ԵՐԻՏԱՍԱՐԴ ԳԻՏՆԱԿԱՆԻ ԱՄԲԻՈՆ

DOI: 10.59560/18291155-2024.2-180

ՇՈՂԵՐ ԳՐԻԳՈՐՅԱՆ
ՀՀ ՆԳՆ փրկարար ծառայության ծառայության կազմակերպման վարչության հրահանգիչ, Հայ-ռուսական համալսարանի քաղաքագիտության ամբիոնի հայցորդ

ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀԱՅԵՑԱԿԱՐԳԸ ԺԱՄԱՆԱԿԱԿԻՑ ՄԱՐՏԱՀՐԱՎԵՐՆԵՐԻ ՀԱՄԱՏԵՔՍՏՈՒՄ

Ամփոփագիր

Ժամանակակից աշխարհում տեղեկատվական անվտանգությունն առանցքային դեր է խաղում պետությունների կայունության և անվտանգության պահպանման գործում: Վերջին տարիներին, միջազգային ասպարեզում ընթացող գործընթացներով պայմանավորված՝ պետություններն ավելի մեծ և առաջնային ուշադրություն են դարձնում տեղեկատվական անվտանգության ապահովմանը, ինչպես նաև ոլորտում հնարավոր սպառնալիքների և մարտահրավերների հակազդմանը:

Սույն հոդվածում ուսումնասիրվում է տեղեկատվական անվտանգության հայեցակարգը՝ շեշտը դնելով դրա քաղաքական ասպեկտի վրա, որը կարևոր է ազգային ինքնիշխանության և պետական կայունության պահպանման համար: Տեղեկատվական անվտանգությունն այս համատեքստում ներառում է տեղեկատվական տարածքի պաշտպանությունը արտաքին և ներքին սպառնալիքներից, ինչպիսիք են ապատեղեկատվությունը, քարոզչությունը և հիբրիդային պատերազմը: Գլոբալիզացիայի և տեխնոլոգիաների արագ զարգացման համատեքստում տեղեկատվությունը դառնում է կարևոր

ռազմավարական ռեսուրս, և դրա պաշտպանությունը անհրաժեշտ պայման է ազգային անվտանգության ապահովման համար:

Հոդվածում ընդգծվում է, որ տեղեկատվական անվտանգությունը քաղաքական համատեքստում պահանջում է ինտեգրված մոտեցում, որը համատեղում է տեխնոլոգիական, իրավական, կրթական և միջազգային միջոցառումները: Միայն բոլոր մակարդակներում ջանքերի համակարգման միջոցով է հնարավոր արդյունավետ հակազդել ժամանակակից տեղեկատվական սպառնալիքներին և ապահովել տեղեկատվական հասարակության երկարաժամկետ կայունությունն ու անվտանգությունը:

Հիմնաբառեր. տեղեկատվական անվտանգություն, մարտահրավերներ, սպառնալիքներ, հիբրիդային պատերազմներ, ապատեղեկատվություն, ռազմավարություն, քաղաքական կայունություն:

1. Տեղեկատվական անվտանգության հայեցակարգը

Անվտանգության հայեցակարգը, չնայած իր թվացյալ պարզությանը, ընդգրկում է հասարակության և անհատի կյանքի տարբեր ասպեկտներ: Գրականության մեջ կարելի է գտնել այս հասկացության տարբեր մեկնաբանություններ և սահմանումներ: Օրինակ, հաճախ կարելի է գտնել հետևյալ սահմանումը. «Ազգային անվտանգությունն ազգի ընդունակությունն է՝ պահպանելով իր հիմնարար արժեքները հնարավորինս նվազագույն կորուստներով՝ բավարարել այն պահանջները, որոնք անհրաժեշտ են ինքնապաշտպանության, ինքնավերարտադրման և ինքնակատարելագործման համար»: Չնայած այս սահմանումը բավականին ընդգրկուն է, սակայն ամբողջությամբ չի արտացոլում շրջակա միջավայրի փոփոխականությունը: Ուստի արժեքավոր է անդրադառնալ Առնոլդ Թոյնբիի տեսակետներին, ով նշանակալի ներդրում է ունեցել անվտանգության փիլիսոփայության զարգացման գործում:

Ըստ Թոյնբիի դասական հայացքների՝ քաղաքակրթությունների, պետությունների, հասարակությունների և անգամ անհատների անվտանգությունն ապահովվում է նրանց՝ մարտահրավերների և

