագրվում են տեղեկատվական ոլորտի աճող դերակատարությունով: Տեղեկատվական ոլորտը տեղեկություն հավաքող, ձևավորող, տարածող և օգտագործող սուբյեկտների, տեղեկատվության և տեղեկատվական ենթահամակարգերի ամբողջությունն է, ինչպես նաև այդ գործընթացների ժամանակ առաջացող հասարակական հարաբերությունների կարգավորման համակարգ: Վերոնշյալ ոլորտը, ունենալով հասարակական կյանքի համակարգման և կարգավորման կարևոր դեր, լրջորեն ազդում է ՀՀ անվտանգության քաղաքական, տնտեսական, ռազմական և այլ բաղադրիչների վրա:

Գիտության, տեխնիկայի, արտադրության ոլորտներում արմատական փոփոխություններով բնութագրվող հետարդյունաբերական կամ տեղեկատվական հասարակության ներկայիս դարաշրջանում պետությունները բախվել են ժամանակակից գլոբալ խնդիրների լուծման անհրաժեշտությանը: Դրանցում առանցքայիններից է տեղեկատվական անվտանգության խնդիրը, որը ներթափանցում է մարդու կենսագործունեության բոլոր ոլորտները:

Անհատի շահերը տեղեկատվական ոլորտում ներառում են մարդու և քաղաքացու՝ օրենքով չարգելված գործունեություն իրականացնելու, ֆիզիկական, հոգևոր և մտավոր զարգացման համար օգտագործվող տեղեկատվության հասանելիության սահմանադրական իրավունքի իրագործումը, ինչպես նաև շրջակա միջավայրի փոփոխությունների վերաբերյալ տեղեկատվության

հասանելիությունը և անձնական անվտանգությունն ապահովող տեղեկատվության պաշտպանությունը:

Հարկ է նկատել, որ տեղեկատվական հասարակությունը սահմանվում է որպես հասարակական և արտադրական հարաբերությունների զարգացման վիճակ, որտեղ արտադրանքի հիմնական մասը ոչ թե արդյունք է նյութական արտադրության, այլ բարձր տեխնոլոգիաների՝ տեղեկատվական արտադրանք ստանալու և վաճառելու նպատակով ստեղծված մտավոր աշխատանքի արդյունք[2]:

Հասարակության շահերը տեղեկատվական ոլորտում ներառում են անձի շահերի ապահովումը, ժողովրդավարության ամրապնդումը, իրավական-սոցիալական պետության կառուցումը, հասարակական համաձայնության և հանդուրժողականության հաստատումը, ինչպես նաև հասարակության տարբեր հատվածների հոգևոր ու պատմամշակութային ժառանգության պահպանումը, ազգային արժեքների և ավանդույթների վերարտադրությունն ու զարգացումը, ազգային ինքնության հիմնասյուների՝ բարոյահոգեբանական կերտվածքի, լեզվի և ազգային եկեղեցու դերի ամրապնդումը, պետության, սփյուռքի միասնության տեղեկատվական կապի ապահովումը: Այս համատեքստում հետաքրքիր է հոգեբան Կ. Նալչաջյանի կարծիքը, ըստ որի՝ ազգային հոգեբանության նվազման և ինքնագիտակցության թուլացման հետևանքով այսօր Հայաստանը կանգնած է ազգային ինքնության վերացման սպառնալիքի առջև, որը նաև պատճառ է արտագաղթի, մշակութային, կրթական արժեքների թուլացման:

Ազգային շահերի հիմքով պետական քաղաքականությունը խնդիր ունի ապահովել պետության և հանրության անվտանգությունն ու զարգացումը: Կարևոր են ոչ միայն այդ շահերի ողջամիտ ու հստակ արժևորումը, այլ նաև ռեսուրսների այն հանրագումարի առկայությունն ու հավաքագրումը, որոնք ազգային շահերի իրականացման հնարավորություն կընձեռեն:

Ժամանակակից աշխարհում պետության հզորության ներուժն անկասկած մեծ դեր է խաղում, սակայն ազգային շահերի իրացման գործում նշանակալի դերակատարում ունեն մի շարք կարևոր գործոններ, որոնցից են՝ միջազգային հանրության դիրքորոշումը և շահերը, պետության ժողովրդավարացման աստիճանը, պետության և ազգի քաղաքակրթական զարգացվածության մակարդակը և այլն[3]:

Հայաստանի Հանրապետությունը, գտնվելով աշխարհաքաղաքական բարդ տարածաշրջանում, ներքաշված է տեղեկատվական ակտիվ ներազդեցությունների և հոսքերի մեջ: Այսօր մեր առջև ծառացած են այնպիսի խնդիրներ,

---

[2] Տե՛ս **Емельянов Г. В., Стрельцов А. А.** Проблемы обеспечения безопасности информационного общества // Распределенная конференция «Технологии информационного общества 98 – Россия», http://www.iis.ru/events/19981130/streltsov.ru.html

[3] Տե՛ս **Ա. Ղևոնդյան**, Ազգային շահերի հիմնահարցը Հայաստանի Հանրապետության անվտանգության ապահովման առաջնային միջավայրում, Եր., 2011, էջ 19:

