ՀՀ ՊՆ ՊԱՇՏՊԱՆԱԿԱՆ ԱԶԳԱՅԻՆ ՀԵՏԱԶՈՏԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

ՄԿՐՏՉՅԱՆ ՀԱՅԿՈՒՀԻ ՎԱՐԴԳԵՍԻ

ՀՀ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ՀԻՄՆԱԽՆԴԻՐՆԵՐԸ ՀԱՄԱՇԽԱՐՀԱՅՆԱՑՄԱՆ ՊԱՅՄԱՆՆԵՐՈՒՄ

ԻԳ. 00. 02 «Քաղաքական ինստիտուտներ և գործընթացներ, միջազգային հարաբերություններ» մասնագիտությամբ
քաղաքական գիտությունների թեկնածուի գիտական աստիճանի հայցման ատենախոսության սեղմագիր

ԵՐԵՎԱՆ-2018

Ատենախոսության թեման հաստատվել է **Երևանի պետական համալսարանում:**

Գիտական ղեկավար՝ պատմական գիտությունների դոկտոր, պրոֆեսոր, ՀՀ ԳԱԱ թղթակից անդամ **Ա. Հ. Սիմոնյան**

Պաշտոնական ընդդիմախոսներ՝ քաղ.գիտ. դոկտոր, պրոֆեսոր, **Տ. Տ. Քոչարյան**

քաղ. գիտ. թեկնածու **Վ. Ա. Դիլանյան**

Առաջատար կազմակերպություն՝ **Հայ-ռուսական համալսարան**

Ատենախոսության պաշտպանությունը տեղի կունենա 2018թ. մայիսի 4–ին՝ ժամը՝ 15:00-ին, ՀՀ ՊՆ Պաշտպանական ազգային հետազոտական համալսարանում գործող ՀՀ ԲՈՀ-ի «Քաղաքագիտություն» 056 մասնագիտական խորհրդի նիստում:

Մասնագիտական խորհրդի հասցեն՝ ՀՀ, Երևան-0037, Կ. Ուլնեցու փողոց 56/6:

Ատենախոսությանը կարելի է ծանոթանալ ՀՀ ՊՆ ՊԱՀՀ-ի գրադարանում:

Սեղմագիրն առաքված է 2018թ. ապրիլի 4–ին:

056 մասնագիտական խորհրդի գիտական քարտուղար,
հոգեբանական գիտությունների թեկնածու,
դոցենտ՝ Զ. Դ. Ասատրյան

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ԸՆԴՀԱՆՈՒՐ ԲՆՈՒԹԱԳԻՐԸ

Ուսումնասիրության թեմայի արդիականությունը պայմանավորված է տարածաշրջանային բարդ իրադրության պայմաններում ՀՀ տեղեկատվական անվտանգության հիմնախնդիրների հետազոտության կարևորությամբ: Երկար տարիներ շարունակվում է տեղեկատվական հակամարտությունը հարևան Ադրբեջանի հետ: 2016թ. ապրիլյան քառօրյա պատերազմը ցույց տվեց, որ Հայաստանը պարբերաբար ենթարկվում է տեղեկատվական ագրեսիայի: Ընդ որում, եթե նախկինում ադրբեջանցի հաքերները հարձակում էին գործում պետական կառույցների կայքերի վրա, ապա այսօր նրանց հետաքրքրում են նաև սոցցանցերից օգտվողների էջերը:

Բացի այդ, մեր երկիրը բավականին խոցելի է կիբեռսպառնալիքների առումով, քանի որ չունի կիբեռանվտանգության հստակորեն ձևակերպված ռազմավարություն, նման սպառնալիքներին հակազդեցության համապատասխան տեղեկատվական ենթակառուցվածք, ինչպես նաև համակարգչային պատահարներին արձագանքման թիմեր (CERT): Կիբեռանվտանգության ապահովման գործում և կիբեռանվտանգության կայացածության մակարդակով տարածաշրջանի երկրների ցանկում Հայաստանն զբաղեցնում է վերջին տեղը՝ զգալիորեն զիջելով հարևան Ադրբեջանին և Վրաստանին:

Թեմայի ուսումնասիրությանը նվիրված են բազմաթիվ գիտական աշխատանքներ, որոնցում լուսաբանվում են ՀՀ տեղեկատվական անվտանգության սպառնալիքները, փոխգործակցության զարգացման տեսական և գործնական դինամիկայի ուսումնասիրման հարցերը, սակայն դրանցում հիմնականում չկան հակազդեցության նոր մեխանիզմները 21-րդ դարի սպառնալիքների դեմ, ինչը հնարավորություն կտա հետագայում ավելի լավ պաշտպանելու մեր երկրի տեղեկատվական անվտանգությունը, դիմակայելու համաշխարհայնացման գործընթացներից բխող վտանգներին ու սպառնալիքներին:

Այս տեսանկյունից հարկ է հստակ տարանջատել համաշխարհայնացման պայմաններում ՀՀ տեղեկատվական անվտանգության ներքին ու արտաքին սպառնալիքները, ակտիվորեն ընդլայնել ոլորտում միջազգային համագործակցությունը ինչպես երկկողմ, այնպես էլ բազմակողմ մասշտաբով:

Սույն աշխատանքն անդրադառնում է 21-րդ դարի սպառնալիքներին հակազդելու նոր մեխանիզմների մշակմանը: Ավելին, ուսումնասիրելով տեղեկատվական անվտանգության ապահովման արտասահմանյան երկրների փորձը (ԱՄՆ-ն՝ որպես տեղեկատվական անվտանգության քաղաքականության մշակման առաջին երկիր, ՌԴ-ն՝ որպես հետխորհրդային երկիր, ՉԺՀ-ն՝ որպես արևելյան արժեքներ կրող ավանդական պետություն)՝ աշխատանքում վերհանվում են ՀՀ-ում դրա կիրառման հնարավորությունները:

Հիմնախնդրի գիտական ուսումնասիրության աստիճանը: Ատենախոսության թեմայի շրջանակում ներառվող հիմնախնդիրների ուսումնասիրութ-

յունը ոլորտի մասնագետների ուշադրության կենտրոնում է: Հետազոտության առարկային վերաբերող տեղեկատվական անվտանգության թեմայով մի շարք հայ հեղինակներ ունեն գիտական վերլուծություններ, որոնց աշխատությունների հետ միասին ատենախոսությունում քննարկվել է նաև արտասահմանյան քաղաքագետների հեղինակած մասնագիտական գրականությունը: Ուսումնասիրվել են տեղեկատվական անվտանգության և դրա ապահովման քաղաքականության տեսական ու մեթոդաբանական հիմնահարցերին, համաշխարհայնացման պայմաններում տեղեկատվական սպառնալիքներին նվիրված մի քանի տասնյակ աշխատություններ, մենագրություններ, հայ և արտասահմանյան մասնագետների գրքեր, հոդվածներ:

Հետազոտության նորմատիվաիրավական հիմքը կազմել են ՀՀ Ազգային անվտանգության ռազմավարությունը, ՀՀ Տեղեկատվական անվտանգության հայեցակարգը, ՀՀ օրենսդրական ակտերը արտաքին քաղաքականության, տարածաշրջանային անվտանգության ոլորտում, տեղեկատվական անվտանգության ոլորտին առնչվող իրավական փաստաթղթեր, միջազգային կոնվենցիաներ, որոնք կանոնակարգում են տեղեկատվական անվտանգության ապահովման քաղաքականությունը, միջազգային կազմակերպությունների, մասնավորապես՝ Հյուսիսատլանտյան պայմանագրի կազմակերպության (այսուհետ՝ ՆԱՏՕ), Միավորված ազգերի կազմակերպության (այսուհետ՝ ՄԱԿ), Հավաքական անվտանգության պայմանագրի կազմակերպության (այսուհետ՝ ՀԱՊԿ), Շանհայի համագործակցության կազմակերպության (այսուհետ՝ ՇՀԿ) պաշտոնական փաստաթղթեր (կանոնադրություններ, աշխատանքային ու փորձագիտական խմբերի եզրակացություններ, ռազմավարություններ, հայեցակարգեր):

Օգտագործված աշխատությունների հայ հեղինակների թվում են Հ. Քոթանջյանը[1], Գ. Հարությունյանը[2], ովքեր ուսումնասիրել են տեղեկատվական անվտանգության հետ կապված խնդիրները պետական տեղեկատվական քաղաքականության մշակման և իրականացման գործում: Տեղեկատվական