դրանց տրվող պատասխանների բարդ համակարգում գործելու ունակությամբ: Թոյնբին ընդգծել է, որ մարտահրավերներին համարժեք չպատասխանելը աղետալի է քաղաքակրթությունների համար: Կարևոր է հիշել, որ մարտահրավերները կարող են հնարավորությունների աղբյուր լինել, քանի որ դրանք ստուգում, փորձաքննում են անվտանգության համակարգի հուսալիությունը և, մարտահրավերներին արժանիորեն դիմագրավելու նպատակով, մոբիլիզացնում են հանրության հոգևոր, մտավոր, ռազմական, քաղաքական ու նյութական ռեսուրսները[1]:

Թոյնբիի դատողությունները կիրառություն են գտնում նաև տեղեկատվական անվտանգության ոլորտում: Վերջինիս շրջանակները երբեմն նեղացվում են, թեև այն ներառում է բազմաթիվ ասպեկտներ, ինչպիսիք են.

- ազգի, պետության, հասարակության և անհատի հոգևոր, հոգեբանական, մտավոր, ճանաչողական և կրթական ոլորտների արդյունավետ զարգացման, կառավարման և անվտանգության ապահովումը.
- պետության, հասարակության և անհատների մակարդակով տեղեկատվական տեխնոլոգիաների համակարգերի արդյունավետ զարգացման և անվտանգության ապահովումը:

Այս և այլ մոտեցումների հիման վրա մասնագիտական գրականության մեջ առաջարկվել են տեղեկատվական անվտանգության բազմաթիվ սահմանումներ:

Օրինակ՝ «Տեղեկատվական անվտանգությունը տեղեկատվության և այն ապահովող ենթակառուցվածքների պաշտպանվածությունն է պատահական կամ միտումնավոր ազդեցություններից», «Ներազդող սպառնալիքների և դրանց արդյունավետ հակազդելու գործընթացների միջև հավասարակշռության պահպանման գործընթաց է»[2] և այլն:

[1] Տես **Тойнби А.Дж.** Цивилизация перед судом истории. Сборник. - М.: Айрис Пресс, 2003. - 592 с.:

[2] Տես ***Հարությունյան Գ.Ա.,*** Տեղեկատվական անվտանգություն: Եր., «Նորավանք» ԳԿՀ, 2017, 320 էջ:

Տարբեր է հասկացության բովանդակությունը նաև անգլալեզու, ռուսալեզու և հայալեզու գրականության մեջ, ինչպես նաև հայեցակարգային փաստաթղթերում: Այսպես՝ անգլալեզու գրականության մեջ «տեղեկատվական անվտանգություն» (information security) հասկացությունը սահմանվում է որպես տեղեկատվության և աջակցող ենթակառուցվածքների պաշտպանվածություն բնական կամ արհեստական բնույթի պատահական կամ կանխամտածված ազդեցություններից, որոնք տեղեկատվական հարաբերությունների սուբյեկտներին, այդ թվում՝ տեղեկատվությունը տիրապետողին ու օգտագործողին, ինչպես նաև աջակցող ենթակառուցվածքին կարող են անուղղակի վնաս հասցնել: Հասկացության մեկ այլ սահմանմամբ՝ «տեղեկատվական անվտանգությունը տեղեկույթի և տեղեկատվական համակարգերի չարտոնված մուտքից, օգտագործումից, հրապարակումից, փոփոխումից կամ ոչնչացումից պաշտպանությունն է, որպեսզի ապահովված լինեն գաղտնիությունը, ամբողջականությունը և մատչելիությունը»: Այս իմաստով տեղեկատվական անվտանգության հոմանիշներն են «կիբեռանվտանգությունը» (Cybersecurity) և «համակարգչային անվտանգությունը» (Computer security)[1]:

Ռուսալեզու գրականության մեջ տեղեկատվական անվտանգության ժամանակակից խնդիրների սահմանման համար հիմք են հանդիսացել Ի.Ա. Լազարևի, Վ.Ն. Լոպատինի, Յու.Ս. Ուֆիմցևի, Ե.Ա. Երոֆեևի համակարգային հետազոտությունները: Այսպես՝ Վ.Ն. Լոպատինն առանձնացնում է տեղեկատվական–հոգեբանական անվտանգությունը և այն սահմանում որպես վնասակար տեղեկատվության ազդեցությունից անհատի, հասարակության և պետության կենսական կարևոր շահերի պաշտպանության իրավիճակ[2]:

