-

Vardan Atoyan, Lilit Dadayan

ՔԱՂԱՔԱԳԻՏՈՒԹՅՈՒՆ

ՎԱՐԴԱՆ ԱԹՈՅԱՆ
ՀՊՏՀ «Ամբերդ» հետազոտական կենտրոնի «Ազգային անվտանգության հետազոտություններ» ծրագրի տնօրեն, տնտեսագիտության թեկնածու

ԼԻԼԻԹ ԴԱՂԱՅԱՆ
ՀՊՏՀ մարքեթինգի ամբիոնի դոցենտ, տնտեսագիտության թեկնածու

ՏԵՂԵԿԱՏՎԱԿԱՆ-ՀԱՂՈՐԴԱԿՑԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԱՐԴԻ ԽՆԴԻՐՆԵՐԻ ՇՈՒՐՋ

Հոդվածը նվիրված է ազգային անվտանգության առանցքային ուղղություն համարվող տեղեկատվական անվտանգության ապահովման արդի հիմնախնդիրներին:

Արդյունաբերական հասարակությունից արմատական փոփոխություններով բնութագրվող հետարդյունաբերական կամ տեղեկատվական հասարակությանն անցման ներկայիս դարաշրջանի որակապես նոր սպառնալիքներին և համընդհանրական մարտահրավերներին դիմակայելու համար տեղական և միջազգային տեղեկատվական դաշտում անհրաժեշտ է գործել այնպիսի կանոններով, որոնցից վճռորոշ են տեղեկատվական հոսքերի համակարգումը, վերահսկումը և անվտանգության ապահովումը:

Տեղեկատվական-հաղորդակցական անվտանգության խնդիրների համատեքստում հոդվածում ներկայացված են այն առանցքային նպատակներն ու խնդիրները, որոնց ձևակերպումն ու համակարգային լուծումը կնպաստեն տեղեկատվական ոլորտում անհատի, հասարակության և պետության պաշտպանվածության մակարդակի բարձրացմանը ինչպես կարճաժամկետ, այնպես էլ երկարաժամկետ հեռանկարում:

Հիմնաբառեր. *տեղեկատվական անվտանգություն, ազգային անվտանգություն, սպառնալիք, տեղեկատվական-հաղորդակցական միջավայր, ազգային շահեր, տեղեկատվական ռեսուրսներ*

Ազգային անվտանգության ապահովումը յուրաքանչյուր պետության առանցքային խնդիրներից մեկն է: Առօրյա գիտակցական մակարդակում «անվտանգություն» հասկացությունը բնորոշվում է որպես «վտանգի բացակայություն», «վիճակ, երբ վտանգ չի սպառնում»[1]: «Վտանգ» հասկացությունն իր հերթին նշանակում է «որևէ վտանգի հնարավորություն, սպառնալիք»[2], իսկ «սպառնալիք» հասկացությունը՝ «հնարավոր վտանգ, ահաբեկություն, որևէ մեկին անախորժություն, չարիք պատճառելու խոստում»[3]: Այսպիսով՝ «անվտանգություն» հասկացությունը մեկնաբանվում է որպես որևէ մեկին և որևէ բանի սպառնալիքի բացակայություն: Նմանատիպ մոտեցմամբ տվյալ հասկացությունը մասնագիտական գրականության մեջ մեկնաբանվում է որպես «իրավիճակ, որի դեպքում որևէ մեկի կամ որևէ բանի համար գոյություն չունի սպառնալիք որևէ մեկի կամ որևէ բանի կողմից, ընդ որում, չի բացառվում վտանգի միաժամանակ մի քանի աղբյուրների առկայությունը»[4]: Փաստորեն, կարող ենք ենթադրել, որ «անվտանգությունը» առկա սպառնալիքի հետևանքով որևէ մեկին կամ որևէ բանի վնաս հասցնելու անհնարինությունն է կամ նրանց պաշտպանվածությունը սպառնալիքից:

Անվտանգության հիմնական օբյեկտներն են՝

- անհատը (իրավունքներն ու ազատությունը),
- հասարակությունը (նյութական և հոգևոր արժեքները),
- պետությունը (սահմանադրական կարգը, ինքնիշխանությունն ու տարածքային ամբողջականությունը)[5]:

Միաժամանակ, պետությունը, հասարակությունը և քաղաքացիները անվտանգության ապահովման հիմնական սուբյեկտներ են: Դրանցից, իհարկե, կարևոր դեր է խաղում պետությունը, որը կոչված է ապահովելու ինչպես ռազմավարական նշանակություն ենթակառուցվածքների (ատոմակայան, ջրամատակարարման և էներգամատակարարման համակարգեր, հեռախոսակապ և այլն), այնպես էլ յուրաքանչյուր քաղաքացու անվտանգությունը:

«Ազգային անվտանգություն» հասկացությունը ներառում է երեք առանցքային բաղադրիչներ՝

- ռազմաքաղաքական անվտանգություն,
- սոցիալ-տնտեսական անվտանգություն,
- տեղեկատվական անվտանգություն:

Եթե առաջին և երկրորդ բաղադրիչների խնդիրների և այդ ոլորտներում ընթացող հակամարտությունների վերաբերյալ ուսումնասիրությունները հենվում են հարուստ պատմական ավանդույթների և արդեն իսկ հղկված տեսական ու գործնական մշակումների վրա, ապա արդի ժամանակաշրջանի տեղեկատվական հեղափոխության համատեքստում առաջացած տեղեկատվական պատերազմների և տեղեկատվական անվտանգության մասին պատկերացումները դեռևս վերջնական տեսական ձևակերպումներ չեն ստացել:

---

[1] Տե՛ս Общая теория национальной безопасности: учебник / под общ. ред. Прохожева А.А., М., 2002, էջ 13–15:

[2] Տե՛ս **Возженников А.В.,** Парадигма национальной безопасности реформирующейся России. М., 2000, էջ 73:

[3] Словарь современного русского литературного языка, т. 8, АН СССР. М., 1959. с. 882.

[4] Безопасность. Толковый словарь терминов и понятий. М., 1999. с. 21.