ինչպիսիք են՝ նվազագույնի հասցնել տեղեկատվական ոլորտում ՀՀ ազգային շահերին սպառնացող վտանգների բացասական ազդեցությունը և ազգային, պետական նպատակների անվտանգ իրականացման գործընթացներում հանդես գալ նոր և ժամանակակից պահանջները բավարարող նախաձեռնություններով, ստեղծել արդի տեղեկատվական գործընթացներին համապատասխան տեղեկատվական քաղաքականության ռազմավարություն, ապահովել ՀՀ տեղեկատվական անվտանգությունը և՛ ներպետական, և՛ միջազգային հարթակներում:

Ներկայումս ՀՀ առջև ծառացած են նաև տեղեկատվական անվտանգային մի շարք խնդիրներ, ինչպիսիք են՝ կեղծ և խեղաթյուրված տեղեկատվության տարածումը, միջազգային ահաբեկչական գործունեությունը տեղեկատվական դաշտում, միջազգային տեղեկատվական աղբյուրներով հակահայկական կեղծ տեղեկատվության տարածումը, ՀՀ տեղեկատվական և հեռահաղորդակցային համակարգերի բնականոն գործունեությունը խաթարելը, տեղեկատվական միջոցների պահպանման անարդյունավետությունը:

Հատկանշական է, որ այսօր Հայաստանի Հանրապետությունում առկա են ոլորտին առնչվող հետևյալ իրավական փաստաթղթերը՝ «Պետական և ծառայողական գաղտնիքի մասին»[4], «Տեղեկատվության ազատության մասին»[5], «Արխիվային գործի մասին»[6], «Անձնական տվյալների մասին»[7], «Էլեկտրոնային փաստաթղթի և էլեկտրոնային թվային ստորագրության մասին»[8], «Էլեկտրոնային հաղորդակցության մասին»[9], «Ահաբեկչության դեմ պայքարի» ազգային ռազմավարությունը[10], «Էլեկտրոնային հասարակության ձևավորման» հայեցակարգը[11], «Զանգվածային լրատվության մասին»[12] Հայաստանի Հանրապետության օրենքները:

Կարող ենք ասել, որ ՀՀ տեղեկատվական անվտանգության ներկայիս մակարդակը դեռևս չի համապատասխանում հասարակության ու պետության

---

[4] Տե՛ս «Պետական և ծառայողական գաղտնիքի մասին» օրենք, https://www.arlis.am/documentview.aspx?docID=26193

[5] Տե՛ս «Տեղեկատվության ազատության մասին» օրենք, https://www.arlis.am/DocumentView.aspx?docID=1372

[6] Տե՛ս «Արխիվային գործի մասին» օրենք, https://www.arlis.am/DocumentView.aspx?docid=1644

[7] Տե՛ս «Անձնական տվյալների մասին» օրենք, https://www.arlis.am/documentview.aspx?docid=98338

[8] Տե՛ս «Էլեկտրոնային փաստաթղթի և էլեկտրոնային թվային ստորագրության մասին» օրենք, https://www.arlis.am/documentview.aspx?docid=1547

[9] Տե՛ս «Էլեկտրոնային հաղորդակցության մասին» օրենք, 2005, https://www.arlis.am/documentview.aspx?docid=1547

[10] Տե՛ս «Ահաբեկչության դեմ պայքարի» ազգային ռազմավարությունը, 2012, https://www.arlis.am/documentview.aspx?docid=75353

[11] Տե՛ս «Էլեկտրոնային հասարակության ձևավորման» հայեցակարգը, Նախագիծ, 2010, http://www.irtek.am/views/act.aspx?aid=52982

[12] Տե՛ս «Զանգվածային լրատվության մասին» օրենք, 2003, http://www.irtek.am/views/act.aspx?aid=23491

արդի պահանջներին, և կարծում ենք, որ անհրաժեշտ է ունենալ այնպիսի իրավակարգավորող օրենքներ, ակտեր, որոնք կունենան հստակ ուղղվածություն և կնպաստեն ոլորտի կայուն զարգացմանն ու անվտանգ ապագայի երաշխիք կդառնան:

Նշենք, որ Հայաստանում բացակայում է ընդհանուր, բազային օրենքը, որը կսահմաներ տեղեկատվության հասանելիության, գաղտնիության և տեղեկատվության պաշտպանության վերաբերյալ ընդհանուր դրույթները:

Այսպես, տեղեկատվական անվտանգային խնդիրները ՀՀ ամենավտանգավոր մարտահրավերներից են թե՛ տեխնիկական, թե՛ բովանդակային առումով: Գտնում ենք, որ մեր հանրապետությունը տեղեկատվական անվտանգության պաշտպանության գործընթացների համար պետք է ձևավորի առավել հստակ տեսլական և ռազմավարություն:

Հանրապետության քաղաքական և սոցիալ-տնտեսական զարգացման արդի պայմանները սրում են հակասությունները հասարակության տեղեկատվության ազատ փոխանակման պահանջմունքների ընդլայնման և տեղեկատվության տարածման առանձին կանոնակարգված սահմանափակումները պահպանելու անհրաժեշտության միջև:

Տեղեկատվության ոլորտում հասարակական հարաբերությունների իրավական կարգավորման թույլ զարգացած և հակասական վիճակը հանգեցնում է բացասական լուրջ հետևանքների: Սահմանադրական կարգի հիմքերի, քաղաքացիների իրավունքների և օրինական շահերի պաշտպանության, երկրի պաշտպանունակության և պետության անվտանգության ապահովման նպատակով կիրառվող զանգվածային տեղեկատվության ազատության՝ սահմանադրական հնարավոր սահմանափակումների բնագավառում հարաբերությունների անբավարար իրավական-նորմատիվային կարգավորումն էապես դժվարացնում է տեղեկատվական ոլորտում անձի, հասարակության և պետության շահերի անհրաժեշտ հավասարակշռության ապահովումը, ինչպես նաև Հայաստանի Հանրապետության տարածքում հայկական տեղեկատվական մրցունակ գործակալությունների և զանգվածային լրատվամիջոցների ձևավորումը[13]:

Անհրաժեշտ է իրականացնել տեղեկատվության ոլորտում հասարակական հարաբերությունների իրավական զարգացմանն ու հակասական վիճակի կայունացմանն ուղղված աշխատանքներ, մշակել տեղեկատվական անվտանգության ապահովման պետական հստակ ծրագրեր, տեղեկատվական անվտանգության ապահովման համակարգերի և միջոցների արդյունավետության գնահատման չափանիշներ ու մեթոդներ, ապահովել և զարգացնել տեղեկատվական տեխնոլոգիաների անվտանգությունը:

Այսպիսով, ամփոփելով վերն ասվածը, նշենք, որ «տեղեկատվական անվտանգություն» հասկացության հիմնական էությունը տեղեկատվական

[13] Տե՛ս ՀՀ նախագահի կարգադրությունը ՀՀ տեղեկատվական անվտանգության հայեցակարգը հաստատելու մասին, https://www.arlis.am/documentview.aspx?docID=52559

փոխազդեցության սուբյեկտների պաշտպանվածությունը բացասական ազդեցությունից ապահովելն ու սոցիալական սուբյեկտների տեղեկատվական պահանջմունքները բավարարելն է: Այդ ամենին հասնել հնարավոր է նախ և առաջ հասարակության ու դրա սուբյեկտների համար տեղեկատվական տեխնոլոգիաների կիրառման գործընթացում բացասական ազդեցության ուսումնասիրմամբ, որը կնպաստի դրանց վնասակար ազդեցության հաղթահարմանը և ապահով տեղեկատվական միջավայրի ձևավորմանը:

## Տեղեկատվական հակամարտության տեխնոլոգիաները

Ինչպես նշում է ԱՄՆ նախագահի ազգային անվտանգության հարցերով նախկին խորհրդական Հենրի Քիսինջերը, սովորական են դարձել տեղեկատվական դարաշրջանի՝ որպես պատմության մեծ, նույնիսկ մեծագույն մտավոր հեղափոխության մասին խոսակցությունները և նրա սոցիալական, տնտեսական ու քաղաքական կողմերի վրա սևեռվելը: Հազվադեպ, սակայն, քննարկվում է նաև նրա ազդեցությունը միջազգային հարաբերությունների վրա, բացառությամբ թերևս ժամանակակից հաղորդակցության միջոցների գլոբալ հնարավորությունների մասին վավերագրումների: Ընդ որում՝ այստեղ նկատի են առնվում միայն թվերը և տեղեկատվության փոխանցման արագությունը: Միջազգային հարաբերությունները, հետևաբար նաև պատմության ընթացքը, կախված չեն միայն տեղեկատվություն ունեցող մարդկանց թվաքանակից. առավել կարևոր են ընկալման եղանակները: Քանի որ հասանելի տեղեկատվության ծավալը սովորաբար գերազանցում է դրանց մշակման հնարավորությունները, բնականաբար խորանում է տեղեկատվության ու գիտելիքի, առավել ևս՝ գիտելիքի և իմացության միջև խզումը:

«Տեղեկատվական պատերազմներ» հասկացությունը, ի հայտ գալով 20-րդ դարի վերջին քառորդում, կարճ ժամանակամիջոցում բազում հեղինակների ուշադրության կենտրոնում է հայտնվել: Առանձնացնենք մի քանիսը՝ Մ. Լիբիկիի «Ի՞նչ է տեղեկատվական պատերազմը», Գ. Պոչեպցովի «Տեղեկատվական պատերազմներ, ռազմական-հաղորդակցական հետազոտությունների հիմունքներ», Գ. Հարությունյանի «ՀՀ տեղեկատվական համակարգի զարգացման հիմնախնդիրները ազգային անվտանգության համատեքստում» և այլն:

1976 թ. Թոմաս Ռոնան իր զեկույցում «Բոինգ» ընկերության համար օգտագործեց «Սպառազինությունների համակարգը և տեղեկատվական պատերազմը»[14] (Weapon Systems and information war) բնորոշումը, որի հիմնական թիրախ էին հաղորդակցության համակարգերը: Թոմաս Ռոնան կարևորում էր, որ ռազմական ոլորտում հաղորդակցության միջոցների նոր ձեռքբերում-

[14] Տե՛ս **Thomas P. Rona**, Weapon Systems and Information War. Boeing Aerospace Co., Seattle, WA, 1976, p.15, https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_ Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf

ները պահանջում են ինտեգրացիոն նոր որակ: Տեղեկատվական արտահոսքերի բացառման միջոցով հակառակորդին չպետք է հասու լինեն հաղորդակցության տեխնոլոգիաների ոլորտում արձանագրված հաջողությունները: Նա գտնում էր, որ տեղեկատվական պատերազմը հակառակորդի վտանգավոր տեղեկատվական արտահոսքերից պաշտպանվածությունն է, միաժամանակ՝ հակառակորդի դեմ ուղղված տեղեկատվական հոսքերի ապահովումը:

Տեղեկատվական պատերազմների մասնագետները «տեղեկատվական պատերազմ» ասելով նկատի ունեն գործողությունների համակարգ, որն ուղղված է հակառակորդի տեղեկատվության և տեղեկատվական ենթակառուցվածքների վրա ազդեցություն գործելուն, սեփական տեղեկատվությունն ու տեղեկատվական համակարգերը պաշտպանելուն: Այս սահմանումից երևում է, որ տեղեկատվական պատերազմները ներառում են ոչ միայն տեղեկատվական հարձակումներ, այլև տեղեկատվական պաշտպանություն և անվտանգություն: «Տեղեկատվական պատերազմներ» և «տեղեկատվական անվտանգություն» հասկացությունները սերտորեն փոխկապված են: Տեղեկատվական պատերազմը սուբյեկտն է, որի խնդիրն է խանգարել, շարքից հանել կամ ոչնչացնել տեղեկատվական անվտանգությունը (օբյեկտը): Տեղեկատվական անվտանգությունը կարելի է բնորոշել որպես հասարակության և ղեկավար մարմինների, պետության տեղեկատվական միջավայրի պաշտպանվածություն: Անհրաժեշտ է նշել, որ տեղեկատվական անվտանգությունը ներառում է ինչպես հասարակության և պետության տեղեկատվական միջավայրի անվտանգության պաշտպանվածությունը, այնպես էլ տեղեկատվական-տեխնիկական համակարգերի ապահովության հիմնախնդիրները:

Ինչպես նշում է տեղեկատվական անվտանգության հայտնի փորձագետ Ի. Պանարինը, մարդկության պատմության ամբողջ ընթացքում տեղեկատվական պատերազմը եղել է համաշխարհային քաղաքականության հիմնական գործիքը, աշխարհում հոգևոր, քաղաքական, ֆինանսական և տնտեսական իշխանության հասնելու գերակայող միջոցը:

**Տեղեկատվական զենք:** Լայն իմաստով այս եզրույթի տակ հասկացվում են հակառակորդին ուղղված տեղեկատվական ներգործության և այդպիսով նրան կառավարելու միջոցները, որոնց նպատակն է հակառակորդի ռազմավարական և մարտավարական մտահղացումները ներգործողի համար բարենպաստ ուղղությամբ փոխելը: Ավելի նեղ իմաստով՝ տեղեկատվական զենք ասելով հասկացվում է մեթոդների, տեխնիկական և տեխնոլոգիական միջոցների այն համալիրը, որը նախատեսված է պոտենցիալ հակառակորդի տեղեկատվական ռեսուրսների հանդեպ վերահսկողություն սահմանելու և նրա տեղեկատվական համակարգերի աշխատանքին միջամտելու համար՝ դրանք շարքից դուրս բերելու, դրանցում պարունակվող տվյալները ստանալու կամ փոխելու, ինչպես նաև ներազդողի համար շահավետ տեղեկատվությունը (կամ ապատեղեկատվությունը) նպատակաուղղված ներմուծելու նպատակով:

Ներկայումս տեղեկատվական զենքի տեսակները և դրանց կիրառման մեթոդները շարունակ կատարելագործվում են: Ակնհայտ է, որ այդ գործընթացն անմիջականորեն փոխկապակցված է տեղեկատվական պատերազմների նոր հայեցակարգերի մշակման և իրականացման խնդիրների հետ:

Տեղեկատվական զենքի կիրառումը ենթադրում է ոչ միայն հնարավորինս լավ իմանալ հակառակորդի տեխնիկական միջոցների բնութագրերը, այլ նաև խորը իմացություն ունենալ թիրախ հանդիսացող անձի և զանգվածների էթնոհոգեբանության, մշակութային առանձնահատկությունների վերաբերյալ, քանի որ դրանք են պայմանավորում մարդու՝ տեղեկատվությունն ընկալելու և վերծանելու ու ըստ այդմ որոշում ընդունելու, այն իրականացնելու գործընթացը:

Տեղեկատվական պատերազմներում կարևոր դերակատարություն ունեն զանգվածային լրատվամիջոցները: Տարբեր երկրներ, ունենալով զարգացած և նորագույն տեխնիկական հնարավորություններով հագեցած, հեղինակություն վայելող և աշխարհի տարբեր երկրներում հեռարձակվող լրատվամիջոցներ, միջազգային զանազան անցուդարձերում ձևավորում են իրենց նպատակահարմար տեղեկատվական մթնոլորտ: Սրանք իրականացնում են տեղեկատվության հավաքում, մշակում, վերլուծում, որից հետո լուրերը հաղորդում են հասցեատիրոջը՝ ունենալով որոշակի ուղղվածություն: Մեթոդներն ու հնարավորությունները, որոնք կիրառվում են տեղեկատվական հակամարտություններում, կարող են ուղղորդել մարդկանց, հասարակության, պետությունների քայլերը:

Խոսելով «տեղեկատվական պատերազմների» մասին՝ անհրաժեշտ է հաշվի առնել, որ այն ոչ թե քարացած, այլև փոփոխվող, զարգացող գործողությունների համախումբ է: Տեղեկատվական պատերազմների գործընթացում սկսվում, շարունակվում են համակարգի բաղադրիչների փոփոխություններ, այդ իսկ պատճառով բարդ է հստակորեն կանխատեսել, թե գործընթացն իր բազմաքանակ տարրերով ինչպիսի վերջնական տեսք կունենա:

Ռազմական հնարքների և անուղղակի գործողությունների (որոնցում կարևոր դերակատարում ունեն տեղեկատվական գործողությունները) տեսական հիմունքներն ու փիլիսոփայությունը հնարավորինս բազմակողմանիորեն մշակել է չինացի խոշոր մտածող Սուն Ցզին (մ.թ.ա. IV դար, ըստ որոշ աղբյուրների՝ մ.թ.ա. VI դար):

Նրա հանրահայտ «Տրակտատ ռազմարվեստի մասին» աշխատությունն առ այսօր հիմք է տեսական տարաբնույթ հետազոտությունների, իսկ այնտեղ ներկայացված հիմնադրույթները լայնորեն օգտագործվում են կիրառական նշանակություն ունեցող մշակումներում: Չինացի փիլիսոփան համարում էր, որ պատերազմել կարելի է միայն այն պարագայում, երբ արդեն սպառվել են հակառակորդին հաղթելու մնացած միջոցները: Իդեալական հաղթանակը, ըստ Սուն Ցզիի, առանց ռազմական գործողություններ կատարելու մրցակիցց

պետություններին դիվանագիտական մեթոդներով ենթարկեցնելն է: Այդ նպատակով անհրաժեշտ է վարել ակտիվ դիվանագիտություն, քայքայել հակառակորդի դաշինքները և խաթարել նրա ռազմավարությունը (այսօր նման քաղաքականությունը հաճախ բնութագրվում է որպես «փափուկ ուժի» կիրառում):

## Տեղեկատվածին (ինֆոգեն) սպառնալիքները և դրանց միջազգային վերահսկողության միջոցները

Բոլոր ժամանակներում յուրաքանչյուր պետության գլխավոր հիմնախնդիրներից է եղել պաշտպանել երկրի անվտանգությունը: Երբ ինֆոգեն գործողություններն ուղղված են մրցակիցների կամ պայմանական հակառակորդների շահերի դեմ, դրանք պետք է ընդունել որպես մարտահրավերներ: Վերջիններս հիմնականում լինում են երկու տիպի.

**1. Հոգևոր-գաղափարախոսական բնույթի ինֆոգեն սպառնալիքներ**, որոնք ուղղված են ազգի, հասարակության ու անհատի դեմ, և որոնք ներազդողի շահերի համատեքստում ենթադրում են՝

- խաթարել հանրության գիտակցությունը (երբեմն անգամ ենթագիտակցության մակարդակով), հոգևոր և ազգային արժեհամակարգը,
- փոխել հասարակության և առանձին անհատների (այդպիսով՝ պետության) քաղաքական ու քաղաքակրթական կողմնորոշումները (այսպես կոչված՝ «քաղաքակրթական կոդը»),
- նվազեցնել հասարակության և պետության ընդհանրական մտավոր-գիտելիքային ռեսուրսները և այդպիսով սահմանափակել տվյալ հանրության զարգացման հնարավորությունները:

**2. Տեխնոգեն բնույթի ինֆոգեն սպառնալիքներ**, որոնք ուղղված են անհատի, հասարակության, ազգի և պետության գործունեությունը կազմակերպող և համակարգող տեղեկատվական-տեխնոլոգիական համակարգերի դեմ:

Ինֆոգեն սպառնալիքների աղբյուրները կարող են լինել ինչպես արտաքին, այնպես էլ ներքին: Արտաքին ինֆոգեն սպառնալիքների աղբյուր հայ հանրության պարագայում կարող են լինել՝

- պետությունների և հանրության մրցակից կամ հակառակորդ երկրներն ու կազմակերպությունները,
- գլոբալ տեղեկատվական դաշտում շրջանառվող, բայց ոչ հատուկ հայ հանրության դեմ ուղղված քաոտիկ տեղեկատվական հոսքերը, որոնք բացասական ներգործություն են ունենում հանրային և անհատական գիտակցության վրա:

Ինֆոգեն ներքին սպառնալիքների աղբյուր կարող են լինել՝

- Հայաստանում տեղակայված, սակայն օտարերկրյա աղբյուրներից սնվող քաղաքական, հասարակական, տնտեսական կազմակերպությունները և զանգվածային լրատվամիջոցները (ԶԼՄ), որոնց գործունեությունը չի համապատասխանում հայ հանրության շահերին,

- մասնավոր և պետական ներքին ռեսուրսների վրա հիմնված քաղաքական, հասարակական, տնտեսական կազմակերպությունները, ընկերությունները, պետական մարմինները և ՋԼՄ-ն, որոնց պատկերացումները հայ հանրության ազգային շահերի վերաբերյալ հստակեցված չեն: Որպես հետեվանք՝ նման կառույցները կարող են ակամա կամ քաղաքական-գաղափարախոսական սխալ կողմնորոշումների հետևանքով ինֆոգեն վտանգի աղբյուր լինել հայ հանրության համար: Գործողությունների որոշ դրսևորումները երբեմն որակվում են որպես «տեղեկատվական պատերազմ սեփական ժողովրդի դեմ»:
- Իրենց հերթին ինֆոգեն մարտահրավերների բացահայտումը, համապատասխանաբար համակարգումը և վերլուծությունը թույլ են տալիս հասկանալ պայմանական հակառակորդի կամ մրցակցի ռազմավարությունը և դրա իրագործման մեթոդաբանությունը: Ի լրումն նշենք, որ ինֆոգեն սպառնալիքները համապատասխան մեկնություններով և «տեղեկատվական ուղեկցությամբ» հանրությանը ներկայացնելը մոբիլիզացնում է հասարակությունն ու պետությունը, ինչը նպաստում է, որ նետված մարտահրավերներին տրվեն համարժեք պատասխաններ:

Պետության անվտանգության մեջ կարևոր տեղ են զբաղեցնում՝

- ռազմաքաղաքական անվտանգությունը,
- սոցիալ-տնտեսական անվտանգությունը,
- տեղեկատվական անվտանգությունը:

Այս բաղադրամասերը փոխկապակցված են, իսկ նրանց միջև սահմանները շատ պայմանական են: Այս երեք տարրերից որևէ մեկի անտեսումը կարող է թերի դարձնել պետության անվտանգությունը: Ավանդաբար ընդունված է համարել, որ անվտանգության համակարգի գագաթում է ռազմական ոլորտը (ռազմական անվտանգության հետ է հիմնականում նույնացվում «անվտանգություն» հասկացությունը), որից ածանցվում են մյուս ոլորտները: Ժամանակակից զարգացումները ստիպում են տեսաբաններին հրաժարվել ավանդական մոտեցումներից և անվտանգության ապահովման գործում ընդունել հասարակության՝ ոչ ռազմական ոլորտների կենսագործունեության կարևորությունը, որի պայմաններում անվտանգության համակարգը ներկայանում է ոչ թե բուրգի, այլ ցանցի տեսքով, որի կենտրոնում (այլ ոչ գագաթին) գտնվող տեղեկատվական անվտանգությունը փոխկապակցվում է անվտանգության համակարգի մյուս բաղադրատարրերի հետ[15]:

Տեղեկատվական հասարակության պայմաններում, երբ փոփոխության են ենթարկվել և մեծացել են տեղեկատվության ծավալները, նոր իրադրություն է ստեղծվել դիվանագիտական գործընթացներում: Իհարկե, դիվանագիտական

[15] Տե՛ս **Գ. Հարությունյան**, ՀՀ տեղեկատվական համակարգի զարգացման հիմնախնդիրները ազգային անվտանգության համատեքստում, Եր., Նորավանք ԳԿՀ, 2002, էջ 5-10, http://www.noravank.am/upload/pdf/71_am.pdf

գործունեության ավանդական միջոցները պահպանում են իրենց արդիականությունը, սակայն նոր մեթոդներին տիրապետելը դառնում է հրամայական: Եթե նախկինում միայն դիվանագետներն էին քաջատեղյակ աշխարհի այս կամ այն հատվածում տեղի ունեցող անցուդարձերին, ապա ներկա պայմաններում յուրաքանչյուր քաղաքացի համացանցի միջոցով հնարավորություն է ստացել ձեռք բերելու համապատասխան տեղեկատվություն:

Տեղեկատվական դիվանագիտությունը միջազգային լայն ճանաչման հասնելու կարևորագույն նուրբ գործիք է: Այն զանգվածային հաղորդակցության միջոցներով առաջ է տանում արտաքին քաղաքական շահերը և տեղեկատվությունը հասցնում է հասարակությանը և քաղաքական վերնախավին: Յուրաքանչյուր պետության արտաքին քաղաքականության մարմնի ներկայացուցիչ կիրառում է տեղեկատվական դիվանագիտության գործիքները:

## Հայաստանի Հանրապետության տեղեկատվական անվտանգության առկա իրավիճակը

Վերջին շրջանում իրականացվել են մի շարք միջոցառումներ Հայաստանի Հանրապետության տեղեկատվական քաղաքականության և տեղեկատվական անվտանգության ապահովման բարելավման ուղղությամբ: Սկսվել է տեղեկատվական անվտանգության իրավական-նորմատիվային դաշտի ձևավորումը:

Հայաստանի Հանրապետության Ազգային ժողովը վավերացրել է «Կիբեռհանցագործությունների մասին» Եվրախորհրդի կոնվենցիան և դրա «Համակարգչային համակարգերի միջոցով կատարվող ռասիստական և քսենոֆոբիական բնույթի արարքների քրեականացման մասին» լրացուցիչ արձանագրությունը, որոշակի աշխատանք է տարվում տեղեկատվական ոլորտում հասարակական հարաբերությունները կարգավորող իրավական հիմքերի մշակման, ինչպես նաև իրավակիրառ պրակտիկայի կատարելագործման ուղղությամբ[16]:

Միաժամանակ, Հայաստանի Հանրապետության տեղեկատվական անվտանգության վիճակի վերլուծությունը ցույց է տալիս, որ դրա մակարդակը դեռևս չի համապատասխանում հասարակության և պետության ներկայիս պահանջներին:

Հանրապետության քաղաքական և սոցիալ-տնտեսական զարգացման արդի պայմանները հակասությունների սրում են առաջացնում հասարակության տեղեկատվության ազատ փոխանակման պահանջմունքների ընդլայնման և տեղեկատվության տարածման առանձին կանոնակարգված սահմանափակումների պահպանման անհրաժեշտության միջև:

---

[16] Տե՛ս ՀՀ նախագահի կարգադրությունը ՀՀ տեղեկատվական անվտանգության հայեցակարգը հաստատելու մասին, https://www.arlis.am/documentview.aspx?docID=52559

Տեղեկատվության ոլորտում հասարակական հարաբերությունների իրավական կարգավորման թույլ զարգացած և հակասական վիճակը հանգեցնում է բացասական լուրջ հետևանքների: Սահմանադրական կարգի հիմքերի, քաղաքացիների իրավունքների և օրինական շահերի պահպանության, երկրի պաշտպանունակության և պետության անվտանգության ապահովման նպատակով կիրառվող զանգվածային տեղեկատվության ազատության սահմանադրական հնարավոր սահմանափակումների բնագավառում հարաբերությունների անբավարար իրավական-նորմատիվային կարգավորումն էապես դժվարացնում է տեղեկատվական ոլորտում անձի, հասարակության և պետության շահերի անհրաժեշտ հավասարակշռության ապահովումը, ինչպես նաև Հայաստանի Հանրապետության տարածքում մրցունակ հայկական տեղեկատվական գործակալությունների և զանգվածային լրատվամիջոցների ձևավորումը:

Քաղաքացիների՝ տեղեկատվություն ստանալու իրավունքի ոչ լիարժեք ապահովումը, նրանց մատուցվող տեղեկատվության միտումնավոր խեղաթյուրումն առաջացնում են բնակչության դժգոհությունը, ինչն առանձին դեպքերում հասարակության մեջ հանգեցնում է սոցիալ-քաղաքական իրավիճակի անկայունության:

Քաղաքացիների մասնավոր կյանքի անձեռնմխելիության, անձնական և ընտանեկան գաղտնիքի, նամակագրության գաղտնիության՝ Հայաստանի Հանրապետության Սահմանադրությամբ ամրագրված իրավունքները դեռևս չունեն իրավական, կազմակերպական և տեխնիկական անհրաժեշտ ապահովվածություն: Բարելավման և արդիականացման կարիք ունի նաև պետական իշխանության և տեղական ինքնակառավարման մարմինների կողմից ֆիզիկական անձանց մասին հավաքվող տվյալների (անձնական տվյալների) պաշտպանությունը:

Որակյալ մասնագետների զանգվածային արտահոսքի հետևանքով զգալիորեն նվազել է տեղեկատվության, հեռահաղորդակցության և կապի բնագավառի կադրային ներուժը:

## Տեղեկատվական տարածքի վերահսկման օրենսդրական և վարչական միջոցները

ՋԼՄ-ի կողմից մարդկանց մտածելակերպի, հոգեվիճակի և վարվելաձևի վրա ազդելու հնարավորությունները մարտահրավեր են ցանկացած հասարակության համար: Այդ մարտահրավերները որոշ դեպքերում վերածվում են լուրջ սպառնալիքների այս կամ այն պետության ազգային և տեղեկատվական անվտանգության տեսանկյունից: Արդարացի են նրանք, ովքեր կարծում են, որ նման տեղեկատվության դեմ պայքարի ամենաարդյունավետ միջոցներն են համապատասխան հակաքարոզչությունը և տեղեկատվական հնարքների բացահայտումը: Հատուկ ուշադրության են արժանի այն իրավիճակները, երբ սպառնալիք ներկայացնող տեղեկատվական հոսքերն իրականացվում են ոչ

բարեկամ պետությունների և կազմակերպությունների կողմից ու հետապնդում են տվյալ հասարակությունն ապակայունացնելու, խարխլելու նպատակ: Հայտնի է նաև, որ մեր դարաշրջանում ոչ բարեկամական ԶԼՄ-ի բովանդակության ձևավորումն ընթանում է տարաբնույթ ՀԿ-ների և ոչ պետական կառույցների անմիջական մասնակցությամբ: Արդյունքում երբեմն ստեղծվում է վիճակ, երբ նման սպառնալիքներից հնարավոր է պաշտպանվել միայն վարչական և օրենսդրական միջոցներով:

Մեր օրերի քարոզչական մեքենաներից մեկը համարվում է համացանցը, որը դարձել է հակամարտության մի մասնիկը: Ադրբեջանական պետական քարոզչամեքենան, նախագահի՝ Ի. Ալիևի գլխավորությամբ և հովանավորությամբ, չի խնայում ո՛չ նյութական, ո՛չ մարդկային ռեսուրսներ համացանցում հակահայկական քարոզչություն իրականացնելու համար: Ադրբեջանն այսօր ավելացնում է իր ներկայությունը համացանցում՝ ի հաշիվ անընդհատ ավելացող լրատվական կայքերի, որոնք ակտիվորեն ապատեղեկատվություն և քարոզչական բնույթի նյութեր են տարածում Հայաստանի դեմ:

Ներկայումս ՀՀ-ի առջև ծառացած են մի շարք տեղեկատվական անվտանգային խնդիրներ, ինչպիսիք են՝ կեղծ և խեղաթյուրված տեղեկատվության տարածումը, միջազգային ահաբեկչական գործունեությունը տեղեկատվական դաշտում, միջազգային տեղեկատվական աղբյուրներով հակահայկական կեղծ տեղեկատվության տարածումը, հայ ազգային և մշակութային ինքնության դեմ ուղղված քայքայիչ գործողությունները, արտաքին սուբյեկտների հետախուզական գործունեությունը, ՀՀ տեղեկատվական և հեռահաղորդակցային համակարգերի բնականոն գործունեությունը խաթարելը, տեղեկատվական միջոցների պահպանման անարդյունավետությունը:

Ի մի բերելով նշենք, որ Հայաստանի Հանրապետության տեղեկատվական անվտանգությունը Հայաստանի Հանրապետության ազգային անվտանգության ռազմավարության բաղկացուցիչ մասն է և իր ազդեցությունն է թողնում երկրի ազգային շահերի պաշտպանվածության վրա հասարակության և պետության կենսագործունեության տարբեր բնագավառներում: Սպառնալիքները ՀՀ տեղեկատվական անվտանգության նկատմամբ և անվտանգության ապահովման ձևերն ընդհանուր են բոլոր բնագավառների համար:

## Եզրակացություն

Ուսումնասիրությունների արդյունքում հանգել ենք հետևյալ հիմնական եզրակացություններին.

- Տեղեկատվական հասարակությունում տեղեկատվությունը ձեռք է բերել նոր որակներ՝ գերակշռող արժեք, ռազմավարական ռեսուրս, քանի որ տեղեկատվության ստեղծումը, մշակումը, փոխանցումը արտադրողականության, իշխանության, կառավարման վճռորոշ աղբյուր են: Տեղեկատվությունը հասարակական և քաղաքական զարգացումները կառավարող որոշիչ գործոն է:

- 21-րդ դարը յուրահատուկ է ցանցայնացման և վիրտուալացման գլոբալ գործընթացներով, որոնք ի սկզբանե ակնառու էին իրենց բացասական կողմերով: Լրջագույն վտանգներից է կիբեռհանցավորության և կիբեռսպառնալիքների աճը, ինչը սպառնում է պետությունների, հասարակությունների և անհատների կայուն կենսագործունեությանն ու բնականոն զարգացմանը:
- Արդի գլոբալ անորոշությունները լուրջ մարտահրավերներ են նետել զարգացման տարբեր մակարդակներում գտնվող երկրների անվտանգային և քաղաքական համակարգերին: Ներկայիս ձևավորվող աշխարհակարգը կոչված է փոփոխության ենթարկելու տեղային, տարածաշրջանային, գլոբալ առկա սպառնալիքները: Գործընթացի առավել վտանգավոր դրսևորումներից են տեղեկատվական պատերազմները, որոնք ընթանում են ազգամիջյան բախումների, միջպետական հարաբերությունների սրման, ներքաղաքական անհանդուրժողականության դրսևորումներով՝ հանգեցնելով աշխարհաքաղաքական քաոսի, կաթվածահար անելով քաղաքական և հասարակական կյանքը:
- Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման վերահսկողությունն իրականացվում է իրավական, ինստիտուցիոնալ, տեխնոլոգիական ապահովման և համակողմանի համագործակցության միջոցներով՝ պետական կառավարման և տեղական ինքնակառավարման մարմինների կողմից օրենսդրությամբ ամրագրված լիազորությունների սահմաններում:

**МАРИАМ ГЗОГЯН – *Проблемы модернизации информационной безопасности Республики Армения.*** – В современных международных отношениях государства уделяют значительное внимание вопросам модернизации и поддержанию механизмов информационной безопасности. Важно подчеркнуть, что с увеличением роли и объема информации соответственно выросли и угрозы информационной безопасности. Следовательно, защита информации стала важнейшим вопросом внутренней и внешней политики многих государств.

Анализируя различные научные работы, считаю необходимым подчеркнуть, что если раньше безопасность была связана прежде всего с военными аспектами как в научном, так и в политическом контексте, то сегодня наблюдается возрастающее внимание к невоенным измерениям безопасности. В результате перед государствами и международными организациями теперь стоит задача обеспечения коллективной безопасности в различных областях, включая политику, экономику, общество, экологию и армию. Более того, в зависимости от характера своего режима страны решают проблему по-разному. Одни закрывают информационное поле, запрещая даже использование социальных сетей, другие ищут более либеральные методы (Мкртчян Г., 2018, с. 55).

Достижения в области информационных технологий и телекоммуникаций стали важным инструментом продвижения собственных интересов и целей в международных обменах, поэтому государства не жалеют усилий для создания профессиональных «информационных армий» и безопасных информационных инфраструктур. Мировой опыт последнего времени показывает, что влияние информационных потоков может стать мощным оружием для государств, ведущих действия против своих противников. Государства, не имеющие возможности противостоять этому оружию, могут оказаться в невыгодном положении.

С точки зрения политологии, здесь подчеркивается необходимость сотрудничества частного сектора и государственных институтов в противодействии различным угрозам в сфере информационной безопасности.

**Ключевые слова:** *международные отношения, информационная безопасность, модернизация, телекоммуникации, либеральные методы, национальные интересы*

**MARIAM GZOGHYAN – *Problems of Modernization of Information Security of the Republic of Armenia.* –** In contemporary international relations, states place significant emphasis on the matters of modernization and the upkeep of information security mechanisms. It is important to highlight that with the increasing role and volume of information, the threats to information security have correspondingly grown. Consequently, safeguarding information has emerged as a foremost focal point within the domestic and foreign policies of numerous states.

Analyzing various scientific works, I consider it necessary to emphasize that in the past, security was primarily associated with military aspects in both scientific and political contexts, today, there is a growing focus on the non-military dimensions of security. As a result, states and international organizations are now tasked with ensuring collective security across various domains, including politics, economics, society, ecology, and the military. Moreover, according to the nature of their regime, countries solve the problem in different ways. Some close the information field, banning even the use of social networks, others are looking for more liberal methods (Mkrtchyan H., 2018, p. 55).

Advancements in information technology and telecommunications have become an important tool for promoting their own interests and goals in international exchanges, so states spare no effort in establishing professional 'information armies' and secure information infrastructures. Recent global experience demonstrates that the influence of information flows can be a powerful weapon for states conducting actions against their adversaries. States lacking the capacity to counter this weapon may find themselves at a disadvantage.

From a political science perspective, it emphasizes the necessity of the private sector and state institutions to collaborate in countering various threats in the field of information security.

**Key words:** *international relations, information security, modernization, telecommunications, liberal methods, national interest*