[1] Տե՛ս Analysis of information security issues in corporate computer networks (Վերջին մուտքը՝ 15.05.2024 թ.),
URL: https://iopscience.iop.org/article/10.1088/1757-899X/1047/1/012117/meta#:~:text=Information%20security%20is%20understood%20as,or%20users%20of%20information%20resources

[2] Տե՛ս **Лопатин В.Н.** Информационное право: Учебник. - СПб., 2005 - 474 с.:

Ա.Դ. Ուրսուլը տեղեկատվական անվտանգությունը սահմանում է որպես տեղեկատվական վտանգավոր ազդեցություններից կենսագործունեության հիմնական բնագավառների պաշտպանության վիճակ[1]: Տ. Ա. Պոլյակովան տեղեկատվական անվտանգությունը դիտում է որպես ազգային շահերի պաշտպանության վիճակ և դա համարում անհատի, հասարակության ու պետության հավասարակշռված շահերի ամբողջություն:

Ինչ վերաբերում է հայալեզու գրականությանը, նշենք, որ ՀՀ ՊՆ ԱՌՀԻ-ի՝ արևմտյան ու ռուսաստանյան պաշտպանական-անվտանգային տերմինաբանական-հասկացութային համակարգերի համադրմամբ կազմված եռալեզու բացատրական բառարանում տեղեկատվական անվտանգությունը բացատրվում է որպես «սուբյեկտի (անհատի, հասարակության) այն վիճակը, որի դեպքում տեղեկույթի և սուբյեկտի փոխազդեցության հետևանքով սուբյեկտի մեջ առաջացած փոփոխությունը սպառնալիք չի հարուցում նրա ֆիզիկական ու հոգեկան առողջության, ինչպես նաև հասարակության ու պետության համար»[2]:

Ընդհանրացնելով և շեշտելով անվտանգության խնդիրներում գիտակրթական-տեխնոլոգիական ռեսուրսների ու հանրության ընդհանրական հմտությունների որոշիչ կարևորությունը՝ տեղեկատվական անվտանգությունը կարելի է սահմանել նաև հետևյալ կերպ. «Տեղեկատվական անվտանգությունը պետության և հասարակության գիտելիքային-տեխնոլոգիական անհրաժեշտ ռեսուրսների ստեղծման միջոցով հանրության անվտանգությունը և զարգացումն ապահովելու ունակությունն է տեղեկատվական մարտահրավերներ-պատասխաններ գործընթացում»[3]:

[1] Տես **Урсул А.Д.** Информатизация общества и безопасность развития цивилизации // "Социально политические науки", 1990, № 10:

[2] Տես **Չիլինգարյան Դ.Ս., Երզնկյան Ե.Լ.,** Պաշտպանական-անվտանգային տերմինների բացատրական հայերեն-ռուսերեն-անգլերեն, ռուսերեն-հայերեն, անգլերեն-հայերեն մեծ բառարան: Եր., 2015:

[3] Տես **Հարությունյան Գ.Ա.,** Տեղեկատվական անվտանգություն: Եր., «Նորավանք» ԳԿՀ, 2017:

2. Տեղեկատվական անվտանգության ժամանակակից մարտահրավերները

Այսօր տեղեկատվական անվտանգության մարտահրավերները բխում են ինչպես արագ տեխնոլոգիական փոփոխություններից, այնպես էլ սոցիալական, տնտեսական և քաղաքական գործոններից:

Ժամանակակից տեղեկատվական անվտանգության մարտահրավերները բազմազան են և բազմակողմանի: Հիմնականներից մեկը հիբրիդային պատերազմների երևույթն է, որտեղ տեղեկատվությունը օգտագործվում է որպես քաղաքական և տնտեսական համակարգերը ապակայունացնելու գործիք: Սա ներառում է ապատեղեկատվության և կեղծ լուրերի տարածում, որոնք ուղղված են պետական կառույցների նկատմամբ վստահությունը խաթարելուն և սոցիալական հակամարտությունների սրմանը: Նման տեղեկատվական հարձակումները կարող են երկարաժամկետ ազդեցություն ունենալ հասարակական կարծիքի և քաղաքական կայունության վրա[1]:

Տեղեկատվական պատերազմն ինֆոգեն սպառնալիքների գործնական իրագործումն է, որում որպես թիրախ հատկապես կարևորվում է քաղաքական որոշումների ընդունման համակարգը: Հաճախ քարոզչությունն ու ապատեղեկատվությունն օգտագործում են հասարակական կարծիք ձևավորելու, քաղաքական ինստիտուտների նկատմամբ վստահությունը խաթարելու և քաղաքական իրավիճակն ապակայունացնելու համար[2]: Օրինակները ներառում են.