[1] Քոթանջյան Հ. Ս., Պաշտպանական կրթության բարեփոխմամբ՝ ռազմավարական փոփոխությունների կառավարումը Հայաստանում «խելացի ուժի» զարգացման տեսանկյունից: «Աշխատանքային տետրեր», 2012, հմ. 4; Գագիկ Հարությունյան, Հայկ Քոթանջյան և ուրիշներ, Ադրբեջանի հակահայկական տեղեկատվական համակարգը, «Նորավանք» գիտակրթական հիմնադրամ, Երևան 2009, էջ 22-27, Քոթանջյան Հ. Ս. Անվտանգության քաղաքագիտական պրոբլեմներ. ԽՍՀՄ վերակառուցում–Ղարաբաղ, Հայաստան, Անդրկովկաս-Աֆղանստան, ՀՀ ՊՆ Դ. Կանայանի անվան ազգային ռազմավարական հետազոտությունների ինստիտուտ, Եր., 2009; Քոթանջյան Հ. Ս., Մարտիրոսով Լ. Ա., Մարտիրոսյան Տ. Ռ., Չիլինգարյան Դ. Ս., ՀՀ պաշտպանական դոկտրինի մշակման որոշ հարցեր // ՀՀ ՊՆ Դ. Կանայանի անվան ԱՌՀԻ-ի «Հայկական բանակ» (այսուհետ՝ նաև «Հայկական բանակ») ռազմագիտական հանդես, 2007, հմ. 1 (51):

անվտանգության ուսումնասիրության եռամակարդակ հետաքրքիր մոտեցում է ցուցաբերել Ա. Աթանեսյանը[3]:

Կիբեռանվտանգության ոլորտում արժեքավոր հետազոտություններ է կատարել Ա. Գրիգորյանը[4]: Տեղեկատվական ապահովման խնդիրը իրական ժողովրդավարական պետություն կառուցելու գործում կարևորում է Վ. Սողոմոնյանը[5]: ՀՀ տեղեկատվական անվտանգության ներկա իրավիճակի, տեղեկատվական հիմնական սպառնալիքների հարցերին անդրադարձել է փորձագետ Ս. Մարտիրոսյանը[6]: ՀՀ ազգային շահերի ապահովման համատեքստում տեղեկատվական անվտանգության հիմնախնդիրներին անդրադարձել է Ռ. Էլամիրյանը[7]:

Ատենախոսության մեջ ընդգրկված առանձին խնդիրների իրենց ատենախոսական աշխատանքներում անդրադարձել են Վ. Դիլանյանը, Է. Քալանթարյանը, Հ. Հակոբյանը, այսպես՝ տեղեկատվական տեխնոլոգիաների կիրառման անհրաժեշտությունը ՀՀ պետական կառավարման արդյունավետության բարձրացման համար կարևորել է Վ. Դիլանյանը[8], ՀՀ պետական կառավարման համակարգում էլեկտրոնային կառավարման ընթացակարգի ներդրման

---

[2] Հարությունյան Գ., Տեղեկատվական անվտանգության խնդիրների շուրջ (http://www.noravank.am/arm/issues/detail.php?ELEMENT_ID=2276, վերջին մուտքը՝ 10.05.2017թ.):

[3] Աթանեսյան Ա.Վ., Սպառնալիքներ ՀՀ տեղեկատվական անվտանգությանը. եռամակարդակ վերլուծություն, «21-րդ ԴԱՐ», Երևան 2010, N6, էջ 26-34; Атанесян А. В., Актуальные проблемы современных политических и конфликтных коммуникаций, Ереван, изд-во ЕГУ, 2008, - 305с.

[4] Գրիգորյան Ա., Կիբեռանվտանգության տեղն ու դերը տեղեկատվական անվտանգության համակարգում, ՀՀ ՊՆ Դ. Կանայանի անվան ԱՌՀԻ-ի «Հայկական բանակ» ռազմագիտական հանդես, 2016, հմ. 1 (87), էջ 48-55:

[5] Согомонян В. Публичность власти: Лингвистика или политология?, «21-й век», №5, 2012, с. 105-117; Согомонян В. «Проблемы информационного обеспечения властей: концепции и процессы», дисс. … д-ра полит. наук, Ереван 2014, -225 с.

[6] Մարտիրոսյան Ս., Համացանցը Հայաստանում. 2016 թվականի ամփոփում (http://www.noravank.am/arm/articles/detail.php?ELEMENT_ID=15344&sphrase_id=58069, վերջին մուտքը՝ 10.05.2017թ.), Սամվել Մարտիրոսյան, Հայաստանի հասարակությունը և կիբեռանվտանգությունը. Իրավիճակը 2016թ. (http://noravank.am/arm/articles/security/detail.php?ELEMENT_ID=15400, վերջին մուտքը՝ 13.05.2017թ.):

[7] Эламирян Р. Проблема информационной безопасности в контексте обеспечения национальных интересов Республики Армения, автореферат дисс. на соискание уч.степени канд. полит. наук.., Ереван 2013, -30с.

[8] Դիլանյան Վ. Հայաստանի Հանրապետության պետական կառավարման համակարգի կատարելագործումը տեղեկատվական տեխնոլոգիաների կիրառմամբ, ք.գ.թ. …ատենախոսություն, Երևան, 2012, -134 էջ:

անհրաժեշտությանն անդրադարձել է Է. Քալանթարյանը[9]: ՀՀ-ում տեղեկատվական հասարակության կայացման հարցերն ուսումնասիրել է Հ. Հակոբյանը[10]:

Տեսական-հայեցակարգային առումով արժեքավոր են Մ. Մարգարյանի, Հ. Բայադյանի, Ս. Մովսիսյանի՝ հանրային կառավարման արդիականացման և տեղեկատվական տեխնոլոգիաների կարևորությանը վերաբերող աշխատությունները[11]: Սակայն, համաշխարհայնացման պայմաններում ՀՀ ներքին ու արտաքին տեղեկատվական սպառնալիքների և դրանց հակազդման մեխանիզմների համալիր հետազոտություն մինչ օրս չի արվել: Սույն աշխատանքը հենց այդ խնդրին է ուղղված:

1970-ական թվականներից սկսվել է ձևավորվել տեղեկատվական հասարակության հայեցակարգը: Դ. Բելլի[12], Մ. Կաստելսի[13], Յ. Մասուդայի[14] աշխատանքները հիմք են հանդիսացել տեղեկատվական հասարակության հայեցակարգի մշակման, դրա հիմնական բնութագրիչների նկարագրման համար: Դրանցում ուսումնասիրվել են նաև համաշխարհայնացման գործընթացի ձևավորման նախադրյալները:

Տեղեկատվական-հաղորդակցային տեխնոլոգիաների ազդեցությամբ հասարակության ու պետության կերպափոխումներին, ինչպես նաև ազգային ու միջազգային մակարդակում ընթացող քաղաքական գործընթացների վրա դրանց ազդեցությանը անդրադարձել են Ջ. Նայը[15], Ա. Թոֆլերը[16], Ֆ. Ֆուկույաման[17], Մ. Լեբեդևան[18] և ուրիշներ:

---

[9] Քալանթարյան Է., ՀՀ պետական տեղեկատվական կառավարումը, քաղ.գիտ.թեկն. …ատենախոսություն, Երևան, 2014, -166 էջ:

[10] Հակոբյան Հ. Տեղեկատվական հասարակության կայացումը Հայաստանի Հանրապետությունում, ք.գ.թ. ատենախոսություն, Երևան 2011, -164 էջ:

[11] Մարգարյան Մ., Քաղաքական արդիականացման և զարգացման հիմնահարցեր. Երևան, «Պետական ծառայություն», 2004; Մարգարյան Մ. Կառավարման համակարգը Հայաստանում. Ինստիտուցիոնալ կարգը և հիմնախնդիրները, ՌԱՀՀԿ, Եր. 2001; Բայադյան Հ. Ժամանակակից տեղեկատվական և հաղորդակցական տեխնոլոգիաների տարածումը և զարգացումը Հայաստանում, Եր. 2009; Մովսիսյան Ս. ՀՀ տեղեկատվական հակազդեցության հիմնական ուղղությունները, «Գլոբուս. Տեղեկատվական անվտանգություն», № 4, հոկտեմբեր, 2008:

[12] Bell D. The Social Framework of the Information Society / Eds. Michael L. Dertouzous, J. Moses (eds) // The Computer Age: A 20 Year View, Cambridge, MA: MIT Press, 1980. – P. 163-212; Bell D. The Third Technological Revolution and Its Possible Socioeconomic Consequences / Daniel Bell // Dissent, – 1989. – 6 (2). – P. 164-176; Bell D. The Coming of Post-Industrial Society: A Venture in Social Forecasting. / Daniel Bell. – New York: Basic Books, 1999. – 616 p.

[13] Castells M. The rise of the network society / Manuel Castells. – Malden, Mass.: Blackwell Publishers, 1996, P. 556.

[14] Masuda Y. The information Society as Post-Industial Society / Yoneji Masuda. – Washington, 1981, P. 179.

[15] Nye J. Power in the Global Information Age: From Realism to Globalization / Joseph S. Nye Jr. – Routledge, 2004. – 240 p.; Nye J. The Future of Power / Joseph S. Nye Jr. – New York: Public

Տեղեկատվական տեխնոլոգիաների արագընթաց զարգացման և տեղեկատվական տարածության համաշխարհայնացման պայմաններում տեղեկատվական ոլորտի համար նոր սպառնալիքներ ի հայտ եկան, որոնց ուսումնասիրության գործում մեծ ներդրում ունեն Ե. Կասպերսկին[19], Վ. Լոպատինը[20], Ա. Ստրելցովը[21], Կ. Ուիլսոնը[22]:

ԱՄՆ-ի տեղեկատվական անվտանգության հարցերի ուսումնասիրությամբ զբաղվել են այնպիսի հայտնի ամերիկացի փորձագետներ,ինչպիսիք են Զ. Բժեզինսկին[23], Հ. Քիսինջերը[24], Ջ. Նայը[25], Ֆ. Ֆուկույաման[26], Ս. Հանթինգտոնը[27]:

Հարկ է նշել, որ հիմնախնդրի ուսումնասիրությանը վերաբերող աշխատությունների մեծ մասում տեղեկատվական անվտանգությանը նեղ մոտեցում

Affairs, 2011., P. 298.

[16] Тоффлер Э. Третья волна / Э. Тоффлер. – М.: АСТ, 2010, с. 784.

[17] Fukuyama, Francis. The Promise and Challenge of emerging technologies [Электронный ресурс] / Information and Biological Revolutions: Global Governance Challenge // Science and Technology Policy Institute. Chapter 2. URL: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1139.pdf (վերջին մուտքը՝ 05.04.2014թ.).

[18] Лебедева М.М. Современные технологии и политическое развитие мира / М.М. Лебедева //Международная жизнь. – 2001. – № 2. – с. 45-53; Лебедева М.М. Мировая политика / М.М. Лебедева. – М.: Аспект Пресс, 2003, С. 351.

[19] Касперский Е. Компьютерное зловредство / Е. Касперский. – Спб: Питер, 2008, с. 208.

[20] Лопатин В.Н. Информационная безопасность России: Человек, общество, государство / В.Н. Лопатин. –М.: 2000, с. 428.

[21] Стрельцов А.А. Обеспечение информационной безопасности России / А.А. Стрельцов. – М.:МЦНМО, 2002, с. 296.

[22] Wilson, Clay. Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress / Congress Research Center Report. October 17, 2003. (http://fpc.state.gov/documents/organization/26009.pdf); Wilson, Clay. Botnets, Cybercrime, and Cyberterrorism:Vulnerabilities and Policy Issues for Congress / Congress Research Service Report. January 28, 2008. – URL: http://fpc.state.gov/documents/organization/102643.pdf (վերջին մուտքը՝05.04.14թ).

[23] Бжезинский З. Великая шахматная доска / Зб. Бжезинский, пер. О.Ю. Уральской. – М.: Международные отношения, 1998. – 256 с.; Бжезинский Зб. Выбор. Мировое господство или глобальное лидерство / Зб. Бжезинский. – М.: Международные отношения, 2004. – 287 с.; Бжезинский Зб. Ещё один шанс. Три президента и кризис американской сверхдержавы / Зб. Бжезинский. – М: Международные отношения,2010.– 190 с.

[24] Киссинджер Г. Дипломатия. / пер. с англ. В.В. Львова. – М.: Ладомир, 1997. – 848 с.; Kissinger H. Does America Need a Foreign Policy?: Toward a Diplomacy for the 21st Century / Henry A. Kissinger. – New York: Simon & Schuster, 2001. – 238 p.

[25] Nye J. The Future of American Power: Dominance and Decline in Perspective / Joseph S. Nye, Jr. // Foreign Affairs. Nov. / Dec. 2010. V. 89. #6. – P. 2-12.

[26] Fukuyama Fr. America at the Crossroads: Democracy, Power, and the Neoconservative Legacy / Francis Fukuyama. – Yale University Press, 2006. – 226 p.

[27] Huntington S. The Lonely Superpower / Foreign Affairs. – March/April 1999. – Vol.78. № 2. – pp. 35-49.

է ցուցաբերվում, մենք ընդունելի ենք համարում այն մոտեցումը, որն ընդգծում է անհատի, հասարակության, պետության եռամիասնական մոտեցումը:

Հետազոտության աղբյուրները հետևյալն են.

- Առաջին խումբ աղբյուրները ՀՀ-ի, ՌԴ-ի, ԱՄՆ-ի պետական պաշտոնական փաստաթղթերն են, մասնավորապես՝ հայեցակարգերը, օրենսդրական ակտերը,
- Երկրորդը հայ և արտասահմանյան գիտական գրականությունն է,
- Երրորդը հայ և արտասահմանյան մամուլի հրապարակումներն են,
- Չորրորդը միջազգային կազմակերպությունների, մասնավորապես՝ ՄԱԿ-ի, ՀԱՊԿ-ի, ՆԱՏՕ-ի, ՇՀԿ-ի պաշտոնական փաստաթղթերն են,
- Հինգերորդը պետական ու ոչ պետական մի շարք կազմակերպությունների պաշտոնական կայքերը:

Հետազոտության օբյեկտն է Հայաստանի Հանրապետության տեղեկատվական անվտանգության համակարգը:

Հետազոտության առարկան համաշխարհայնացման գործընթացներից բխող ՀՀ տեղեկատվական անվտանգության սպառնալիքների և դրանց հակազդման մեխանիզմների, տեղեկատվական անվտանգության ապահովման կառուցակարգերի և դրանց կատարելագործման հեռանկարների փոխկապված հիմնախնդիրների ամբողջությունն է:

Հետազոտության նպատակն է համապարփակ և հետևողական վերլուծության ենթարկել Հայաստանի Հանրապետության տեղեկատվական անվտանգության համակարգը, մատնանշել համաշխարհայնացման պայմաններում ՀՀ տեղեկատվական անվտանգության հիմնախնդիրները: Սա կանխորոշում է գիտականորեն հիմնավորված համակարգի մշակման անհրաժեշտությունը, համաշխարհայնացման պայմաններում տեղեկատվական սպառնալիքների համատեքստում տեղեկատվական անվտանգության վիճակի և հեռանկարների գնահատումը, համապատասխան միջոցառումների մշակումը՝ ազգային արժեքներին, շահերին, նպատակներին սպառնացող իրական և հնարավոր վտանգներին հակազդելու համար:

Վերոնշյալ նպատակին հասնելու համար հետազոտության ընթացքում առաջադրվել են հետևյալ **խնդիրները.**

- Ընդհանրացնել քաղաքագիտական գրականության մեջ, ինչպես նաև տարբեր երկրների՝ ոլորտին առնչվող հայեցակարգային փաստաթղթերում տեղեկատվական անվտանգության սահմանման տարբեր տեսակետները և մոտեցումները,
- Վերլուծել տեղեկատվական անվտանգության տեսական հիմքերն ու ապահովման առանձնահատկությունները համաշխարհայնացման պայմաններում,
- Բացահայտել թվային դիվանագիտության ծրագրերի դերը տեղեկատվական անվտանգության քաղաքականության իրականացման ժամանակ,

- Վերլուծել տեղեկատվական անվտանգության ապահովման արտասահմանյան փորձը՝ ԱՄՆ-ի, ՌԴ-ի, ՉԺՀ-ի օրինակով, բացահայտել ՀՀ-ում դրա կիրառման հնարավորությունները,
- Բացահայտել համաշխարհայնացման պայմաններում ՀՀ տեղեկատվական անվտանգության ներքին ու արտաքին սպառնալիքները, սահմանել դրանց հակազդման հիմնական ուղղությունները, մեթոդները և տալ գործնական առաջարկներ,
- Տեղեկատվական անվտանգության իրավական հիմքերի բացահայտման նպատակով համակարգային վերլուծության ենթարկել ՀՀ տեղեկատվական անվտանգության հայեցակարգն ու արժևորել փոփոխությունների անհրաժեշտությունը,
- Հետազոտել ՀՀ տեղեկատվական անվտանգության ապահովման տեսանկյունից միջազգային համագործակցության ընդլայնման հեռանկարները,
- Վերլուծել և գնահատել ՀՀ պետական տեղեկատվական քաղաքականության հիմնական ուղղություններն ու զարգացման հեռանկարները:

Հետազոտության շրջանը ընդգրկում է Հայաստանի երրորդ Հանրապետության ժամանակաշրջանը (1990-ական թվականների սկզբներից մինչև մեր օրերը):

Հետազոտության ընդհանուր մեթոդաբանությունը և եղանակները: Հետազոտության ընթացքում օգտագործվել են բովանդակային և դիսկուրս վերլուծության, գործընթացային հետազոտության մեթոդները, համակարգա-կառուցվածքային մոտեցումը: Համագիտական մեթոդներից՝ դիալեկտիկական, համակարգային, նկարագրական, համեմատական մեթոդները, ինչպես նաև ընդհանուր գիտական մեթոդներ՝ անալիզ, սինթեզ, դեդուկցիա: Հետազոտության ընթացքում կիրառվել են նաև քննարկվող ոլորտի վերաբերյալ քաղաքագիտության հայտնի մասնագետների բազմաթիվ աշխատություններ, շատ դեպքերում համադրվել են մասնագիտական գրականության մեջ առկա դիրքորոշումները, որոնց հիման վրա էլ արվել են սեփական եզրահանգումները:

Ատենախոսության գիտական նորույթը: Հետազոտության գիտական նորույթը համաշխարհայնացման պայմաններում հիմնախնդրի լուծման տեսական և մեթոդաբանական հիմքերի մշակումն է՝ հաշվի առնելով ՀՀ տեղեկատվական անվտանգության սպառնալիքները:

Ատենախոսական աշխատանքում ստացվել են գիտական նորույթ պարունակող հետևյալ արդյունքները՝

1. Մշակվել են համաշխարհայնացման պայմաններում տեղեկատվական անվտանգության ապահովման, սպառնալիքների հակազդման մեխանիզմների տեսական հայեցակարգային հիմքերը՝ հաշվի առնելով ՀՀ տեղեկատվական անվտանգության համակարգի առանձնահատկությունները:

2. Տեղեկատվական անվտանգության ապահովման պաշտպանողական և հարձակողական չափումների համադրմամբ մշակվել են տեղեկատվական օպերացիաների իրականացման մի շարք եղանակներ:
3. Հետազոտության արդյունքների հիման վրա հիմնավորվել է Հայաստանի տեղեկատվական անվտանգությունը Արցախի տեղեկատվական անվտանգության հետ միասնության մեջ դիտարկելը: Ընդգծվել է Արցախի տեղեկատվական անվտանգության հայեցակարգի մշակման անհրաժեշտությունը, որը համահունչ կլինի ՀՀ համապատասխան հայեցակարգին:
4. Միջազգային առաջատար փորձի ուսումնասիրության հիման վրա առաջարկվել է տեղեկատվական անվտանգության ապահովման բնագավառում տեղեկատվական վտանգներին և համակարգչային պատահարներին արագ արձագանքման խմբերի ստեղծման գերատեսչական մոդել:
5. Բացահայտվել են համաշխարհայնացման պայմաններում ՀՀ տեղեկատվական անվտանգության դեմ ուղղված սպառնալիքների աճը պայմանավորող ներքին և արտաքին հիմնական գործոնները, առաջարկվել են դրանց կանխարգելման միջոցներն ու եղանակները: Այս համատեքստում ընդգծվել են թվային դիվանագիտության ընձեռած հնարավորությունները, արժևորվել է դրա գործիքարանի արդյունավետ կիրառումը:

Հետազոտության գիտական նորույթը պայմանավորված է նաև նրանով, որ ատենախոսության շրջանակում տեղեկատվական անվտանգության հարցերը վերլուծվում են որպես ՀՀ հանրային անվտանգության մաս՝ անհատ-հասարակություն-պետություն եռամիասնության մեջ:

Հետազոտության **տեսական և գործնական նշանակությունը** կայանում է նրանում, որ աշխատանքի հիմնական դրույթները կարող են կիրառվել ԲՈՒՀ-երի գիտակրթական գործունեությունում, ինչպես նաև պետական և գիտահետազոտական հաստատությունների հետազոտական աշխատանքներում: Հետազոտության հիմնական արդյունքները կարող են օգտագործվել Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգային հետագա մշակումների համար: Բացի այդ, ստացված արդյունքները թույլ են տալիս ավելի լավ ընկալել միջազգային հարաբերություններում ՀՀ հիմնական խնդիրները՝ կապված տեղեկատվական անվտանգության ապահովման հետ, ինչը թույլ կտա ՀՀ տեղեկատվական անվտանգության հայեցակարգը վերանայելիս հաշվի առնել դրական և բացասական միտումները:

Աշխատանքի փորձաքննությունը: Ատենախոսության հիմնական դրույթները քննարկվել և հրապարակային պաշտպանության են երաշխավորվել Երևանի պետական համալսարանի Միջազգային հարաբերությունների ֆակուլտետի Քաղաքական ինստիտուտների և գործընթացների 2017թ.-ի

դեկտեմբերի 4-ի նիստում: Հետազոտության առանցքային գաղափարներն ու դրույթներն արտացոլված են գրախոսվող պարբերական գիտական հրատարակություններում հրապարակված հեղինակի գիտական հոդվածներում, որոնք հրապարակվել են 2013-2017 թթ-ների ընթացքում: Ատենախոսության որոշակի դրույթներ նաև ներառվել են 2016 թ.-ի սեպտեմբեր ամսին Էստոնիայի Տալլինի համալսարանում կազմակերպված «VII International Concept mapping» միջազգային գիտաժողովի ընթացքում: Ատենախոսության առանցքային գաղափարները ներառված են ԵՊՀ Միջազգային հարաբերությունների ֆակուլտետի Քաղաքագիտության բակալավրիատի «Քաղաքականություն և կառավարում», Հանրային կառավարման բակալավրիատի «Ժողովրդավարական կառավարման տեսություն և արդիականություն» դասընթացների ուսումնական ծրագրում:

Աշխատանքի ծավալն ու կառուցվածքը: Ատենախոսությունը շարադրված է 155 մեքենագիր էջի վրա և բաղկացած է ներածությունից, երեք գլուխներից (ութ ենթագլուխներով), եզրակացություններից, օգտագործված գրականության ցանկից: Աշխատանքում բերված են 2 գծապատկեր, 164 անուն գրականության ցանկ:

ԱՏԵՆԱԽՈՍՈՒԹՅԱՆ ՀԱՄԱՌՈՏ ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆԸ

Ներածության մեջ հիմնավորվում է ատենախոսության թեմայի արդիականությունը, սահմանվում են հետազոտության նպատակներն ու խնդիրները, ուսումնասիրության օբյեկտն ու առարկան, հիմնախնդրի գիտական ուսումնասիրության աստիճանը, հետազոտության մեթոդաբանական հիմքը, ինչպես նաև ատենախոսության գիտական նորույթն ու առաջարկվող հիմնադրույթների կիրառման հնարավոր ուղղությունները:

Ատենախոսության **«Տեղեկատվական անվտանգության հիմնախնդիրները համաշխարհայնացման պայմաններում»** խորագրով երեք ենթագլուխներից բաղկացած առաջին գլխում վերլուծվում են տեղեկատվական անվտանգության էվոլյուցիան, համաշխարհայնացման պայմաններում տեղեկատվական սպառնալիքների առաջացման առանձնահատկությունները, տեղեկատվական անվտանգության քաղաքականության համատեքստում թվային դիվանագիտության դերը:

Առաջին՝ **«««Տեղեկատվական անվտանգություն» հասկացության սահմանման հիմնախնդիրները և էվոլյուցիան»** ենթագլխում ներկայացվում են տեղեկատվական անվտանգության հասկացության տարբեր մոտեցումները անգլալեզու, ռուսերեն ու հայերեն գրականության մեջ, ինչպես նաև հայեցակարգային փաստաթղթերում: Հիմնավորվում է հասկացության այնպիսի սահմանման անհրաժեշտությունը, որը կընդգրկի դրա ընկալման և՛

լայն, և՛ նեղ մոտեցումները: Ցույց է տրվում, թե ինչպես էր ի սկզբանե «տեղեկատվական անվտանգություն» հասկացությունը օգտագործվում տեղեկատվական-հաղորդակցային տեխնոլոգիաների զարգացման համատեքստում՝ համակարգչային ցանցերի միջոցով ծագած խնդիրների վերհանման նպատակով, իսկ հետագայում ավելի ընդգրկուն դառնում՝ դուրս գալով բացառապես տեխնոլոգիական բնագավառին առնչվող շրջանակներից: Կարևորվում է տեղեկատվական անվտանգությունը հանրային անվտանգության ապահովման համատեքստում դիտարկելը: Այս տեսանկյունից անհրաժեշտ է տեղեկատվական ներքին ու արտաքին սպառնալիքներից հանրության բարոյահոգեբանական անվտանգության ապահովումը:

Երկրորդ՝ **«Տեղեկատվական սպառնալիքների առաջացման առանձնահատկություններն ու դրսևորումները համաշխարհայնացման համատեքստում»** ենթագլխում ներկայացվում և վեր են լուծվում համաշխարհայնացման պայմաններում տեղեկատվական հիմնական սպառնալիքները, որոնք իրական վտանգ են պարունակում անհատի, հասարակության ու պետության կենսական կարևոր շահերի համար: Հիմնավորվում է, որ նոր քաղաքական հակամարտությունների կանխարգելման համար յուրաքանչյուր պետության գործունեության կարևոր ուղղություններից մեկը պետք է դառնա տեղեկատվական անվտանգության ապահովումը: Բացի այդ, պետությունների համար կարևոր է նաև գլոբալ սպառնալիքներին հակազդելու համար համապատասխան ռազմավարության մշակումը: Այս շրջանակում որոշ պետություններ ավելի լիբերալ մեթոդներ են որդեգրում, իսկ մյուսները՝ հակառակը՝ հնարավորինս ուժեղ վերահսկում են տեղեկատվական տարածությունը: Կարևորվում է ոչ միայն ազգային, այլև միջազգային տեղեկատվական անվտանգության ապահովումը, քանզի տեղեկատվական տեխնոլոգիաների միջոցով իրականացվող հանցագործություններն ունեն անդրազգային բնույթ, իսկ առանձին պետությունների համար գրեթե անհնարին է դրանք հաղթահարել: Առաջնային է համարվում նաև սպառնալիք, վտանգ, ռիսկ հասկացությունների հստակ տարանջատումը: Ի տարբերություն առաջինների, վերջինն առավել կառավարելի է, ուստի կարևորվում է տեղեկատվական ռիսկերի գնահատման և կառավարման մեխանիզմի ներդնումը:

Երրորդ՝ **«Թվային դիվանագիտության ծրագրերը տեղեկատվական անվտանգության քաղաքականության համատեքստում»** ենթագլխում ներկայացվում են թվային դիվանագիտության առանձնահատկությունները գերտերությունների և փոքր պետությունների համար: Առաջին դեպքում այն ունի հարձակողական գործառույթներ, ընդհանուր արտաքին քաղաքականության գործիքարանի տեղեկատվական բաղադրիչն է՝ ուղղված սեփական գործունեության համար դրական տեղեկատվական դաշտի ստեղծմանը: Այնինչ սահմանափակ ռեսուրսներ ունեցող փոքր պետությունների համար այն ավելի շատ պաշտպանական և տեղեկատվական

ավտանգության սպառնալիքներին հակադարձելու նկատառումներով է կարևորվում, քանզի թվային ազդեցիկ և թիրախավորված դիվանագիտության մշակումն ու իրականացումը խիստ ռեսուրսատար է: Հիմնավորվում է արդի մարտահրավերների պայմաններում Հայաստանի արդյունավետ զարգացման համար թվային բնագավառում նոր արտաքին քաղաքական նախագծերի անհրաժեշտությունը՝ ուղղված փափուկ ուժի ամրապնդմանը և գիտության, տեխնոլոգիաների ու կրթության զարգացմանը: Նման պայմաններում թվային դիվանագիտությունը կարող է դառնալ համաշխարհային թատերաբեմում ազգային շահերի առաջքաշման միջոց, եթե մտավոր, տեխնոլոգիական ու կազմակերպչական բավարար ռեսուրսներ ներդրվեն: Կարևորվում է թվային դիվանագիտության ոլորտում արտասահմանյան երկրների հաջող փորձը Հայաստանում կիրառելը, այդ թվում՝ վիրտուալ դաշտում պետական գերատեսչությունների գործունեության ակտիվացումը, օտար լեզուներով բլոգների, կայքերի թվի մեծացումը, թվային դիվանագիտության սեփական համակարգի մշակումը:

Երկրորդ՝ **«ՀՀ-ում տեղեկատվական անվտանգության ապահովման միջազգային փորձի կիրառման հնարավորությունները»** գլխում ներկայացվում են ԱՄՆ-ի՝ որպես տեղեկատվական հեղաշրջման ազդեցությունն իր վրա առաջինը կրած և անվտանգության քաղաքականության մշակման առաջին երկրներից մեկի, ՌԴ-ի՝ որպես հետխորհրդային տարածաշրջանի երկրի, ՉԺՀ-ի՝ որպես արևելյան արժեքներ կրող ավանդական պետության, տեղեկատվական անվտանգության ապահովման ուղղությամբ կատարված աշխատանքները, վերլուծվում են ոլորտին առնչվող հայեցակարգային փաստաթղթերը, տեղեկատվական անվտանգության ապահովման մեխանիզմները, ՀՀ-ում դրանց կիրառման հնարավորությունները:

Առաջին՝ **«Տեղեկատվական անվտանգության ապահովման ԱՄՆ փորձի, հայեցակարգային մոտեցումների և կարգավորման մեխանիզմների կիրառման նշանակությունը ՀՀ-ում»** ենթագլխում հիմնավորվում է, որ ԱՄՆ տեղեկատվական անվտանգության քաղաքականության էվոլյուցիան համաշխարհային զարգացումների պրոյեկցիան էր. Այդտեղ տեղեկատվական անվտանգության խնդիրները ի սկզբանե տեխնիկական՝ համակարգչային տվյալների պաշտպանությունից, սկսեցին դիտվել որպես կրիտիկական, իսկ տեղեկատվական քաղաքականությունը դարձավ արտաքին և անվտանգության քաղաքականության անքակտելի բաղադրիչ: Որպես տեղեկատվական անվտանգության ապահովման կարևոր միջոցառումներ, առանձնացվում են՝

- Պետական մարմինների ու մասնավոր սեկտորի փոխգործունեության ընդլայնումը,
- Կիբեռանվտանգության հետ կապված հարցերի մասին տեղեկացվածության բարձրացումը,
- Ոլորտում որակյալ կադրերի պատրաստումը,

- Միջազգային համագործակցության ընդլայնումը:

Կարևորվում է տեղեկատվական անվտանգության կառուցակարգերի մշակման և անհրաժեշտ գործիքարանի հստակեցման հարցում ԱՄՆ օրինակի ուսուցողական լինելը:

Երկրորդ՝ **«Տեղեկատվական անվտանգության ապահովման ՌԴ փորձի նշանակությունը ՀՀ-ում»** ենթագլխում վերլուծվում է ՌԴ նորմատիվային բազան, ինչի արդյունքում կատարվում է եզրակացություն առ այն, որ, ի տարբերություն ԱՄՆ-ի, այն հիմնականում ունի պաշտպանողական բնույթ և ուղղված է ռազմավարական կայունությանը, իրավահավասար ռազմավարական գործընկերությանը և տեղեկատվական ինքնիշխանության պաշտպանությանը: Մինչդեռ ԱՄՆ-ի՝ նույն ոլորտի փաստաթղթերում նկատվում է երկրի ձգտումը՝ տեղեկատվական գերակայություն հաստատելու համաշխարհային մակարդակում: Ինչ վերաբերվում է ոլորտում միջազգային համագործակցությանը, ապա ՌԴ-ն նույնպես հիմնահարցի արդյունավետ լուծման համար կարևորում է համագործակցության ընդլայնումը: Սակայն եթե ԱՄՆ-ի համար որպես հիմնական հարթակ ՆԱՏՕ-ն է, որտեղ ինքը թելադրող դիրք ունի, ապա ՌԴ-ն ակտիվորեն գործում է ՀԱՊԿ-ի և ՇՀԿ-ի շրջանակներում: Հիմնավորվում է, որ բացի երկկողմ, ՄԱԿ-ի մակարդակով և տարածաշրջանային կազմակերպությունների մասշտաբով համագործակցություններից, ՌԴ-ի համար արդյունավետ կարող է լինել նաև պետական մասնավոր ընկերությունների հետ համագործակցությունը (ինտերնետ ծառայություն տրամադրողներ, ծրագրային ապահովումը մշակողներ, համակարգչային տեխնիկա արտադրողներ), ինչպես նաև այնպիսի նորմատիվային փաստաթղթերի մշակումը, որոնք ոչ միայն կլինեն պաշտպանողական բնույթի, այլև հնարավորություն կտան Ռուսաստանին հարձակողական միջոցներով ոլորտում գերակա դիրք զբաղեցնել:

Երրորդ՝ **«Տեղեկատվական անվտանգության ապահովման մեխանիզմների ՉԺՀ փորձի կիրառական նշանակությունը ՀՀ-ում»** ենթագլխում վերլուծվում է տեղեկատվական անվտանգության ապահովման ՉԺՀ փորձը, որի արդյունքում եզրակացություն է արվում առ այն, որ Չինաստանն ավելի գործնական քայլերի է դիմում՝ համապատասխան գործակալություններ բացելով, տեղեկատվական հարձակողական օպերացիաներ իրականացնելով: Բացի այդ, Չինաստանում համացանցը խիստ վերահսկվում և ուղղորդվում է պետության կողմից: Դա մի կողմից հնարավորություն է տալիս երկրի իշխանություններին առանց մեծ ծախսերի ձևավորելու Չինաստանի դրական կերպարը, մյուս կողմից՝ արգելելու անցանկալի տեղեկատվության տարածումը երկրի ներսում: Այդ է վկայում այն հանգամանքը, որ ոլորտում աննախադեպ՝ Կիբեռանվտանգության մասին օրենքը, ՉԺՀ-ում միայն 2017թ-ին է ուժի մեջ մտել, թեպետ, իհարկե, երկրում հիմնահարցի հետ կապված տարբեր հայեցակարգեր ևս մինչ այդ մշակված են եղել:

Ատենախոսության երրորդ՝ **«Հայաստանի Հանրապետության տեղեկատվական անվտանգության ներկա իրավիճակն ու դրա ապահովման ուղիները»,** խորագրով գլխում ներկայացվում են ՀՀ տեղեկատվական անվտանգության ներքին ու արտաքին սպառնալիքները, առաջարկվում դրանց կանխարգելման միջոցառումները, ներկայացվում են նաև ՀՀ պետական տեղեկատվական քաղաքականության հիմնական ուղղությունները, առաջարկվում կատարելագործման ուղիները:

Առաջին ենթագլխում՝ **«ՀՀ տեղեկատվական անվտանգության ներքին ու արտաքին սպառնալիքները»**, ներկայացվում է ՀՀ-ում կիբեռհանցագործությունների աճի վիճակագրությունը, կանխարգելիչ միջոցառումների իրականացման անհրաժեշտությունը: Վերլուծվում են ՀՀ տեղեկատվական անվտանգության ներքին ու արտաքին սպառնալիքների հիմնական աղբյուրները, հիմնավորվում է այնպիսի մեթոդների ու միջոցների մշակման անհրաժեշտությունը, որոնք կօգնեն դիմակայելու այդ սպառնալիքներին, մասնավորպես՝ արտաքին սպառնալիքներին դիմակայելու համար որպես նման միջոցառումներ կարող են լինել թվային դիվանագիտության գործիքարանի լայնորեն կիրառումը, որը հնարավորություն կտա համաշխարհային քաղաքական թատերաբեմում ՀՀ հեղինակության բարձրացման ու պետության համար շահեկան քաղաքական իմիջի ձևավորման ու առհասարակ երկրի տեղեկատվական անվտանգության ապահովման համար, ֆինանսական աջակցության ավելացումը տեղեկատվական անվտանգության ապահովման կոնկրետ ուղղությունների, մասնավորապես՝ թվային դիվանագիտության համար, հայկական քարոզչական և հակաքարոզչական կենտրոնների աշխատանքները համակարգող կառույցի ձևավորումը: Ներքին սպառնալիքներին դիմակայելու համար կարևորվում է այնպիսի միջոցառումների իրականացումը, ինչպիսիք են տեղեկատվական անվտանգության ապահովման նպատակով ՀՀ պետական իշխանության մարմինների գործողությունների համակարգումն ու կանոնակարգումը, տարաբնույթ ապակառուցողական օտարերկրյա տեղեկատվական հոսքերից ՀՀ տեղեկատվական ներքին ռեսուրսների անվտանգության ապահովումը սեփական արտադրանքի որակի բարձրացմամբ, թվային դիվանագիտության ծրագրերի կատարելագործմամբ, ՀՀ պետական լեզվի դերի բարձրացումը:

Երկրորդ՝ «**ՀՀ պետական տեղեկատվական քաղաքականության հիմնական ուղղությունները և կատարելագործման հեռանկարները**» ենթագլխում հիմնավորվում է Հայաստանի Հանրապետության տեղեկատվական անվտանգության ապահովման համար համապատասխան քաղաքականության մշակման անհրաժեշտությունը և առաջնային կարևորվում տեղեկատվական անվտանգության ժամանակակից պահանջներին համապատասխան Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգի լրամշակումը, այնպիսի փաստաթղթի մշակման անհրաժեշտությունը,

որը հայեցակարգային հիմքեր կստեղծի ՀՀ տեղեկատվական անվտանգության կոշտ և փափուկ, հարձակվողական և պաշտպանողական չափումների ամրապնդման համար, ՀՀ տեղեկատվական անվտանգությունը Արցախի տեղեկատվական անվտանգության հետ միասնության մեջ դիտարկելը, համայն հայության տեղեկատվական ինտեգրման նպատակով համապատասխան քաղաքականության իրականացումը, հեռուստաընկերություններով այնպիսի հաղորդաշարների պատրաստումը, որոնք կբարձրացնեն տեղեկատվական սպառնալիքների հետ կապված հասարակության իրազեկվածության աստիճանը, դպրոցներում տեղեկատվական անվտանգության հարցերին վերաբերող դասընթացների կազմակերպում, որը հնարավորություն կտա առավել վաղ տարիքից ծանոթանալու ոլորտին վերաբերող հիմնախնդիրներին և խուսափել տեղեկատվական տարածությունից բխող սպառնալիքներից, տեղեկատվական անվտանգության ապահովման ոլորտում միջազգային համագործակցության ընդլայնումը, փորձի փոխանակումը ոլորտի առաջատար մասնագետների հետ:

«Եզրակացություններ» մասում ամփոփված են հետազոտության հիմնական եզրակացությունները և ՀՀ տեղեկատվական անվտանգության ապահովման արդյունավետության բարձրացմանն ուղղված առաջարկությունները: Ատենախոսության շրջանակներում ներկայացված եզրակացություններից և առաջարկություններից հարկ ենք համարել առանձնացնել հետևյալները.

1. Որպես գլոբալացման արդյունք՝ ի հայտ են գալիս տեղեկատվական սպառնալիքների նոր ձևեր, ինչպիսիք են կիբեռհանցագործությունները, կիբեռահաբեկչությունը, տեղեկատվական պատերազմները, որոնք նորովի են վերաիմաստավորում անվտանգության քաղաքականությունն իր բոլոր դրսևորումներով:
2. Տեղեկատվական համակարտությունը դարձել է կարևորագույն աշխարհաքաղաքական գործոններից մեկը, որը կանխորոշում է երկրների ճակատագիրը: Նման պայմաններում չափազանց կարևոր է տեղեկատվական ոլորտում ազգային շահերի ապահովման պետական միասնական քաղաքականության ձևավորումը, գործող օրենսդրության կատարելագործումը, հայկական քարոզչական և հակաքարոզչական կառույցների աշխատանքները համակարգող կառույցի ստեղծումը, պետական իշխանության մարմինների գործունեության համակարգումը, պետական իշխանության մարմինների ու ոլորտի հիմնահարցերով զբաղվող գիտական հաստատությունների միջև համագործակցության ընդլայնումը:
3. Նոր մարտահրավերների պայմաններում թվային դիվանագիտությունը կարող է դառնալ համաշխարհային թատերաբեմում ազգային շահերի առաջքաշման միջոց: Այդ իսկ պատճառով

պետական մարմինների ջանքերի ակտիվացումն այդ բնագավառում պետք է ամենամոտ ապագայում դիտվի առաջնային:

4. Որպես գլոբալացման անխուսափելի հետևանք՝ համաշխարհային հանցագործությունների ժամանակակից ձևերը, որոնք իրականացվում են հաղորդակցային տեխնոլոգիաների միջոցով, տարածվում են բոլոր երկրների վրա, ինչի հետևանքով, հանցագործություններն այժմ ունեն անդրազգային բնույթ, իսկ առանձին պետությունների համար գրեթե անհնարին է հաղթահարել դրանք առանձին: Ուստի խնդրի լուծման համար Հայաստանին անհրաժեշտ է միջազգային համագործակցության ընդլայնում:
5. Տեղեկատվական անվտանգության ապահովման ամերիկյան փորձը ցույց է տալիս, որ ԱՄՆ տեղեկատվական անվտանգության և քաղաքականության էվոլյուցիան համաշխարհային զարգացումների հետևանք էր. այդտեղ տեղեկատվական անվտանգության խնդիրները ի սկզբանե տեխնիկական՝ համակարգչային տվյալների պաշտպանությունից, սկսեցին դիտվել որպես կրիտիկական, իսկ տեղեկատվական քաղաքականությունը դարձավ արտաքին և անվտանգության քաղաքականության անքակտելի բաղադրիչ: ԱՄՆ օրինակը խոսուն է և ուսուցողական տեղեկատվական անվտանգության կառուցակարգերի մշակման և անհրաժեշտ գործիքարանի հստակեցման հարցում: ԱՄՆ-ի կողմից կիրառվող թվային դիվանագիտության մեխանիզմները կարելի է լայնորեն կիրառել նաև Հայաստանում:
6. Ռուսաստանի փորձը կարող է կիրառելի լինել Հայաստանի՝ տեղեկատվական անվտանգության ոլորտին առնչվող նորմատիվային բազայի լրամշակման տեսանկյունից: Այդ առումով արդիական է հատկապես տեղեկատվական անվտանգության հայեցակարգի լրամշակումը, տեղեկատվական ենթակառուցվածքը երկրի կրիտիկական, այսինքն կենսական կարևոր ոլորտների շարքին դասելը:
7. Տեղեկատվական անվտանգության ապահովման ՉԺՀ փորձից ելնելով՝ բացի պաշտպանական միջոցառումներից անհրաժեշտ է դիմել գործնական քայլերի, հատուկ մասնագետներ պատրաստել, ովքեր կարող են իրականացնել տեղեկատվական պատերազմներ կամ կիրառել թվային դիվանագիտության ընձեռած հնարավորությունները՝ երկրի դրական կերպար ստեղծելու և հակահայկական քարոզչությանը հակազդելու համար:

Վերոնշյալ եզրահանգումները հնարավորություն են տվել հեղինակին կատարելու հետևյալ առաջարկությունները.

1. Արդի մարտահրավերների պայմաններում Հայաստանի արդյունավետ զարգացման համար անհրաժեշտ են թվային բնագավառում նոր արտաքին քաղաքական նախագծեր՝ ուղղված փափուկ ուժի ամրապնդմանը և գիտության, տեխնոլոգիաների ու կրթության

զարգացմանը: Նման պայմաններում թվային դիվանագիտությունը կարող է դառնալ համաշխարհային թատերաբեմում ազգային շահերի առաջքաշման միջոց, եթե մտավոր, տեխնոլոգիական ու կազմակերպչական բավարար ռեսուրսներ ներդրվեն: Այդ իսկ պատճառով պետական մարմինների ջանքերի ակտիվացումն այդ բնագավառում պետք է ամենամոտ ապագայում դիտվի առաջնային:

2. Արտաքին տեղեկատվական սպառնալիքներին դիմակայելու համար կարևոր է այնպիսի միջոցառումների իրականացումը, ինչպիսիք են՝
   - տեղեկատվական անվտանգության ապահովման ժամանակ միջազգային համագործակցության ընդլայնումը,
   - ոլորտի առաջատար պետությունների համապատասխան մասնագետների հետ փորձի փոխանակումը,
   - թվային դիվանագիտության ընձեռած հնարավորությունները կիրառելով համաշխարհային քաղաքական թատերաբեմում ՀՀ հեղինակության բարձրացումն ու պետության համար շահեկան քաղաքական իմիջի ձևավորումը,
   - արտերկրում հայկական ներկայացուցչությունների ու կազմակերպությունների համար ապատեղեկատվության տարածումը կանխարգելելու նպատակով անհրաժեշտ պայմանների ստեղծումը,
   - ֆինանսական աջակցության ավելացումը տեղեկատվական անվտանգության ապահովման ուղղությամբ,
   - հայկական քարոզչական և հակաքարոզչական կառույցների աշխատանքները համակարգող կազմակերպության ստեղծումը:

Ներքին սպառնալիքներին դիմակայելու համար կարևոր միջոցառումներից են՝

- ՀՀ պետական իշխանության մարմինների գործողությունների համակարգումը և կանոնակարգումը,
- ՀՀ տեղեկատվական կառույցների կատարելագործումը,
- Տեղեկատվական նոր տեխնոլոգիաների զարգացումը և դրանց՝ ժամանակակից գլոբալ տեղեկատվական կառույցների պահանջներին համապատասխան լայն տարածումը,
- ՀՀ-ում տեղական հեռահաղորդակցության և տեղեկատվական միջոցների զարգացումը և ներքին շուկայում արտասահմանյան արտադրանքի նկատմամբ դրանց առաջնայնության հաստատումը,
- Տարաբնույթ ապակառուցողական օտարերկրյա տեղեկատվական հոսքերից ՀՀ տեղեկատվական ներքին ռեսուրսների անվտանգության ապահովումը սեփական արտադրանքի որակի բարձրացմամբ, թվային դիվանագիտության կատարելագործմամբ,

- ՀՀ պետական լեզվի դերի բարձրացումը:

3. ԱՄՆ-ի. ՌԴ-ի, ՉԺՀ-ի փորձի ուսումնասիրությունը տեղեկատվական անվտանգության ապահովման նպատակով կիրառել ՀՀ-ում, մասնավորապես՝ տեղեկատվական անվտանգությունը դասել երկրի կրիտիկական ենթակառուցվածքների շարքին, կատարելագործել ոլորտի նորմատիվային բազան, դիմել գործնական քայլերի՝ բացի պաշտպանությունից անհրաժեշտության դեպքում նաև հարձակողական օպերացիաներ իրականացնելու համար, ընդլայնել միջազգային համագործակցությունը երկկողմ և բազմակողմ մասշտաբներով:

4. ՀՀ տեղեկատվական անվտանգության ապահովման տեսանկյունից միջազգային համագործակցության ընդլայնման համար որպես հիմնական հարթակ կարող է դիտարկվել ՀԱՊԿ-ը, որի շրջանակում արդեն բավականին գործնական քայլեր են արվել հիմնախնդրի ուղղությամբ: Հետաքրքիր է նաև հասկանալ, թե ինչ այլ հարթակներ կարող են օգտագործվել, մասնավորապես ՆԱՏՕ-ի շրջանակում ինչ քայլեր կարող են իրականացվել:

Հետազոտության հիմնական դրույթներն արտացոլված են հեղինակի հետևյալ գիտական հոդվածներում.

1. **Մկրտչյան Հ.,** ՌԴ և ԱՄՆ տեղեկատվական անվտանգության հայեցակարգային մոտեցումների համեմատական վերլուծություն, «Բանբեր Երևանի համալսարանի», «Միջազգային հարաբերություններ, Քաղաքագիտություն» 141.6, Երևան 2013թ., էջ 61-65:
2. **Մկրտչյան Հ.,** Թվային դիվանագիտություն. Հնարավորություններ և հեռանկարներ, «Բանբեր Երևանի համալսարանի. Միջազգային հարաբերություններ. Քաղաքագիտություն», Երևան 2016, №2 (20), էջ 78-85:
3. **Մկրտչյան Հ.,** ՀՀ պետական տեղեկատվական քաղաքականության հիմնական ուղղությունները, «Բանբեր Երևանի համալսարանի. Միջազգային հարաբերություններ. Քաղաքագիտություն», Երևան 2017, №2 (22), էջ 73-81:
4. **Մկրտչյան Հ.,** ՀՀ տեղեկատվական անվտանգության արտաքին սպառնալիքներն ու դրանց կանխարգելման միջոցառումները, «Բանբեր ՀՊՏՀ 2017.3», Երևան 2017, էջ 93-102:
5. **Մկրտչյան Հ.,** Տեղեկատվական սպառնալիքների առաջացման առանձնահատկություններն ու դրսևորումները համաշխարհայնացման համատեքստում, «Կրթությունը և գիտությունը Արցախում», 1-2, «Ասողիկ» հրատ. Երևան 2017, էջ 70-75:

6. **Մկրտչյան Հ.,** «Տեղեկատվական անվտանգություն» հասկացության զարգացումը, «Բանբեր Երևանի համալսարանի. Միջազգային հարաբերություններ. Քաղաքագիտություն», Երևան 2017, №3 (24), էջ 55-62:
7. **Մկրտչյան Հ.,** ԱՄՆ և ՉԺՀ տեղեկատվական անվտանգության ապահովման մեխանիզմների համեմատական վերլուծություն, «Արևելագիտության հարցեր», ԵՊՀ, հատ.13, Երևան 2017, էջ 208-225:

Мкртчян Айкуи Вардгесовна

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РА В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ

Диссертация на соискание ученой степени кандидата политических наук по специальности 23.00.02 – "Политические институты и процессы, международные отношения".

Защита состоится 4 мая 2018 г., в 15:00 часов, на заседании специализированного совета ВАК РА 056 "Политология" при Национальном исследовательском университете обороны МО РА (ул. К. Улнеци 56/6, 0037, г. Ереван, Республика Армения).

Резюме

Цель исследования – провести комплексный и последовательный анализ системы информационной безопасности Республики Армения, указать на проблемы информационной безопасности РА в условиях глобализации. Это предопределяет необходимость разработки научно обоснованной системы, оценку состояния и перспектив информационной безопасности в контексте информационных угроз в условиях глобализации, разработку соответствующих мероприятий для противодействия настоящим и возможным угрозам национальным ценностям, интересам и целям.

В Главе первой – **"Проблемы информационной безопасности в условиях глобализации"** – анализируются эволюция информационной безопасности, особенности возникновения информационных угроз в условиях глобализации, роль цифровой дипломатии в контексте политики информационной безопасности. Акцентируется рассмотрение информационной безопасности в контексте обеспечения общественной безопасности. В этом аспекте необходимо обеспечение нравственно-психологической безопасности общества от внутренних и внешних информационных угроз. Обосновывается тот факт, что для эффективного развития Армении в условиях новых вызовов необходимы новые внешнеполитические проекты в цифровой сфере, направленные на укрепление мягкой силы и развитие науки, технологий и образования.

Во второй главе – **"Аспекты применения в РА международного опыта по обеспечению информационной безопасности"** – представлена работа, проделанная в направлении обеспечения информационной безопасности со стороны США, РФ и КНР. Анализируются концептуальные документы, имеющие отношение к данной сфере, механизмы обеспечения информационной безопасности. Опираясь на опыт вышеуказанных стран, автор работы делает вывод о том, что для Армении могут быть эффективными как оборонительные мероприятия, так и наступательные. Опыт России может быть применен для усовершенствования нормативной базы, у опыта Китая можно позаимствовать практические шаги: открыть соответствующие агентства, провести операции по информационной атаке. Опыт США особенно важен в плане проведения цифровой дипломатии, что позволит нашей стране без значительных финансовых средств проводить эффективную информационную политику.

В третьей главе диссертации – **“Нынешнее состояние информационной безопасности Республики Армения и пути ее обеспечения”** – представлены внутренние и внешние угрозы информационной безопасности РА, предлагаются мероприятия по их предотвращению, представлены также основные направления государственной информационной политики РА, предлагаются пути их совершенствования. Обосновывается необходимость разработки таких документов, которые создадут концептуальную базу для укрепления жестких и мягких, наступательных и оборонительных измерений; рассмотрение информационной безопасности РА в единстве с информационной безопасностью Арцаха.

Основными заключениями исследования являются:

1. Информационная безопасность стала одним из важнейших геополитических факторов, определяющих судьбу стран. В подобных условиях чрезвычайно важно формирование единой государственной политики по обеспечению национальных интересов в информационной сфере, усовершенствование действующего законодательства, расширение сотрудничества между органами государственной власти и научными заведениями, занимающимися основными проблемами данной сферы.
2. Для эффективного развития Армении в условиях новых вызовов необходимы новые внешнеполитические проекты в цифровой сфере, направленные на укрепление мягкой силы и развитие науки, технологий и образования. В подобных условиях цифровая дипломатия может стать способом продвижения национальных интересов на мировой арене.
3. Пример США красноречив и поучителен в вопросе уточнения необходимого инструментария и разработки механизмов информационной безопасности. Механизмы цифровой дипломатии, применяемые Соединенными Штатами Америки, можно широко использовать и в Армении.
4. Опыт России может быть применен в Армении, в аспекте поправок нормативной базы, связанной со сферой информационной безопасности. В этом плане особенно актуальна поправка концепции информационной безопасности.
5. Исходя из китайского опыта по обеспечению информационной безопасности, помимо оборонительных мероприятий, необходимо предпринять и практические шаги, подготовить особых специалистов, которые смогут вести информационные войны или использовать возможности, предоставляемые цифровой дипломатией, для создания положительного образа страны и противодействия антиармянской пропаганде.

Haykuhi Vardges Mkrtchyan

INFORMATION SECURITY ISSUES OF THE RA IN THE CONTEXT OF GLOBALIZATION

"Dissertation under 23.00.02 – "Political Institutions and Processes, International Relations" aspiring to earn PhD in Political Sciences.

The public defense will take place on May 4, 2018 at 15:00 at the National Defense Research University, MoD RA at 056 "Political Sciences" HAC Specialized Chamber session.
(Address K. Ulnetsi str. 56/6, Yerevan 0037, Republic of Armenia)

Summary

The primary purpose of the study is to comprehensively and systematically analyze the information security system in the Republic of Armenia. The thesis is concerned with issues relating to the management of information security system in the Republic of Armenia in general, as well as it highlights the impact of globalization on the system of information security in the RA. The thesis argues the necessity to scientifically elaborate information security system, to assess the state and perspectives of information security threats in a global perspective, and to work out appropriate measures to counter any real or possible threats and challenges posed to national values, interests and goals.

The first chapter "**Information Security Issues in the Context of Globalization**" touches upon the aspects of the evolution of information security, the peculiarities of the emergence of information threats in the context of globalization and the role of the digital diplomacy of information security in political context. The thesis specifies the need for the observation of information security in the context of public security provision. There is a necessity to provide moral and psychological security to the public both internally and externally. The necessity of new external projects directed at the reinforcement of soft power and science, technological and educational development in the context of new challenges for the efficient development of Armenia is emphasized. The research underscores the importance of the application of the successful experience of foreign countries in the area of digital diplomacy in Armenia.

The second chapter **"The Aspects of Application of International Experience for the Provision of Information Security in RA"** presents the study that observes the work directed at the provision of information security of the USA, the RF and the PRC. It analyzes conceptually relevant documents and mechanisms ensuring information security. Basing on the data and observations of the above-mentioned countries we conclude that both defensive and offensive actions of the area under discussion may prove to be beneficial for Armenia. Russia's experience may be applicable to perfect the normative background; China's experience may serve as an example for practical measures such as the establishment of appropriate agencies and carrying out informative offensive operations. The US experience is of great importance in the area of digital diplomacy implementation, which will allow our country to carry out information policy efficiently without any tangible expenses.

The third chapter of the thesis **'The Present State of Information Security in the RA and Means of its Provision"** observes internal and external threats to information security in the RA, puts forward prevention measures, presents the main directions of RA state information policy and suggests means of perfection. Chapter three justifies the necessity of elaboration of such a document which will create conceptual bases to strengthen soft and tough, offensive and defensive measures for the RA information security; a joint observation of the RA and Artsakh's information security;

The main points of **Conclusion** are as follows:

1. Information confrontation has become one of the most important geopolitical factors, which decides countries' destiny. In such conditions it of utmost importance to create a uniform policy directed at the provision of national interests; to improve the existing constitution; to extend the cooperation among the scholarly institutions concerned with the issues of information security.
2. Under the conditions of new challenges to successfully develop Armenia requires new projects in the digital sphere directed at strengthening soft power and science and developing of technology and science. Thus, the activation of state bodies' endeavors must be viewed as a primary issue in the near future.
3. The US example is vivid and educational while elaborating information security structures and clarifying the question of necessary tools. The US mechanism of digital diplomacy may be practiced extensively in Armenia.
4. The Russian experience of information security may be applicable for Armenia from the point of view of upgrading the normative base relevant to information security.
5. The Chinese experience of information security provision assumes in addition to defensive measures undertaking of practical ones such as the training of specialists, who will be able to wage information wars far and to take advantage of digital diplomacy opportunities to create a positive image of the country and to counteract anti-Armenian propaganda.