[5] Տե՛ս Информационно-коммуникационная безопасность:монография / под общ. ред. проф. Василенко В.И., М., Проспект, 2015, էջ 38:

Ներկայումս ազգային անվտանգության տեսության զարգացումը հիմնվում է հետևյալ հիմնական ուղղությունների հետազոտությունների և արդյունքների վրա.

1. Մարդկային գործունեության և պետությունների միջև անվտանգության ապահովման ոլորտում միջազգային համագործակցության, էվոլյուցիայի հիմնական միտումների և համաշխարհային, տարածաշրջանային ու ներպետական անվտանգության հետագա համակարգերի մոդելների, դրանց արդյունավետության գնահատման չափանիշների պատմական փորձի ուսումնասիրություն: Այստեղ հարկավոր է հատուկ ուշադրություն դարձնել, այսպես կոչված, շրջադարձային դարաշրջանների ուսումնասիրությանը, երբ անցյալում և ներկայում գոյություն ունեցող հասարակություններն ու պետությունները բախվում էին տարբեր ցնցումների և ճգնաժամերի, որոնք կամ միավորում էին նրանց՝ դիմակայելու առկա մարտահրավերներին, կամ փոփոխությունների ալիքները դուրս էին մղում նրանց աշխարհաքաղաքական բոլոր գործընթացներից՝ պարտադրելով կորցնել պետականությունը և ցրվելով աշխարհով մեկ:

2. Միասնական հայեցակարգային համակարգի և տերմինաբանական բազայի ստեղծում, միասնական մեթոդաբանության մշակում ինչպես ազգային շահերի դիտարկմամբ, այնպես էլ ազգային անվտանգության ապահովման տեսանկյունից:

3. Երկրի ազգային անվտանգության արդի վիճակի ուսումնասիրություն և առկա, այդ թվում՝ ներքին և արտաքին, համաչափ և անհամաչափ, իրական և հնարավոր սպառնալիքների բացահայտում ու գնահատում: Այստեղ անհրաժեշտ է կարևորել նաև սպառնալիքների ցուցիչների մշակումը, ինչն էլ, իր հերթին, դրանց դասակարգման հնարավորություն կընձեռի:

4. Անվտանգության համակարգերի կառուցման օրինաչափությունների և սկզբունքների ուսումնասիրություն՝ հաշվի առնելով միջազգային առաջավոր փորձը և տվյալ երկրի առանձնահատկությունները: Ներկայումս առկա են ազգային անվտանգության ապահովման տարբեր համակարգեր և մոդելներ: Բացի այդ, գոյություն ունեն հավաքական անվտանգության ապահովման համակարգեր, ինչպիսիք են, օրինակ՝ Հյուսիսատլանտյան դաշինքը (ՆԱՏՕ) և Հավաքական անվտանգության պայմանագրի կազմակերպությունը (ՀԱՊԿ):

Մարդկության զարգացման ժամանակակից փուլը բնորոշվում է արդյունաբերական հասարակությունից հետարդյունաբերական կամ տեղեկատվական հասարակությանն անցմամբ, ինչն էլ բնութագրվում է անհատի կյանքում և երկրի սոցիալ-տնտեսական զարգացման մեջ տեղեկատվության տեղի ու դերի փոփոխությամբ: Տեղեկությունների հավաքագրման և տարածման գործընթացները հանգեցրին նոր ոլորտի ձևավորմանը, որը «տեղեկատվություն» և «հաղորդակցություն» տերմինների միավորմամբ ստացել է տեղեկատվական-հաղորդակցական անվանումը: Առավել պատկերավոր ներկայացնելու համար նշենք միայն, որ վերջին 50 տարում տեղեկատվության արագությունը ավելացել է 300 000 անգամ[6]:

Տեղեկատվական-հաղորդակցական միջավայրը համընդգրկուն հեռահաղորդակցական ցանց է, որը համապատասխան տեխնոլոգիաների օգտա-

[6] Տե՛ս **Панарин И.Н.,** Информационная война, PR и мировая политика. Курс лекций, 2-е изд., стереотип. М., Горячая линия – Телеком, 2014, էջ 135:

գործման և հաղորդագրությունների փոխանցման միջոցով բավարարում է տեղեկատվության նկատմամբ հասարակության պահանջմունքները՝ միաժամանակ դառնալով գիտելիքների հանրամատչելի պահեստարան:

Ընդ որում, տեղեկատվական ոլորտը, որպես տեղեկություններ հավաքող, ձևավորող, տարածող և օգտագործող սուբյեկտների, ենթահամակարգերի ամբողջություն, ինչպես նաև այդ գործընթացներում առաջացող հասարակական հարաբերությունների համակարգ, ունենալով հասարակական կյանքը համակարգող և կարգավորող կարևոր գործառույթ, ակտիվորեն ազդում է պետության անվտանգության քաղաքական, տնտեսական, ռազմական և այլ բաղադրիչների վրա: Այդ իսկ պատճառով էլ այսօր ազգային անվտանգությունն էականորեն կախված է տեղեկատվական անվտանգության ապահովումից, և այդ կախվածությունն աստիճանաբար մեծանում է գիտատեխնիկական առաջընթացին համընթաց:

Տեղեկատվական իրավունքի ոլորտում տեղեկատվական-հաղորդակցական միջավայրը դիտարկվում է որպես «տեղեկատվության շրջանառության միջավայր (ստեղծում–տարածում–սպառում), որի դեպքում սուբյեկտներն իրագործում են իրենց պահանջները և հնարավորությունները տեղեկատվության և տեղեկատվական համակարգերի նկատմամբ, որտեղ տեղի է ունենում դրա շրջանառությունը»[7]:

Տեղեկատվական ռեսուրսները, տեղեկատվական-հեռահաղորդակցական տեխնոլոգիաները և հեռահաղորդակցման ենթակառուցվածքը միասին ձևավորում են ժամանակակից հասարակության տեղեկատվական միջավայրը: Տեղեկատվական-հաղորդակցական միջավայրի հիմնական սուբյեկտներն են՝ իշխանության և կառավարման մարմինները, զանգվածային լրատվամիջոցները (մամուլ, ռադիո, հեռուստատեսություն), համացանցը, լրատվաբովանդակության ստեղծողները, գովազդատուները, օգտագործողները:

Ժամանակակից տեղեկատվական-հեռահաղորդակցական տեխնոլոգիաներն առաջացնում են բաց և հասանելի տեղեկատվական միջավայր, որն ապահովում է գրեթե ցանկացած տեղեկատվության նկատմամբ անհատի պահանջմունքների բավարարումը: Դրան զուգահեռ, տեղեկատվական-հեռահաղորդակցական տեխնոլոգիաները ստեղծում են հաղորդակցական տարածություն, ընդգրկում են հասարակության կենսագործունեության բոլոր ոլորտները և դառնում են հասարակության շարժիչ ուժը, ընդ որում, հաղորդակցության նոր միջոցները ձևավորում են նոր սոցիալ-մշակութային իրականություն, որը պահանջում է փոխհարաբերությունների կարգավորման նոր իրավական ձև: Բացի այդ, ժամանակակից հասարակության հաղորդակցությունները դադարում են լինել հաջորդական ակտերի շղթա. դրանք անցնում են միաժամանակության վիճակի:

Արդյունքում ստեղծվում է հագեցած տեղեկատվական-հաղորդակցական միջավայր, որն ունի իր կառուցվածքը և ընթացակարգերը, փոխգործունեության նորմերն ու կանոնները: Ինչպես արդարացիորեն նշում է Մ.Մ. Նազարովը, «....հասարակության զարգացման ժամանակակից փուլը բնութագրվում է տեղեկատվական ոլորտի աճող դերով, որը ներկայացնում է տեղեկությունների, տեղեկատվական ենթակառուցվածքի, տեղեկատվության

[7] Информационное право / под ред. акад. РАН Топорнина Б.Н., 2-е изд., с изм. и доп., СПб.: Издательство Р. Асланова «Юридический центр Пресс», 2005., с. 73.

հավաքում, ձևավորում, տարածում և օգտագործում իրականացնող սուբյեկտների, ինչպես նաև այդ ժամանակ առաջացող հասարակական հարաբերությունների կարգավորման համակարգի ամբողջություն»[8]:

Հարկ է նշել, որ տեղեկատվական հեղափոխության արդյունքում այսօր էապես աճել է տեղեկատվական հոսքերի դերակատարումը: Դրական միտումներին զուգահեռ ի հայտ են գալիս նաև որակապես նոր բնույթի սպառնալիքներ և մարտահրավերներ, որոնք պետություններից պահանջում են միջազգային դաշտում գործել այնպիսի կանոններով, որոնց մեջ վճռորոշ են տեղեկատվական հոսքերի համակարգումը, վերահսկումը և անվտանգությունը, ինչպես նաև ապատեղեկատվության տարածման և հավաստի տեղեկատվության արգելափակման միջոցով հասարակական կարծիքի խեղաթյուրման կանխարգելումը և այլն: Այդ իսկ պատճառով փոխներթափանցելիության այսօրինակ իրողությունների պայմաններում ներկայումս առանձնահատուկ նշանակություն է ձեռք բերում պետության անվտանգության ապահովումը տեղեկատվական ոլորտում:

«Տեղեկատվական անվտանգություն» հասկացությունը հասարակության տեղեկատվական միջավայրի պաշտպանվածության վիճակն է, որն ապահովում է դրա ձևավորումը և զարգացումը՝ ի շահ քաղաքացու, հասարակության և պետության[9]: Աշխարհում ընթացող որակական տեխնոլոգիական թռիչքն առաջացրել է նոր սոցիալական հեղափոխություն, որը հասարակության վրա ազդեցության ուժով բացարձակապես չի զիջում անցյալի հեղափոխություններին: Տեղեկատվական անվտանգություն ասելով պետք է հասկանալ նաև այնպիսի իրավիճակ, երբ հասարակությունում ստեղծվում են պայմաններ, որոնք առկա տեղեկատվության հիման վրա հնարավորություն են տալիս օբյեկտիվորեն գնահատելու պատմական ընթացքը, աշխարհում, տարածաշրջանում և երկրի ներսում տիրող իրադրությունը, մշակելու և ընդունելու ինքնուրույն որոշումներ:

Նոր տեխնոլոգիաների, համաշխարհային տեղեկատվական ցանցերի, կապի և հաղորդակցության արբանյակային և այլ միջոցների ներդրման ու կիրառման հետ միասին ավելի բարդ ու յուրահատուկ է դառնում տարբեր կառույցների, այդ թվում՝ հատուկ ծառայությունների գործունեությունը, որոնք օգտագործում են ԳՏՀ նվաճումները տարաբնույթ տեղեկատվության հավաքման, մշակման, վերլուծության, փոխանցման և օգտագործման, միաժամանակ՝ տարբեր պետությունների ռազմական, քաղաքական և տնտեսական գործընթացների զարգացման կանխատեսման և մշտադիտարկման համար: Այդ առումով, երկրի տեղեկատվական հոսքերի պաշտպանվածությունը յուրաքանչյուր պետության առանցքային խնդիրներից է:

Հարկ է նշել, որ առանց հաղորդակցման հնարավոր չէ սոցիալական ընդհանրությունների, ինստիտուտների և կազմակերպությունների գործունեությունը, պետության բնականոն զարգացումը: Պետական մարմինների համար տեղեկատվության տիրապետման անհրաժեշտությունը դիտարկվում է որպես պահանջմունք, առանց որի բավարարման հնարավոր չէ պետական կառավարումը:

---

[8] **Назаров М.М.,** Массовая коммуникация в современном мире. М., Эдиториал УРСС, 1999, с. 233.

[9] **Վ.Կ. Աթոյան,** Ազգային անվտանգության հիմնախնդիրներ: Դասախոսություններ: Եր., «Տնտեսագետ», 2014, էջ 89:

Մյուս կողմից՝ տեղեկատվական հոսքերի հիմնական մասի տեղափոխումը էլեկտրոնային ցանցեր դժվարացնում է դրանց վերահսկողությունը սոցիալական ինստիտուտների, ինչպես նաև պետական կառավարման մարմինների կողմից: Օրինակ՝ ֆլեշ-մոբի տեխնոլոգիան, իր կայծակնային էֆեկտի շնորհիվ, թույլ է տալիս հաշված րոպեների ընթացքում իրազեկել բազմաթիվ մարդկանց ինչ-որ խնդրի կամ գաղափարի մասին և ձեռք բերել մեծ թվով կողմնակիցներ:

Ցանկացած տեղեկատվական տեխնոլոգիա հաղորդակցական գործառույթ է իրականացնում: Այսօր սկսվել է հաղորդակցությունների հիմնարար ապակենտրոնացման դարաշրջանը, որն իրականացվում է զանգվածային լրատվամիջոցների օգնությամբ: Միևնույն ժամանակ, վերջիններս, պայքարելով իշխանության պետական մարմիններից անկախության համար, ընկնում են իրենց հովանավորող կառույցների ուղիղ ենթակայության տակ, հակառակ դեպքում՝ դրանցից շատերը պարզապես գոյություն ունենալ չեն կարող:

Ցանցային տեղեկատվահաղորդակցական միջավայրի պետական կարգավորումը, ըստ իր առանձնահատկության, նվազագույն մակարդակի վրա է գտնվում: Բազմաթիվ երկրների ղեկավարներ չեն ժխտում պետական միջամտության անհրաժեշտությունն անհատական տեղեկատվության պահպանման, ծածկագրման միջոցների օգտագործման ու վաճառքի ազատության և պետական ու այլ կառույցների կողմից ծածկագրերի նկատմամբ պարտադիր մուտքի արգելքի, հատուկ միջոցներով ծնողներին ապահովման հարցում, որոնք հնարավորություն են տալիս կանխելու երեխաների մուտքը դեպի համացանցի անցանկալի ռեսուրսներ:

Հեռահաղորդակցական ցանցերի դերը ոչ թե դրանց բովանդակության, այլ հասանելիության փաստի մեջ է: Եթե անհատը կամ կազմակերպությունը գրանցված չեն ցանցում, ապա նրանք չեն կարող լիարժեք մասնակցություն ունենալ ժամանակակից հասարակական, քաղաքական և տնտեսական կյանքին: Այսօր համացանցը դարձել է առանցքային գործոն, այսինքն՝ ով ներկայացված է և աշխատում է համացանցում, մասնակցում է արդի գործընթացներին, հակառակ դեպքում՝ անհուսալիորեն հետ է մնում դրանից: Հետևաբար՝ կարևորագույն հարց է դառնում ցանցի հասանելիությունը, քանի որ ներառվածությունը տեղեկատվահաղորդակցական տարածքում ժամանակակից հասարակության կյանքին լիարժեք մասնակցության նախապայման է համարվում:

Ակնհայտ է, որ այսօր ձևավորվում է նոր տեղեկատվահաղորդակցական միջավայր, որն աստիճանաբար առավել մեծ թվով մարդկանց է մասնակից դարձնում հարափոփոխ գործընթացներին և տեղեկատվության փոխանակմանը: Փորձագիտական գնահատումների համաձայն՝ 2014 թ. վերջին աշխարհում համացանցի օգտատերերի ընդհանուր թիվն արդեն իսկ պետք է կազմեր շուրջ 3 մլրդ[10]:

Այդ միջավայրում սոցիալական փոխազդեցությունը չի սահմանափակվում հաղորդակցման ավանդական ձևերով: Այդ իմաստով, դրա նախորդ ձևերը կարելի է դիտարկել որպես զարգացման հաջորդական փուլեր:

Հարկ է նշել, որ երբեմն տեղեկատվական տեխնոլոգիան ներկայացվում է կամ որպես ազատության ճնշման գործիք, կամ ազատագրման միջոց:

[10] Տե՛ս МСЭ: количество пользователей Интернета к концу 2014 года достигнет 3 млрд, (09.05.2014), http://www.3dnews.ru/819820

Սակայն, կարծում ենք՝ ցանկացած տեխնոլոգիա, այդ թվում նաև տեղեկատվականը, որպես կանոն, չեզոք է, իսկ դրա դերը և հետևանքները որոշվում են կիրառությամբ: Տեղեկատվության պաշտպանության խնդրի, տեղեկատվությունից պաշտպանելու և տեղեկատվության որակի ապահովման խնդիրների լուծումը պայմանավորում է օբյեկտների գործունեության արդյունավետությունը: Առաջանում է նաև տեղեկատվության արդյունավետ կառավարման խնդիրը՝ տեղեկատվահաղորդակցական միջավայրի հիմնական սուբյեկտների գործունեության անվտանգության հայեցակարգի ձևավորման և պահպանման համար:

Ըստ Վ.Ի. Վասիլենկոյի՝ ներկա պայմաններում նկատելի են երկու հակոտնյա գործընթացներ: Մի կողմից՝ տեղեկատվական ազդակներից կախված, հասարակությունը հարմար օբյեկտ է կառավարման համար, քանի որ հեշտությամբ է ենթարկվում մանիպուլյացիայի (աճպարարություն): Մյուս կողմից՝ հասարակությունը որոշ չափով դառնում է ինքնակառավարվող, քանի որ տեղեկատվությունը, որով ղեկավարվում է սովորական անհատը, միշտ չէ, որ կարգավորվում է իշխանության մարմինների կողմից, իսկ երբեմն էլ ընտրվում է պատահականության սկզբունքով[11]: Միաժամանակ, հասարակությունը որպես վարքագծի կողմնորոշիչներ է ընտրում ոչ թե «իրական» վարքագծով «իրական» մարդկանց, այլ ընդհանրական կերպարների և այս ընտրության դեպքում ևս ղեկավարվում է սեփական ցանկություններով և սպասումներով:

Սակայն, ըստ ազդեցության խորության և ուղղվածության, նոր տեղեկատվական տեխնոլոգիաների հնարավորությունների իրագործման աստիճանը կախված է հասարակության մեջ այն սոցիալ-մշակութային փոփոխություններից, որոնք պետք է նախաձեռնվեն պետության կողմից՝ ներառյալ կենսագործունեության բոլոր ոլորտներում կարգավորման նոր մեխանիզմների կազմակերպումը: Այդ վերափոխումները դեռևս զգալիորեն հետ են մնում տեխնոլոգիական գործընթացի տեմպերից: Տեղեկատվահեռահաղորդակցական տեխնոլոգիաների բոլոր հնարավորությունները և առավելությունները ինքնուրույն չեն կարող գործադրվել: Անհրաժեշտ է որոշակի պետական քաղաքականություն իրականացնել ոչ միայն այդ տեխնոլոգիաների կիրառման, այլև համապատասխան միջավայրում սոցիալական հարաբերությունների կառուցման ոլորտում: Այդ քաղաքականության առանձնահատկությունը կախվածությունն է տեղեկատվահաղորդակցական միջավայրի հասարակ օգտագործողների տրամադրություններից, հավակնություններից և պահանջներից: Դժբախտաբար, երբեմն տեղեկատվական քաղաքականության ձևավորման և իրագործման գործընթացներում գերիշխող դիրք են գրավում մարդիկ, ովքեր հեռու են ազգային և համամարդկային իդեալներից: Արդյունքում՝ ժամանակակից կառավարման սկզբունքները հիմնվում են այն մարդկանց կամ հասարակության կառավարչական խնդիրներին հարմարվողականության վրա, որոնց առջև դրանք դրվում են[12]:

Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգում առանձնացվել են տեղեկատվության ոլորտում ՀՀ ազգային

---

[11] Տե՛ս Информационно-коммуникационная безопасность, նշվ. հրատ., էջ 55:

[12] Տե՛ս **Патракова Г.В.,** Общество как объект управления: вчера и сегодня // Вестник Тюменского государственного университета. 2009, № 5. Сер. “Педагогика. Психология. Философия”, էջ 224–228:

շահերը բնութագրող հինգ հիմնական բաղադրիչներ, որոնք ներառում են պետության ներքին և արտաքին քաղաքականության առանցքային խնդիրները[13]:

Առաջին բաղադրիչը ներառում է տեղեկատվության ստացման և օգտագործման ոլորտում մարդու սահմանադրական իրավունքների և ազատությունների պաշտպանությունը, երկրի հոգևոր զարգացման ապահովումը, հասարակության բարոյական արժեքների, հայրենասիրական և մարդասիրական ավանդույթների, մշակութային և գիտական ներուժի պահպանումն ու ամրապնդումը:

Երկրորդ բաղադրիչն ամփոփում է Հայաստանի Հանրապետության պետական քաղաքականության տեղեկատվական ապահովումը՝ կապված հայ և միջազգային հանրությանը հավաստի տեղեկատվության մատուցման, հանրապետության և միջազգային կյանքում տեղի ունեցող քաղաքական և սոցիալական կարևորագույն իրադարձությունների նկատմամբ պետության պաշտոնական դիրքորոշման իրազեկման հետ՝ միաժամանակ ապահովելով հասանելիությունը պետական բաց տեղեկատվական միջոցներին:

Երրորդ բաղադրիչն ընդգրկում է ժամանակակից տեղեկատվական տեխնոլոգիաների զարգացումը, կապված արտադրանքի ներքին շուկայի պահանջարկի բավարարման և համաշխարհային շուկա արտահանման հետ, ինչպես նաև հայրենական տեղեկատվական միջոցների կուտակման, պահպանման և արդյունավետ օգտագործման ապահովումը:

Չորրորդ բաղադրիչը ներառում է երկրի տեղեկատվական ոլորտի միասնացումը միջազգային տեղեկատվական դաշտին, Հայաստանի և հայության մասին ճշմարիտ տեղեկատվության անկողմնակալ և արհեստավարժ ներկայացումը միջազգային հանրությանը, հակազդումը ապատեղեկատվությանն ու ստահոդ քարոզչությանը, համացանցում և Հայաստանին, հայագիտության բոլոր ճյուղերին ու հայությանն առնչվող հայալեզու տեղեկատվության անհրաժեշտ ծավալի և որակի, ինչպես նաև դրանց համաչափության ապահովումը:

Հինգերորդ բաղադրիչն ընդգրկում է տեղեկատվական ռեսուրսների պաշտպանվածությունը չթույլատրված հասանելիությունից, տեղեկատվության, կապի և հեռահաղորդակցության համակարգերի անվտանգության ապահովումը:

Գտնվելով աշխարհաքաղաքական բարդ տարածաշրջանում և ներքաշված լինելով տարաբնույթ տեղեկատվական ակտիվ ներազդեցությունների և հոսքերի մեջ՝ Հայաստանի Հանրապետությունն ազգային անվտանգության ապահովման համատեքստում այսօր կարևորագույն խնդիր ունի՝ նվազագույնի հասցնել տեղեկատվական ոլորտում պետության ազգային շահերին սպառնացող վտանգների բացասական միտումները: Որպես տեղեկատվական ոլորտի սպառնալիք՝ կարելի է առանձնացնել հեռահաղորդակցային համակարգերի բնականոն գործունեության խաթարումը, ինչպես նաև տեղեկատվական ռեսուրսների և տեղեկատվության միջոցների թույլ պաշտպանվածությունը, չթույլատրված մուտքերի հնարավորությունը, հեռահաղորդակցության ոլորտում մենաշնորհային դիրքի ամրագրումը, անօրինական կարգով տրամադրված տեղեկատվությունը /տեղեկատվության արտահոսք/ և այլն:

---

[13] Տե՛ս Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգ. http://www.arlis.am/documentview.aspx?docID=52559

Պետության տեղեկատվական անվտանգության սպառնալիքները, ըստ ընդհանուր ուղղվածության, դասակարգվում են հետևյալ տիպերի.

1. սպառնալիքներ՝ ուղղված մարդ-քաղաքացու սահմանադրական իրավունքներին և ազատություններին հոգևոր կյանքի և տեղեկատվական գործունեության բնագավառում, նրա անհատական, խմբային և հասարակական գիտակցության ձևավորմանը,
2. սպառնալիքներ՝ ուղղված երկրի պետական քաղաքականության տեղեկատվական ապահովմանը,
3. սպառնալիքներ՝ ուղղված հայրենական տեղեկատվական ռեսուրսների զարգացմանը, արտադրանքի ներքին շուկայի բավարարմանը և համաշխարհային շուկա արտահանմանը, ինչպես նաև հայրենական տեղեկատվական միջոցների կուտակման, պահպանման և արդյունավետ օգտագործման ապահովմանը,
4. սպառնալիքներ՝ ուղղված երկրի տեղեկատվական և հեռահաղորդակցային ռեսուրսների և համակարգերի անվտանգությանը[14]:

Նշված սպառնալիքներն իրենց հերթին ներառում են՝

- պետական իշխանության մարմինների կողմից նորմատիվային իրավական ակտերի ընդունումը, որոնք սահմանափակում են հոգևոր կյանքի և տեղեկատվական գործունեության բնագավառում քաղաքացիների սահմանադրական իրավունքները և ազատությունը,
- նորմատիվների անբավարար մշակվածությունը, որոնք կարգավորում են հարաբերությունները տեղեկատվական ոլորտում,
- տեղեկատվության ձևավորման, ստացման և տարածման մենաշնորհի ստեղծումը,
- քաղաքացիների կողմից իրենց սահմանադրական իրավունքների և ազատության իրագործումը,
- զանգվածային և անհատական գիտակցության վրա ազդեցության արգելված միջոցների կիրառումը (ազդեցություն ենթագիտակցական բնազդների վրա տեսալսողական արտադրանքների, հեռուս-տա-, տեսաֆիլմերի և կինոծրագրերի, ձայնային արահետների, համակարգչային ծրագրերի մեջ թաքնված ներդիրներ[15]),
- պետական իշխանության մարմինների, կազմակերպությունների և քաղաքացիների կողմից օրենսդրության պահանջների անտեսումը,
- անհատական տվյալներ պարունակող գաղտնի տեղեկատվության, պետական գաղտնիքի, բանկային գաղտնիքի և այլնի օգտագործման կանոնների խախտումները,
- մշակութային արժեքների, ներառյալ՝ արխիվների, կուտակման և պահպանման համակարգի ոչնչացումը,
- պետական մարմինների բաց տեղեկատվական ռեսուրսներ քաղաքացիների մուտքի, այլ՝ սոցիալապես արժեքավոր տեղեկատվության սահմանափակումները,
- տեղեկատվության մանիպուլյացիա (ապատեղեկատվություն, տեղեկատվության գաղտնի պահում կամ խեղաթյուրում) և այլն:

---

[14] Տե՛ս **Վ.Կ. Աթոյան,** նշվ. աշխ., էջ 91:

[15] Տե՛ս **Чумаков А.Н., Бочаров М.П.,** Актуальные связи с общественностью: сфера, генезис, технологии, области применения, структуры: учеб.-практ. пособие. М., Высшее образование, Юрайт-Издат, 2009. էջ 230: **Линдстром М.,** Buyology: увлекательное путешествие в мозг современного потребителя / пер. с англ. Е. Фалюк. М., Эксмо, 2010, էջ 83-102:

Ցավոք, այսօր հաճախ անտեսվում են տեղեկատվական քաղաքականության այնպիսի հիմնական բաղկացուցիչներ, ինչպիսիք են՝ տեղեկատվության բովանդակությունը և վերջնական օգտագործողը՝ մարդը, ով նաև այդ տեղեկատվության ստեղծողը, կրողն ու փոխանցողն է: Տեղեկատվության ծավալի աճի պայմաններում փոխվում են ոչ միայն տեղեկատվական հոսքերը, այլև նոր տեղեկատվության հավաքման, պահպանման և դասակարգման վերահսկողության եղանակները, ինչպես նաև հասանելիության և օգտագործման խնդիրները: Դրա շուրջ առաջանում են գործունեության նոր բնագավառներ, որոնք պետության կողմից պահանջում են կարգավորում, ինչպես նաև քաղաքացիների տեղեկատվական անվտանգությանը վերաբերող պետության պատասխանատվության նոր ոլորտների ստեղծում:

Ժամանակակից սպառնալիքների թվին պետք է դասել նաև տեղեկատվական հոսքերի ազդեցությամբ անհատի կառավարման խնդիրը: Քանի դեռ նոր տեղեկատվական տեխնոլոգիաները շարունակում են մնալ սահմանափակ թվով խմբերի ձեռքում, պահպանվում է մարդկանց զանգվածային կառավարման սպառնալիքը: Ուստի կարևոր է ոչ միայն հասկանալ հասարակական փոփոխությունների միտումները, այլև սոցիալական ինստիտուտները հարմարեցնել ներկա և նախապատրաստել ապագա փոփոխություններին:

Անկասկած, պետությունը պետք է իր տեղեկատվական քաղաքականությունում պատշաճ ուշադրություն դարձնի մարդկանց մեջ տեղեկատվություն գտնելու կարողության և տեղեկատվությունից օգտվելու մշակույթի ձևավորմանը, որն անհրաժեշտ է առօրյա կյանքում: Հավաստի անհրաժեշտ տեղեկատվությունը կարևոր է նաև Հայաստանի ազգային անվտանգության ապահովման տեսանկյունից՝ հաշվի առնելով Ադրբեջանի հետ տեղեկատվական և քարոզչական պատերազմի առկայությունը:

Ակնհայտ է, որ տեղեկատվական անվտանգության ապահովումը ազգային անվտանգության համակարգի առանցքային տարրերից է, որի դերն ու նշանակությունը տեղեկատվական-հաղորդակցական միջավայրի զարգացմանը զուգընթաց, բնականաբար, աճելու է: Պատահական չէ, որ այսօր անհատի, հասարակության և պետության տեղեկատվական անվտանգության խնդիրներն ամբողջ աշխարհում մանրակրկիտ ուսումնասիրվում են: Այդ խնդիրների վերլուծության գործում մասնագիտացել են բազմաթիվ միջազգային ճանաչում ունեցող կենտրոններ: Հայաստանը ևս փորձում է հետ չմնալ այդ գործընթացներից: Մասնավորապես՝ այդ ուղղությամբ աշխատանքներ են իրականացնում ՀՀ նախագահի աշխատակազմի Հանրային կապերի և տեղեկատվության կենտրոնը, «Նորավանք» գիտակրթական հիմնադրամը և մի շարք այլ կազմակերպություններ:

Վերջին շրջանում հանրապետությունում իրականացվել են մի շարք միջոցառումներ տեղեկատվական քաղաքականության և անվտանգության ապահովման բարելավման նպատակով, աշխատանքներ են տարվում նաև տեղեկատվական անվտանգության իրավական նորմատիվային դաշտի բարելավման ուղղությամբ: Ընդունվել են այդ բնագավառին առնչվող «Պետական և ծառայողական գաղտնիքի մասին», «Տեղեկատվության ազատության մասին», «Արխիվային գործի մասին», «Անհատական տվյալների մասին», «էլեկտրոնային փաստաթղթի և էլեկտրոնային թվային ստորագրության մասին», «էլեկտրոնային հաղորդակցության մասին», «Զանգվածային լրատվու-

թյան մասին» Հայաստանի Հանրապետության օրենքները, ՀՀ Ազգային ժողովը վավերացրել է «Կիբեռհանցագործությունների մասին» Եվրոխորհրդի կոնվենցիան և նույնի «Համակարգչային համակարգերի միջոցով կատարվող ռասիստական և քսենոֆոբիական բնույթի արարքների քրեականացման մասին» լրացուցիչ արձանագրությունը, աշխատանքներ են տարվում տեղեկատվական ոլորտում հասարակական հարաբերությունները կարգավորող իրավական հիմքերի մշակման, ինչպես նաև իրավակիրառական պրակտիկայի կատարելագործման ուղղությամբ: Սակայն հարկ է նշել, որ Հայաստանի Հանրապետության տեղեկատվական անվտանգության բնագավառում դեռևս կան բազմաթիվ անելիքներ ոլորտը ժամանակի պահանջներին համապատասխանեցնելու առումով:

Մերօրյա փոխկապակցված աշխարհում բազմաթիվ գործողությունների հետևանքներ հաճախ ուղղակի կամ անուղղակի ձևով ազդում են ոչ միայն որոշակի նեղ շրջանակի, այլև համընդգրկուն սոցիալական տարածության վրա: Շատ կարևոր է, որ համաշխարհային քաղաքացիական հասարակությունը ունենա մշակույթի նոր տեսակ, որը մասնագիտական շրջանակներում անվանվում է «անվտանգության գեոտեղեկատվական մշակույթ»: Դա սահմանվում է որպես՝

- քաղաքացիների կողմից «արգելքի կանոնների» գիտակցում և ընդունում սոցիալական համակարգի ապահովման նպատակով,
- համընդհանրական տեղեկատվական տարածության զարգացման միտումների իմացություն և մարդկային վարքագծի նորմերի պարբերական թարմացում,
- սոցիալական փոփոխությունների շարժընթացին համապատասխան՝ «արգելքի կանոնների» շտկման անհրաժեշտություն՝ հաշվի առնելով ազգերի մշակութային բազմազանությունը,
- համաշխարհային սոցիալական տարածությունում մարդկանց համախմբվելու կարողություններ՝ օրինական ճանապարհով նոր «արգելքի կանոնները» պահպանելու նպատակով[16]:

Հարկ է նշել, որ մեզանում անվտանգության գեոտեղեկատվական մշակույթի ոլորտում մշակույթների և տեղեկատվական ցանցային փոխազդեցությունների ողջ բազմազանությունն ընդգրկող հետազոտություններ բավարար չափով չեն կատարվել: Այս առումով, հայրենական գիտությանն առաջադրվում են մի շարք նոր խնդիրներ, որոնք պահանջում են համակարգային լուծում: Մասնավորապես՝ դրանք վերաբերում են կառուցվածքային և ինստիտուցիոնալ փոփոխությունների նորարարական ռազմավարությանը, այդ գործընթացների կառավարման համար նոր մոտեցումների մշակմանը: Ըստ այդմ՝ հարկավոր է որոշել անհատների միջև ընդունելի փոխադարձ կապերը, հաղորդակցություններում մշակույթների, ավանդույթների և սովորույթների բազմազանությունը հաշվի առնելու եղանակները:

Ցանցային տեղեկատվական տարածության համընդհանրացման պայմաններում անվտանգության մշակույթի ձևավորման ևս մեկ կարևոր խնդիր է նշված տարածության և զանգվածային լրատվամիջոցների անվտանգությունը:

---

[16] Տե՛ս **Кузнецов В.Н.,** О социологическом смысле идеологии консолидации: геокультурный аспект // Безопасность Евразии, 2003, № 3 (13):

21-րդ դարում տեղի ունեցող գործընթացներն իմաստավորման կարիք ունեն: Մի կողմից՝ թարմացվում է ընդհանուր բառապաշարը. լայնորեն սկսել են օգտագործվել հատուկ հասկացություններ՝ զանգվածային լրատվամիջոց (մասսմեդիա), տեղեկատվական մշակույթ, տեղեկատվական անվտանգություն, մեդիակրթություն, կրեատիվություն և այլն: Մյուս կողմից՝ գիտական հանրության առջև խնդիր է դրվում հետազոտել անհատական և զանգվածային գիտակցության վրա ԶԼՄ-ների ազդեցության հետևանքները:

Յուրաքանչյուր պետության տեղեկատվական անվտանգության ապահովումը ենթադրում է տեղական և միջազգային համապատասխան դաշտում որոշակի հիմնախնդիրների առանձնացում ու դրանց լուծմանն ուղղված համակարգային միջոցառումների իրականացում: Այս դեպքում համակարգային մոտեցմամբ շեշտադրվում են այն առանցքային նպատակներն ու խնդիրները, որոնց ձևակերպումն ու լուծումը կնպաստեն պետության և հասարակության պաշտպանվածությանը ինչպես կարճաժամկետ, այնպես էլ երկարաժամկետ հեռանկարում:

Տեղեկատվության պաշտպանությունը ենթադրում է՝

- անհատին, հասարակությանը և պետությանը սպառնացող վտանգների կանխում,
- տեղեկատվության արտահոսքի, յուրացման, կորստի, խեղաթյուրման, կեղծման, ռեսուրսների և համակարգերի մեջ անօրինական միջամտության կանխում,
- պետական և անձնական գաղտնիք պարունակող տեղեկությունների և տվյալների պահպանում:

Ելնելով վերոնշյալից՝ առանձնացնենք Հայաստանի Հանրապետության տեղեկատվական ոլորտի կարևորագույն խնդիրները.

- տեղեկատվական ոլորտում ՀՀ քաղաքացիների սահմանադրական իրավունքների և ազատությունների պաշտպանությունն ու օրենսդրական դաշտի կատարելագործումը,
- համաշխարհային տեղեկատվական տարածքին ՀՀ միասնացումը և համապատասխան ենթակառուցվածքների կատարելագործումն ու պաշտպանությունը,
- տեղեկատվության ոլորտի մասնակիցների գործունեության համար հավասար պայմանների ստեղծումը և սպառնալիքների կանխումը,
- պետական գաղտնիք համարվող տեղեկատվության պաշտպանությանն ուղղված միջոցառումների մշակումն ու իրականացումը,
- արտաքին տեղեկատվական ագրեսիայի և հասարակական կարծիքի մանիպուլյացիայի, հասարակական գիտակցությանը հասցվող բարոյական վնասի կանխմանը միտված միջոցառումների իրականացումը,
- տեղեկատվական անվտանգության ապահովման մասնագետների պատրաստումն ու վերապատրաստումը,
- ԶԼՄ-ների և թեմատիկ սեմինարների անցկացման միջոցով ՀՀ քաղաքացիների իրազեկումը տեղեկատվական անվտանգության ապահովման հիմնական խնդիրների և այս ոլորտում իրենց ազատությունների ու իրավունքների մասին:

Այսպիսով՝ տեղեկատվական-հաղորդակցական անվտանգության խնդիրների համատեքստում արդի ժամանակաշրջանի սպառնալիքներին և համընդգրկուն մարտահրավերներին դիմակայելու համար անհրաժեշտ ենք համարում.

- հասարակական զարգացման, հայ հասարակության համախմբման, հայ ժողովրդի հոգևոր վերելքի ապահովման նպատակով բարձրացնել տեղեկատվական ենթակառուցվածքների գործունեության արդյունավետությունը՝ կատարելագործելով հոգևոր ներուժի համար որպես հիմք ծառայող տեղեկատվական ռեսուրսների ձևավորման, պահպանման և օգտագործման համակարգը,
- ստեղծել զանգվածային տեղեկատվության ազատության գործուն երաշխիքներ՝ միաժամանակ կանխելով սոցիալական, ազգային կամ կրոնական ատելության բորբոքմանը նպաստող տեղեկատվության հոսքը,
- հզորացնել պետական և հանրային տեղեկատվական ռեսուրսները, ձևավորել միասնական համահայկական տեղեկատվական տարածություն, որը կարող է նպաստել մեր պետության միջազգային կշռի և դերակատարման մեծացմանը,
- հեռահաղորդակցության և տեղեկատվության ոլորտներում հիմնարար մշակումների և կիրառական հետազոտությունների իրականացմանը ցուցաբերել պետական աջակցություն, բարձրացնել այդ բնագավառներում ընդգրկված կադրերի մասնագիտական մակարդակը, զարգացնել միջազգային համագործակցությունը և խթանել միջազգային կրթական փոխանակման ծրագրերի իրագործումը,
- կիբեռհանցագործությունների նորահայտ տեսակների բացահայտման, ուսումնասիրման և դրանց դեմ պայքարի արդյունավետության մակարդակի բարձրացման նպատակով ակտիվացնել շահագրգիռ կողմերի միջև (համացանցային ծառայություններ մատուցող կազմակերպություններ, իրավապահ մարմիններ) տեղեկությունների փոխանակումը, ընդլայնել միջազգային համագործակցությունը տեղեկատվական ռեսուրսների զարգացման և անվտանգ կիրառման, ինչպես նաև տեղեկատվական ոլորտում սպառնալիքներին հակազդման գործում:

ВАРДАН АТОЯН
Директор программы ,,Исследования национальной безопасности" исследовательского центра ,,Амберд" АГЭУ, кандидат экономических наук

ЛИЛИТ ДАДАЯН
Доцент кафедры ,,Маркетинга" АГЭУ, кандидат экономических наук

О современных проблемах обеспечения информационно-коммуникационной безопасности.– Статья посвящена одному из ключевых направлений национальной безопасности - современным проблемам обеспечения информационной безопасности.

Для того, чтобы противостоять качественно новым угрозам и глобальным вызовам перехода к постиндустриальному или информационному обществу современной эпохи, которая характеризуется радикальными изменениями от промышленного общества, на местном и международном информационном поле необходимо руководствоваться такими правилами, в которых решающее значение имеют координация и контроль информационных потоков и обеспечение безопасности.

В контексте проблем информационно-коммуникационной безопасности в статье представлены те ключевые цели и задачи, формулировка и системное решение которых будут способствовать повышению безопасности личности, общества и государства в информационной сфере как в краткосрочной, так и в долгосрочной перспективе.

Ключевые слова: *информационная безопасность, национальная безопасность, угроза, информационно-коммуникационная среда, национальные интересы, информационные ресурсы.*

VARDAN ATOYAN
Director of "National Security Research" Program at "Amberd" Research Center, ASUE, PhD in Economics

LILIT DADAYAN
Associate Professor at the Chair of "Marketing" at ASUE, PhD in Economics

Issues Related to the Security of Information and Communication Systems.– The report is devoted to the issues related to insuring information security that are key for the national defense.

In the current era of information age it's necessary to be prepared for new threats and global attacks, and as such the local and international information and communication systems

should be based on rules and regulations that provide oversight and defense of information flow.

The report discusses the goals and issues related to the information and communication systems which will enhance the security for individuals, society and the national defense in the short-term as well as in the long-term period.

Key words: *information security, national security, threat, information and communication environment, national interests, information resources.*