- Քարոզչությունը. միակողմանի կամ կեղծ տեղեկատվության համակարգված տարածումն է՝ հասարակական կարծիքը շահարկելու նպատակով: Պետությունները կարող են քարոզչությունն օգտագործել իրենց քաղաքական դիրքորոշումները պաշտպանելու և հակառակորդներին վարկաբեկելու համար: Պատմականորեն դա դրսևորվել է տպագիր և հեռուստատեսային լրատվամիջոցների միջոցով, սակայն վերջին տարիներին սոցիալական մեդիան դարձել է հիմնական քարոզչական գործիք:

[1] Տես Гибридное оружие войны, URL: https://www.gazeta.ru/army/2016/08/10/10112729.shtml (Վերջին մուտքը՝ 15. 05. 2024 թ.):

[2] Տես **Հարությունյան Գ.Ա.,** Տեղեկատվական անվտանգություն: Եր., «Նորավանք» ԳԿՀ, 2017:

- Ապատեղեկատվությունը. բնակչությանը կամ պետական մարմիններին մոլորեցնելու նպատակով դիտավորյալ կեղծ տեղեկատվության տարածումն է: Ապատեղեկատվությունը կարող է ներառել կեղծ լուրեր, կեղծ փաստաթղթեր և խեղաթյուրված փաստեր: Այն հաճախ օգտագործվում է քաոս ստեղծելու, հասարակության վստահությունը խաթարելու և ընտրությունների վրա ազդելու համար:

Տեղեկատվական անվտանգության ժամանակակից մարտահրավերներից են քաղաքական լրտեսությունը և տվյալների արտահոսքը:

Քաղաքական լրտեսությունը ներառում է հետախուզական ծառայությունների և այլ գործակալների գործունեությունը, որն ուղղված է գաղտնի տեղեկատվության հասանելիությանը:

Ժամանակակից տեխնոլոգիաները հնարավորություն են տալիս հեռակա կարգով լրտեսություն իրականացնել կիբեռհարձակումների միջոցով, ինչը մեծացնում է տվյալների արտահոսքի վտանգը և պահանջում ուժեղացված անվտանգության միջոցներ:

Տվյալների արտահոսք կարող է առաջանալ նպատակաուղղված հարձակումների արդյունքում, աշխատակիցների կողմից անփութության կամ չարաշահումների հետևանքով: Արտահոսքերը կարող են հանգեցնել գաղտնի փաստաթղթերի բացահայտմանը, ինչը կարող է զգալի վնաս հասցնել ազգային անվտանգությանը և միջազգային հարաբերություններին:

Ժամանակակից տեխնոլոգիաները և լրատվամիջոցները հնարավորություն են տալիս աննախադեպ մակարդակով շահարկել հասարակական կարծիքը: Սոցցանցերի և այլ թվային հարթակների օգտագործումը քարոզչություն և ապատեղեկատվություն տարածելու համար դարձել է քաղաքական գործընթացների վրա ազդելու կարևորագույն գործիք:

Համացանցի և սոցիալական ցանցերի միջոցով տարածվող կեղծ կամ խեղաթյուրված լուրերը կարող են լուրջ ազդեցություն ունենալ իրադարձությունների ընկալման և հասարակական կարծիքի ձևավորման վրա: Կեղծ լուրերի դեմ պայքարը պահանջում է և՛ տեխնոլոգիական լուծումներ (օրինակ՝ անարժանահավատ տեղեկատվությունը

բացահայտելու ալգորիթմներ), և՛ օրենսդրական կարգավորումներ, և՛ բնակչության մեդիա գրագիտության բարձրացում:

Միևնույն ժամանակ, տեղեկատվական անվտանգության հիմնական մարտահրավերներից մեկը անվտանգության ապահովման և խոսքի ազատության պաշտպանության միջև հավասարակշռություն գտնելն է: Մի կողմից՝ անհրաժեշտ է սահմանափակել ապատեղեկատվության և քարոզչության տարածումը, մյուս կողմից՝ կարևոր է պահպանել քաղաքացիների կարծիքն ազատ արտահայտելու իրավունքը:

Նմանօրինակ իրավիճակներում, հաղորդակցման ուղիները վերահսկելու և վնասակար տեղեկատվության տարածումը կանխարգելելու համար պետությունները կարիք ունեն մշակելու նոր կանոնակարգեր և ռազմավարություններ:

3. Տեղեկատվական անվտանգության ապահովման ռազմավարությունները

Տեղեկատվական անվտանգությունն ապահովելու համար պետությունները մշակում և իրականացնում են համապարփակ ռազմավարություններ: Սա ներառում է օրենսդրական կարգավորում՝ ուղղված տեղեկատվական տարածքի պաշտպանությանը և ապատեղեկատվությանը հակազդելուն, ինստիտուցիոնալ պաշտպանություն մասնագիտացված մարմինների և ստորաբաժանումների ստեղծման միջոցով, կրթական ծրագրեր՝ ուղղված տեղեկատվական գրագիտության մակարդակի բարձրացմանը, և միջազգային համագործակցություն՝ արդյունավետորեն պայքարելու անդրազգային տեղեկատվական սպառնալիքների դեմ:

Տեղեկատվական անվտանգության հստակ քաղաքականության և չափորոշիչների մշակումը գերակա առաջնահերթություն է պետական կառույցների և քաղաքական հաստատությունների համար: Այս քաղաքականությունը պետք է սահմանի տեղեկատվության մշակման, պահպանման և փոխանցման կանոններն ու ընթացակարգերը, ինչպես նաև սպառնալիքներից և հարձակումներից պաշտպանվելու միջոցները: Կարևոր է, որ նման քաղաքականությունը հաշվի առնի

քաղաքական ոլորտի հատուկ կարիքները, ներառյալ ընտրությունների, դիվանագիտական հարաբերությունների և ռազմավարական որոշումների հետ կապված տեղեկատվության պաշտպանությունը:

Տեղեկատվական անվտանգության ռազմավարության կարևոր բաղադրիչներից է տեղեկատվական անվտանգության առաջադեմ տեխնոլոգիաների մշակումն ու ներդրումը: Սա ներառում է գաղտնագրման, վիրուսների և չարամիտ ծրագրերի պաշտպանության, ներխուժման հայտնաբերման համակարգերի և նույնականացման մեխանիզմների օգտագործումը:

Մյուս կարևոր բաղադրիչը միջազգային համագործակցությունն է: Տեղեկատվական սպառնալիքների գլոբալացման համատեքստում միջազգային համագործակցությունը գնալով ավելի է կարևորվում: Պետությունները պետք է ակտիվորեն համագործակցեն տեղեկատվական անվտանգության ոլորտում, համատեղ մշակեն պաշտպանական միջոցներ և համակարգեն գործողությունները կիբեռհարձակումների կամ տեղեկատվական արշավների դեպքում: Սա նաև ներառում է համագործակցություն միջադեպերի հետաքննության և տեղեկատվական անվտանգության լավագույն փորձի փոխանակման համար:

Ռազմավարության կարևոր կողմն է համարվում իրավական պաշտպանությունը: Արդյունավետ քաղաքականության իրականացումը, իր հերթին, պայմանավորված է ինչպես համապատասխան իրավական փաստաթղթերի մշակմամբ, այնպես էլ իրավակիրառ պրակտիկայում ոլորտում առկա խնդիրների շարունակական լուծմանն ուղղված թիրախային միջոցառումների իրականացմամբ, դրանց ղեկավարման, մոնիտորինգի արդյունավետ ընթացակարգերի կենսագործմամբ:

4. Եզրակացություն

Տեղեկատվական անվտանգության ժամանակակից մարտահրավերները պետություններից պահանջում են ինտեգրված մոտեցում, ներառյալ տեխնիկական, կազմակերպչական և իրավական միջոցները՝ քաղաքականապես զգայուն տեղեկատվության պաշտպանության համար: Գլոբալիզացիայի և թվայնացման համատեքստում տեղեկատվական անվտանգության ապահովումը

դառնում է պետական ռազմավարության անբաժանելի մասը, որը նպաստում է կայուն զարգացմանը և հասարակության շահերի պաշտպանությանը:

Այսպիսով, միայն ինտեգրված և համակարգված մոտեցումը կարող է ապահովել տեղեկատվության հուսալի պաշտպանությունը ժամանակակից սպառնալիքներից, նպաստել քաղաքական կայունության և պետական անվտանգության ամրապնդմանը համաշխարհային տեղեկատվական տարածքում: Տեխնոլոգիաների շարունակական զարգացման և մշակված տեղեկատվության ծավալների մեծացման պայմաններում տեղեկատվական անվտանգության ապահովումը դառնում է պետական գերատեսչությունների առանցքային խնդիրներից մեկը՝ ուղղված ազգի ինքնիշխանության և անվտանգության պահպանմանը:

Օգտագործված գրականության ցանկ

1. **Հարությունյան Գ.Ա.,** Տեղեկատվական անվտանգություն: Եր., «Նորավանք» ԳԿՀ, 2017, 320 էջ:

2. **Չիլինգարյան Դ.Ս., Երզնկյան Ե.Լ.,** Պաշտպանական-անվտանգային տերմինների բացատրական հայերեն-ռուսերեն-անգլերեն, ռուսերեն-հայերեն, անգլերեն-հայերեն մեծ բառարան: Եր., 2015:

3. **Лопатин В.Н.** Информационное право: Учебник. - СПб., 2005. - 474 с.

4. **Тойнби А.Дж.** Цивилизация перед судом истории. Сборник. - М.: Айрис Пресс, 2003. - 592 с.

5. **Урсул А.Д.** Информатизация общества и безопасность развития цивилизации // “Социально политические науки”, 1990, № 10.

6. Гибридное оружие войны, URL: https://www.gazeta.ru/army/2016/08/10/10112729.shtml (Վերջին մուտքը՝ 15.05.2024թ.).

7. Analysis of information security issues in corporate computer networks (Վերջին մուտքը՝ 15.05.2024թ.), URL:https://iopscience.iop.org/

article/10.1088/1757-899X/1047/1/012117/meta#:~:text=Information%20security%20is%20understood%20as,or%20users%20of%20information%20resources

ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ СОВРЕМЕННЫХ ВЫЗОВОВ

Аннотация

В современном мире информационная безопасность играет ключевую роль в поддержании стабильности и безопасности государств. В последние годы в связи с процессами, происходящими на международной арене, государства уделяют все больше приоритетного внимания обеспечению информационной безопасности, а также противодействию возможным угрозам и вызовам в этой сфере.

В данной статье рассматривается понятие информационной безопасности, подчеркивается ее политический аспект, который важен для поддержания национального суверенитета и государственной стабильности. Информационная безопасность в этом контексте включает защиту информационной сферы от внешних и внутренних угроз, таких как дезинформация, пропаганда и гибридная война. В условиях глобализации и стремительного развития технологий информация становится важным стратегическим ресурсом, а ее защита – необходимым условием обеспечения национальной безопасности.

В статье подчеркивается, что информационная безопасность в политическом контексте требует комплексного подхода, сочетающего в себе технологические, правовые, образовательные и международные меры. Только благодаря координации усилий на всех уровнях можно эффективно противостоять современным информационным угрозам и обеспечить долгосрочную стабильность и безопасность информационного общества.

Ключевые слова: информационная безопасность, вызовы, угрозы, гибридные войны, дезинформация, стратегия, политическая стабильность.

THE CONCEPT OF INFORMATION SECURITY IN THE CONTEXT OF MODERN CHALLENGES

Annotation

In the modern world, information security plays a key role in maintaining the stability and security of states. In recent years, due to the processes taking place in the international arena, states pay more and more priority attention to ensuring information security, as well as countering possible threats and challenges in the field.

This article examines the concept of information security, emphasizing its political aspect, which is important for maintaining national sovereignty and state stability. Information security in this context includes protecting the information sphere from external and internal threats such as disinformation, propaganda and hybrid warfare. In the context of globalization and the rapid development of technology, information is becoming an important strategic resource, and its protection is a necessary condition for ensuring national security.

The article emphasizes that information security in a political context requires an integrated approach that combines technological, legal, educational and international measures. Only through coordination of efforts at all levels can we effectively counter modern information threats and ensure long-term stability and security of the information society.

Keywords: information security, challenges, threats, hybrid wars, disinformation, strategy, political stability.

Հոդվածը հանձնված է խմբագրություն 19.05.2024 թ., տրվել է գրախոսության 20.05.2024 թ., ընդունվել է տպագրության 21.05.2024 թ.: