ՀԱՅԿՈՒՀԻ ՄԿՐՏՉՅԱՆ
ԵՊՀ միջազգային հարաբերությունների ֆակուլտետի քաղաքական ինստիտուտների և գործընթացների ամբիոնի դասախոս

ՀՀ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՐՏԱՔԻՆ ՍՊԱՌՆԱԼԻՔՆԵՐՆ ՈՒ ԴՐԱՆՑ ԿԱՆԽԱՐԳԵԼՄԱՆ ՄԻՋՈՑԱՌՈՒՄՆԵՐԸ

Քսանմեկերորդ դարի աշխարհաքաղաքական նոր իրադարձությունները փոփոխել են նախկին վտանգների ու սպառնալիքների ծավալները, բնույթը: Նման պայմաններում ՀՀ տեղեկատվական անվտանգության ապահովման առաջնահերթ միջոցառումներից են արտաքին սպառնալիքների բացահայտումը և դրանց կանխարգելման միջոցառումների իրականացումը:

Հիմնաբառեր. *տեղեկատվական անվտանգություն, տեղեկատվական սպառնալիքներ, արտաքին տեղեկատվական սպառնալիքներ, տեղեկատվական պատերազմներ*

JEL: C80, C89, L86

Արդի դարաշրջանում աշխարհաքաղաքական նոր իրադարձությունների պայմաններում փոփոխվել են նախկին վտանգների ու սպառնալիքների ծավալներն ու բնույթը: Տեղեկատվության բնագավառում անհատի, հասարակության ու պետության կենսական կարևոր շահերը վտանգվում են տեղեկատվական սպառնալիքների պատճառով, ուստի պետությունների համար բավական բարդացել է տեղեկատվական անվտանգության ապահովումը:

Նոր քաղաքական հակամարտությունների կանխարգելման համար յուրաքանչյուր պետության գործունեության կարևոր ուղղություններից մեկը պետք է դառնա տեղեկատվական անվտանգության ապահովումը, և պատահական չէ, որ պետությունները մշակում են տեղեկատվական անվտանգության ապահովման համապատասխան քաղաքականություն:

ՀՀ տեղեկատվական ոլորտը բնութագրվում է տեղեկատվության փոխանակման ժամանակակից միջոցների և տարատեսակ համակարգչային տեխնոլոգիաների արագընթաց զարգացմամբ: Ժամանակակից հայ հասարակությունն արագ տեմպերով մտնում է համացանց, շարժական կապի ներթափանցումը նույնպես շարունակում է աճել[1]: Ներկայումս հանրապետությունում տեղեկատվության մշակման, պահպանման և փոխանցման համար լայնորեն օգտագործվում են տեղեկատվական հեռահաղորդակցական տեխնոլոգիական միջոցներ և տեղեկատվական հեռահաղորդակցման համակարգեր՝ ներառյալ միջազգային տեղեկատվական համացանցը:

Բացի այդ, հասարակությունն օգտվում է բազմաթիվ էլեկտրոնային, առցանց բանկային ծառայություններից, ինչի հետևանքով Հայաստանում բարդանում է տեղեկատվական անվտանգության ապահովումը: Կանխատեսվում է, որ մոտ ապագայում համակարգիչները և տեղեկատվական համակարգերը ամբողջովին կապահովեն տեղեկատվական ռեսուրսների ոլորտում տարբեր գործարքների իրականացումը[2]: Ուստի պատահական չէ, որ այսօր մեծապես կարևորվում են տեղեկատվական անվտանգության հիմնախնդիրների քննարկումը և դրանց լուծումների մշակումը:

Դրա հետ մեկտեղ, տեղեկատվական անվտանգության ապահովման խնդիրներին բավարար ուշադրություն չդարձնելը հաճախ հանգեցնում է անցանկալի հետևանքների. մուտք դեպի փակ տեղեկատվություն, դրա ոչնչացում կամ խափանում: Այսպես՝ դեռ 2012 թ. Հայաստանը կիբեռանվտանգության տեսանկյունից ամենախոցելի երկրներից մեկն էր: Ըստ Կասպերսկու լաբորատորիայի տվյալների՝ Հայաստանը երրորդ տեղում էր այն երկրների ցանկում, որտեղ համացանցից օգտվողները ենթարկվում են ամենամեծ թվով հարձակումների: Իրավիճակը բացասական էր նաև 2013 թ., երբ Հայաստանը կրկին ամենավտանգավորների եռյակում էր[3]: Սակայն արդեն 2016 թ. նույն Կասպերսկու լաբորատորիայի զեկույցում ակնհայտ են դրական փոփոխությունները: Այսպես՝ վարակված համակարգիչների քանակով Հայաստանը միջին ռիսկայնությամբ երկրների ցանկում էր[4]:

Կիբեռանվտանգության ապահովման և կայացման մակարդակով տարածաշրջանի երկրների ցանկում Հայաստանը զբաղեցնում է վերջին տեղը՝ զգալիորեն զիջելով հարևան Ադրբեջանին և Վրաստանին[5]:

Ցավալի են նաև համաշխարհային մասշտաբով Հայաստանի արդյունքները: Այսպես՝ ըստ ՄԱԿ-ի հեռահաղորդակցության միջազգային միության (ITU) «Կիբեռանվտանգության գլոբալ ինդեքս 2017» վարկանշի՝ կիբեռանվտանգության ապահովման բնագավառում Հայաստանը 111-րդն է հարց-

---

[1] Տե՛ս **Ս.Մարտիրոսյան,** Համացանցը Հայաստանում. 2016 թվականի ամփոփում (http://www.noravank.am/arm/articles/detail.php?ELEMENT_ID=15344&sphrase_id=58069, վերջին մուտքը՝ 10.05.2017 թ.):

[2] Տե՛ս Տեղեկատվական անվտանգության ապահովման միջոցառումների համալիր ծրագիրը հաստատելու մասին Հայաստանի Հանրապետության Կառավարության որոշման նախագիծ (http://mtcit.am/edfiles/files/Naxagcer/6791arm-TexAnvtang.pdf, վերջին մուտքը՝ 11.04.2017 թ.):

[3] Տե՛ս **Ս. Մարտիրոսյան,** Հայաստանի հասարակությունը և կիբեռանվտանգությունը. իրավիճակը 2016 թ. (http://noravank.am/arm/articles/security/detail.php?ELEMENT_ID=15400, վերջին մուտքը՝ 13.05.2017 թ.):

[4] Տե՛ս նույն տեղը:

[5] Տե՛ս Global Cybersecurity Index & Cyberwellness Profiles. International Telecommunication Union and ABI Research, 2015 (http://www.itu.int/dms_pub/itud/opb/str/D-STR-SECU-2015-PDF-E.pdf):

ման ցուցակում ընդգրկված 193 երկրների շարքում[6]: Հարցման արդյունքներով գնահատվում է պետությունների կիբեռանվտանգության մակարդակը՝ ըստ հինգ հիմնական ցուցանիշների՝ օրենսդրական բազա, տեխնիկական տվյալներ, կազմակերպչական հարցեր, որակի բարձրացում և համագործակցություն:

Հարկ է նշել, որ ՀՀ քրեական օրենսգրքի մի ամբողջ գլուխ (24) անդրադառնում է համակարգչային տեղեկատվության անվտանգության դեմ ուղղված հանցագործություններին: Ընդ որում, գլխի բոլոր յոթ հոդվածները (251՝ Համակարգչային տեղեկատվության համակարգ առանց թույլտվության մուտք գործելը (ներթափանցելը), 252՝ Համակարգչային տեղեկատվությունը փոխելը, 253՝ Համակարգչային սաբոտաժ, 254՝ Համակարգչային տեղեկատվությանն ապօրինի տիրանալը, 255՝ Համակարգչային տեղեկատվություն ապօրինի մուտք գործելու համար հատուկ միջոցներ պատրաստելը կամ իրացնելը, 256՝ Վնասաբեր ծրագրեր մշակելը, օգտագործելն ու տարածելը, 257՝ Համակարգչային համակարգը կամ ցանցը շահագործելու կանոնները խախտելը) սահմանում են քրեական պատասխանատվություն:

Սակայն ՀՀ օրենսդրական դաշտում բացակայում են որոշակի ձևակերպումները, թե ինչ քայլեր պետք է ձեռնարկվեն այն դեպքերում, երբ համակարգչային հանցագործությունները կատարում են այլ պետությունների քաղաքացիները:

Ըստ ոստիկանության պաշտոնական տվյալների՝ վերջին երկու տարում ավելացել է համակարգչային հանցագործությունների թիվը.

Աղյուսակ 1

ՀՀ-ում կիբեռհանցագործությունները 2015 թվականին

Հանցատեսակ	*Գրանցված գործ*	*Հարուցված քր. գործ*
Հոդված 181 (Հափշտակությունը, որը կատարվել է համակարգչային տեխնիկայի օգտագործմամբ)	39	39
Հոդված 251 (Համակարգչային տեղեկատվության համակարգ առանց թույլտվության մուտք գործելը)	1	1
Հոդված 252 (Համակարգչային տեղեկատվությունը փոփոխելը	1	1
Հոդված 253 (Համակարգչային սաբոտաժը)	4	4
Հոդված 254 (Համակարգչային տեղեկատվությանն ապօրինի տիրանալը)	15	15
Ընդամենը	**60**	**60**

Աղյուսակ 2

ՀՀ-ում կիբեռհանցագործությունները 2016 թվականին

Հանցատեսակ	*Գրանցված գործ*	*Հարուցված քր. գործ*
Հոդված 181 (Հափշտակությունը, որը կատարվել է համակարգչային տեխնիկայի օգտագործմամբ)	48	44
Հոդված 253 (Համակարգչային սաբոտաժը)	1	1
Հոդված 254 (Համակարգչային տեղեկատվությանն ապօրինի տիրանալը)	28	28
Ընդամենը	**77**	**73**

Այսպիսով՝ կիբեռանվտանգությունն առնչվում է տեղեկատվական անվտանգության տեխնիկական խնդիրներին, այն է՝ համակարգչային տվյալների պաշտպանությանը չարտոնված մուտքից, օգտագործումից, հրապա-

[6] ITU-ի կիբեռանվտանգության գլոբալ ինդեքս. Հայաստանը 111-րդն է 193 երկրների շարքում (https://news.am/arm/news/399731.html, վերջին մուտքը՝ 10.08.2017 թ.):

րակումից, փոփոխումից կամ ոչնչացումից, որպեսզի ապահովված լինեն դրանցում առկա տեղեկատվության գաղտնիությունը, ամբողջականությունը և մատչելիությունը, իսկ բովանդակային առումով տեղեկատվական անվտանգությունն առնչվում է քարոզչական, հակաքարոզչական, տեղեկատվական հոսքերի հետ կապված խնդիրներին: Նշենք, որ վերջին շրջանում Հայաստանում սկսել են մեծ ուշադրություն դարձնել նաև տեղեկատվական անվտանգության տեխնիկական խնդիրներին: Մասնավորապես՝ ՀՀ ՊՆ Պաշտպանական ազգային հետազոտական համալսարանի Ազգային ռազմավարական հետազոտությունների ինստիտուտի ազգային անվտանգության քաղաքականության և տեղեկատվական-հաղորդակցային տեխնոլոգիաների կենտրոնը կիբեռանվտանգության ոլորտում միջազգային փորձի վերլուծության հիման վրա մշակել և ԱՄՆ Պաշտպանական ազգային համալսարանի Տեղեկատվական ռեսուրսների կառավարման քոլեջի, նույն համալսարանի Տեխնոլոգիաների և ազգային անվտանգության քաղաքականության կենտրոնի, ինչպես նաև Հարվարդի և «Գործընկերություն հանուն խաղաղության» կոնսորցիումի կիբեռանվտանգության ոլորտի փորձագետների հետ սերտ համագործակցությամբ փորձաքննել է ՀՀ կիբեռանվտանգության ազգային ռազմավարության նախագիծը[8]:

Տեղեկատվական անվտանգության համար սպառնալիքները նպատակային և կանոնակարգված գործողությունների ամբողջություն են՝ ուղղված ինչպես անձի, հասարակության և պետության, այնպես էլ պետությունների դաշինքների տեղեկատվական միջավայրի զարգացման ու գործառման դեմ[9]:

Քաղաքական գիտությունների դոկտոր Ա. Աթանեսյանը Հայաստանի և հայ հասարակության պարագայում տեղեկատվական անվտանգության սպառնալիքները բաժանում է երեք մակարդակի՝ ներպետական, տարածաշրջանային և գլոբալ[10]:

ՀՀ ներպետական սպառնալիքների կարող է հանգեցնել հասարակության ոչ միասնական լինելը ազգային ռազմավարական խնդիրների լուծման ուղղություններին և միջոցներին առնչվող հարցերում, պետական իշխանության մարմինների լեգիտիմության ընդունման ոչ բավարար մակարդակը, ազգային ինքնության և անվտանգության տեսանկյունից հիմնարար խնդիրների (ղարաբաղյան հակամարտության լուծում, ցեղասպանության ճանաչում, բնակչության արտագաղթ և այլն) շահարկումը տարբեր քաղաքական ուժերի կողմից, արտասահմանյան ընկերությունների՝ հայաստանյան հեռախոսակապի շուկայի կառավարումը և պետության՝ հեռախոսային ու համացանցային ծառայությունների ոլորտում քաղաքացիների շահերի պաշտպանության բացակայությունը:

Տարածաշրջանային առումով, ՀՀ տեղեկատվական անվտանգության սպառնալիքները հիմնականում պայմանավորված են հարևան երկու երկրների՝ Թուրքիայի և Ադրբեջանի հնարավոր սպառնալիքներով: Ադրբեջանը

---

[8] Տե՛ս **Բ. Պողոսյան,** ՀՀ կիբեռանվտանգության ազգային ռազմավարության մշակումը և ՊԱՀՀ-ի կազմում կիբեռտարածության ռեսուրսների կառավարման ռազմավարության ինստիտուտի ստեղծումը ՀՀ ազգային անվտանգության ռազմավարության վերանայման համատեքստում, «Հայկական բանակ» (ՀՀ ՊՆ Պաշտպանական ազգային հետազոտական համալսարանի ռազմագիտական հանդես), 1–2, 2017, էջ 58:

[9] Տե՛ս Угрозы информационной безопасности (http://kirillykk.narod.ru/ugroz.html, վերջին մուտքը՝ 20.06.2017 թ.):

[10] Տե՛ս **Ա. Աթանեսյան,** Սպառնալիքներ ՀՀ տեղեկատվական անվտանգությանը. եռամակարդակ վերլուծություն, 21-րդ ԴԱՐ, 2010, N6:

պարբերաբար նախաձեռնում է հարձակողական հակահայկական տեղեկատվական պատերազմներ, որոնց նպատակներից են ադրբեջանական ինքնության «կերտումն» ու ամրապնդումը, աշխարհում Ադրբեջանի դրական կերպարի ստեղծումը, տարբեր միջազգային կառույցներին անդամակցման միջոցով սեփական ռազմավարական շահերի պաշտպանությունն ու այդ կազմակերպությունների օգտագործումը հակահայկական քարոզչության ու միջազգային համայնքում հակահայկական տրամադրությունների ստեղծման նպատակով: Այսպես՝ Լոնդոնի ադրբեջանական համայնքի կազմակերպության նախաձեռնությամբ «Խոջալուի ողբերգությունը. միջազգային տեսակետ» և «Միջազգային տեսակետներ. ԼՂՀ-ի շուրջ հայ-ադրբեջանական հակամարտությունը» անգլալեզու ադրբեջանամետ հրատարակությունների օրինակներ են ուղարկվել միջազգային լրատվամիջոցներին՝ «Վաշինգթոն փոստին», «Սանդի թայմսին», «Նյու Յորք թայմսին», «Նյուզուիքին», «Բոսթոն գլոբին» և աշխարհի 60 գրադարանների[11]:

Վերոհիշյալին գումարվում է նաև Թուրքիայի հետ դիվանագիտական հարաբերությունների բացակայությունը, ինչն անընդհատ զգոնություն է պահանջում տեղեկատվության բնագավառում հավանական սպառնալիքներին դիմակայելու համար:

Միջազգային մակարդակում ՀՀ տեղեկատվական սպառնալիքների կարող է հանգեցնել ադրբեջանական հակաքարոզչությունը, որով վիճարկվում են հայկական երաժշտության ծագումն ու էությունը, հայկական խոհանոցի հայկական լինելը, հայ ժողովրդի ծագումն ու բնակության տարածքը և այլն: Պետության ներսում ոչ բավարար մակարդակով այնպիսի գաղափարների նյութականացումը, ինչպիսիք են ժողովրդավարությունը, կոռուպցիայի բացակայությունը, բարձր կենսամակարդակն ու հանրային համերաշխությունը, օրենքի գերակայությունն ու քաղաքացիների իրավունքների պաշտպանվածությունը զգալիորեն խոչընդոտում են բարձր վարկանիշի և համբավի ձեռքբերմանը:

Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգում սպառնալիքների աղբյուրները դասակարգվում են երկու տիպի՝ արտաքին և ներքին[12] : Արտաքին սպառնալիքների կարող է հանգեցնել օտարերկրյա քաղաքական, տնտեսական, ռազմական, հետախուզական և տեղեկատվական կառույցների գործունեությունը՝ ուղղված տեղեկատվական ոլորտում Հայաստանի Հանրապետության շահերի դեմ, համաշխարհային տեղեկատվական շուկաներից Հայաստանի դուրսմղմանը:

Ավելին, միջազգային տեղեկատվական աղբյուրներով հակահայկական կեղծ տեղեկատվության տարածումը, հայ ազգային հոգեբանական խառնվածքի, մշակութային ինքնության և Հայ առաքելական եկեղեցու դեմ ուղղված քայքայիչ գործողությունները, այլ պետությունների կողմից ՀՀ պետական տեղեկատվության նկատմամբ չթույլատրված հասանելիություն ստանալու ձևերն ու մեթոդները կիրառելը նույնպես արտաքին սպառնալիք է մեր տեղեկատվական անվտանգության համար[13]:

---

[11] Տե՛ս **Հ. Նահապետյան,** Ադրբեջանական սփյուռքի քարոզչական ձեռնարկները. (http://www.noravank.am/am/?page=theme&thid=5&nid=1276, վերջին մուտքը՝ 12.05.2017 թ.):

[12] Տե՛ս Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգ (http://www.arlis.am/DocumentView.aspx?DocID=52559, վերջին մուտքը՝ 11.05.2017 թ.):

[13] Սրանք հիմնականում Թուրքիայից ու Ադրբեջանից եկող սպառնալիքներն են:

Այդուհանդերձ, կարծում ենք՝ հարկ է ընդլայնել ՀՀ տեղեկատվական անվտանգության հայեցակարգում թվարկված սպառնալիքների շրջանակը: Վերոհիշյալին կարելի է գումարել նաև ՀՀ տեղեկատվական ոլորտի վրա ներգործելու, տեղեկատվական և հեռահաղորդակցային համակարգերի բնականոն ընթացքը խախտելու նպատակով արտաքին սուբյեկտների կողմից տեղեկատվական պատերազմների հայեցակարգերի մշակումը:

Համարվում է, որ Հայաստանի և հայության անվտանգությանը սպառնացող արտաքին սպառնալիքների աղբյուրները գլխավորապես մի քանի ադրբեջանական և թուրքական լրատվամիջոցներ են: Բանն այն է, որ երկար տարիներ շարունակվում է տեղեկատվական հակամարտությունը հարևան Ադրբեջանի հետ: Ընդ որում, կարելի է առանձնացնել այդ հակամարտության մի քանի փուլ[14].

- Առաջին փուլը սկսվում է 1994 թվականից, երբ հայկական և ադրբեջանական կողմերի միջև հրադադարի կնքումից սկսած՝ տեղեկատվական քաղաքականությունը, մնալով կոնֆլիկտային հաղորդակցման տրամաբանության շրջանակներում, մտնում է նոր՝ հետպատերազմյան շրջան: Հայաստանը ներկայացվում էր որպես «ոճիրների ունակ» երկիր, որը Սփյուռքի օգնությամբ կարողացավ «գրավել» ադրբեջանական տարածքները:
- Երկրորդ փուլում (1995–1997 թթ.) Բաքվի քարոզչության նպատակը միջազգային հանրության միջոցով պատերազմի հետևանքների վերացումն էր, զինադադարի երկարաձգումը և փախստականների սոցիալական խնդիրների բարձրաձայնումը:
- Իբրև Ադրբեջանի հակահայկական տեղեկատվական քաղաքականության երրորդ փուլ՝ առանձնացվում են 1998–2002 թվականները: 2000 թվականին ադրբեջանական հաքերների(կայքահեն) կողմից առաջին անգամ ժամանակավորապես շարքից դուրս բերվեցին հայկական մի շարք համացանցային կայքեր, որոնցում շոշափվում էին ցեղասպանության և ԼՂՀ թեմաները: 1998–2002 թթ. ադրբեջանական հակահայկական տեղեկատվական քաղաքականության աշխուժացումը պայմանավորված էր Հայաստանի ներքաղաքական բարդ իրավիճակով (1999 թ. հոկտեմբերի 27-ի ահաբեկչություն) և ադրբեջանական տնտեսությունում նավթային գործոնի ուժգնացմամբ: Փաստորեն, տնտեսական գործոնը թույլ տվեց Ադրբեջանին զգալի ֆինանսական միջոցներ տրամադրել հակահայկական տեղեկատվական քաղաքականության մշակման, կազմակերպման և իրականացման գործին, ինչպես նաև ներգրավել ոլորտի մասնագետների այլ երկրներից:
- 2003 թվականից՝ Իլհամ Ալիևի իշխանության գալուց ի վեր, սկսվում է հակահայկական քաղաքականության չորրորդ փուլը: Այս փուլում Բաքվի հիմնական նպատակը Հայաստանի ու հայության հեղինակազրկումն էր, հայությանը որպես ցեղասպան ազգ ներկայացնելը, որի հետ համատեղ գոյակցումը սպառնում է Ադրբեջանի ազգային անվտանգությանը և այլն:

Մեր կարծիքով՝ ադրբեջանական հակահայկական քաղաքականության հերթական փուլի սկիզբ կարելի է համարել 2016 թ., երբ ապրիլյան քառօրյա պատերազմի ընթացքում այդ հակամարտությունն իր գագաթնակետին հա-

[14] Տե՛ս **Գ. Հարությունյան, Հ. Քոթանջյան** և ուրիշներ, Ադրբեջանի հակահայկական տեղեկատվական համակարգը, «Նորավանք» գիտակրթական հիմնադրամ, Եր., 2009, էջ 22–27:

սավ: Նշված ժամանակահատվածում Ադրբեջանի տեղեկատվական քաղաքականությունն ուղղված էր՝

1. Ներքին լսարանին. իշխանության նպատակն էր հանրության ուշադրությունը շեղել ներքին խնդիրներից (2016 թ. սկզբին Ադրբեջանում նավթի գինը հասավ վերջին հինգ տարիներին արձանագրված նվազագույն մակարդակին՝ 1 բարելի դիմաց 90 դոլարից նվազեց մինչև 30-ի՝ դրանով իսկ կանգնեցնելով երկիրը լուրջ սոցիալ-տնտեսական խնդիրների առջև: Ադրբեջանում սկսվեց բողոքի ցույցերի ալիք, և նկատվեց կենսամակարդակի զգալի անկում), արտաքին սպառնալիքի պատրվակով փորձել համախմբել հասարակությանը, պատերազմի ընթացքի մասին ապատեղեկատվություն տարածելով՝ հասարակական դրական կարծիք ստեղծել իշխանությունների հանդեպ:
2. Արտաքին լսարանին. ադրբեջանական տեղեկատվական գործողությունների թիրախը միջազգային հանրությունն էր՝ Հայաստանը որպես պատերազմի սանձազերծող կողմ, իսկ Ադրբեջանը «զոհի կարգավիճակում» էր ներկայացվում:
3. Հայկական լսարանին. սոցիալական ցանցերում գրանցվեցին հայկական անուններով կեղծ օգտատերեր, ովքեր, տեղեկություններ կորզելու նպատակով, հայատառ հարցեր էին ուղղում հայ օգտատերերին Երևանում և Ստեփանակերտում տիրող իրավիճակի մասին, կամ, իբր առաջնագծում գտնվող իրենց ծանոթների պատմածների հիման վրա, լուրեր էին տարածում՝ փորձելով խուճապ առաջացնել, թե ամեն ինչ կորած է հայերի համար[15]:

Ամբողջ պատերազմի ընթացքում երկկողմանի կիբեռհարձակումներ էին իրականացվում: Հայկական և ադրբեջանական լրատվական և պաշտոնական կայքերն անընդհատ DDoS տիպի հարձակումների էին ենթարկվում, որոնց ժամանակ համակարգչային վիրուսների ներմուծմամբ, էլեկտրոնային նամակների գրոհով (E-mail bombing) և այլ եղանակներով խափանվում էր սերվերների աշխատանքը:

Ընդ որում, այդ ընթացքում ադրբեջանական հաքերային խմբերին միացել էին թուրքական ազգայնական հաքերները:

Սակայն ասել, թե Հայաստանի և հայության անվտանգությանը արտաքին սպառնալիքների աղբյուրները գլխավորապես մի քանի ադրբեջանական և թուրքական լրատվամիջոցներ են, բավականին պարզունակ մոտեցում է: Կարելի է բազմաթիվ օրինակներ բերել, որոնք հաստատում են Հայաստանի՝ տեղեկատվական պատերազմի սուբյեկտ լինելը[16]: Բացի դրանից, Հայաստանի ու հայության համար հատկապես վտանգավոր են հոգևոր-գաղափարական բնույթի գործոնները, որոնց նպատակը հայկական մշակութային ժառանգության նկատմամբ բացասական վերաբերմունքի ստեղծումն է, երկրում անվստահության մթնոլորտի ձևավորումը, Հայաստանի հեղինակազրկումը միջազգային ասպարեզում, տարբեր ոլորտներում (քաղաքական, տնտեսական և այլն) պետության և ազգի կենսական կարևոր շահերի վնասումը[17]:

---

[15] Տե՛ս **Ս. Մարտիրոսյան,** Հայկական և ադրբեջանական ուժերի դիմակայությունը լրատվական դաշտում (http://www.noravank.am/arm/articles/detail.php?ELEMENT_ID=14592, վերջին մուտքը՝ 10.05.2017 թ.):

[16] Տե՛ս **Мартиросян С.,** Некоторые вопросы информационной безопасности Армении и армянства: http://www.noravank.am/ru/?page=analitics&nid=679

[17] Տե՛ս **Գ. Տեր-Հարությունյանց,** Հոգևոր անվտանգությունը որպես տեղեկատվական անվտանգության բաղադրամաս: Տարածաշրջան, «Նորավանք» գիտակրթական հիմնադրամի տեղեկագիր, 2005, էջ 29:

Մեր կարծիքով՝ արտաքին սպառնալիքներին դիմակայելու համար նախ պետք է հստակ բացահայտվեն սպառնալիքների աղբյուրները, փորձագիտական վերլուծության ենթարկվեն դրանց տեխնոլոգիական ու մեթոդաբանական առանձնահատկությունները: Առանց նման աշխատանքի՝ անհնարին է բացահայտել տեղեկատվական սպառնալիքների իրական կենտրոնները, հասկանալ դրանց նպատակները և ռազմավարությունը:

Ինչպես ցույց է տալիս միջազգային փորձը, տեղեկատվական անվտանգության և կիբեռանվտանգության ապահովման բնագավառում վերը նշված խնդիրների համապարփակ և արդյունավետ լուծման համար կարևոր է միջգերատեսչական համագործակցությամբ մշակված համապետական ռազմավարության և համապատասխան քաղաքականության, ինչպես նաև միջգերատեսչական ներուժի համախմբմամբ կիբեռանվտանգության ոլորտը կառավարող մարմնի ստեղծումը[18]:

Ակնհայտ է, որ այդ ոլորտում պետք է օգտագործել անհրաժեշտ գիտելիքների ձեռքբերման ընդունված մեխանիզմները (ուսուցում արտասահմանյան կենտրոններում, փորձագետների հրավիրում և այլն) ու կիրառել դրանք գործնական հարթությունում:

Կարծում ենք՝ արտաքին սպառնալիքներին դիմակայելու այդպիսի միջոցառումներ կարող են լինել՝

- արտաքին սպառնալիքների փորձագիտական վերլուծությունը՝ դրանց աղբյուրները բացահայտելու, ռիսկերը գնահատելու և հակազդման մեթոդները հասկանալու համար,
- տեղեկատվական անվտանգությունն ապահովելիս միջազգային համագործակցության ընդլայնումը,
- ոլորտի առաջատար պետությունների համապատասխան մասնագետների հետ փորձի փոխանակումը,
- թվային դիվանագիտության գործիքարանի լայն կիրառությունը, որը համաշխարհային քաղաքական թատերաբեմում ՀՀ հեղինակության բարձրացման ու պետության համար շահեկան քաղաքական կերպարի ձևավորման ու, առհասարակ, երկրի տեղեկատվական անվտանգության ապահովման հնարավորություն կընձեռի,
- արտերկրում հայկական ներկայացուցչություններին ու կազմակերպություններին ներկայացվող ապատեղեկատվության տարածումը կանխարգելելու նպատակով անհրաժեշտ պայմանների ստեղծումը,
- տեղեկատվական անվտանգության ապահովման որոշակի ուղղություններին, մասնավորապես՝ թվային դիվանագիտությանը ֆինանսական աջակցության մեծացումը,
- քարոզչական և հակաքարոզչական հայկական կենտրոնների աշխատանքները համակարգող կառույցի ձևավորումը:

[18] Տե՛ս ITU National Cybersecurity Strategy Guide. International Telecommunication Union, September 2011 (http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurity StrategyGuide.pdf); “National Cyber Security Strategies”. “European Network and Information Security Agency”, May 2012 (http://www.enisa.europa.eu/ activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/ cyber-securitystrategies-paper):

Օգտագործված գրականություն

1. Աթանեսյան Ա.Վ., Սպառնալիքներ ՀՀ տեղեկատվական անվտանգությանը. եռամակարդակ վերլուծություն, 21-րդ ԴԱՐ, 2010, N6:
2. Պողոսյան Բ., ՀՀ կիբեռանվտանգության ազգային ռազմավարության մշակումը և ՊԱՀՀ-ի կազմում կիբեռտարածության ռեսուրսների կառավարման ռազմավարության ինստիտուտի ստեղծումը ՀՀ ազգային անվտանգության ռազմավարության վերանայման համատեքստում, «Հայկական բանակ», ՀՀ ՊՆ Պաշտպանական ազգային հետազոտական համալսարանի ռազմագիտական հանդես, 1-2, 2017:
3. Հարությունյան Գ., Հայկ Քոթանջյան և ուրիշներ, Ադրբեջանի հակահայկական տեղեկատվական համակարգը, «Նորավանք» գիտակրթական հիմնադրամ, Եր., 2009:
4. Տեր-Հարությունյանց Գ., Հոգևոր անվտանգությունը որպես տեղեկատվական անվտանգության բաղադրամաս. Տարածաշրջան, «Նորավանք» գիտակրթական հիմնադրամի տեղեկագիր, 2005:
5. Մարտիրոսյան Ս., Հայաստանի հասարակությունը և կիբեռանվտանգությունը. Իրավիճակը 2016 թ. (http://noravank.am/arm/articles/security/detail.php?ELEMENT_ID=15400, վերջին մուտքը՝ 13.05.2017թ.):
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.):
7. Մարտիրոսյան Ս., Հայկական և ադրբեջանական ուժերի դիմակայությունը լրատվական դաշտում (http://www.noravank.am/arm/articles/detail.php?ELEMENT_ID=14592 վերջին մուտքը՝ 10.05.2017 թ.):
8. Նահապետյան Հ., Ադրբեջանական սփյուռքի քարոզչական ձեռնարկները, http:// www.noravank.am/am/?page=theme&thid=5&nid=1276, վերջին մուտքը՝ 12.05.2017թ.):
9. Мартиросян С., Некоторые вопросы информационной безопасности Армении и Армянства. http://www.noravank.am/ru/?page=analitics&nid=679
10. Global Cybersecurity Index & Cyberwellness Profiles. International Telecommunication Union and ABI Research, April 2015 (http://www.itu.int/dms_pub/itud/opb/str/D-STR-SECU-2015-PDF-E.pdf):
11. ITU National Cybersecurity Strategy Guide. International Telecommunication Union, September 2011 (http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf); “National Cyber Security Strategies”. “European Network and Information Seurity Agency”, May 2012 (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-securitystrategies-paper):
12. ITU-ի Կիբեռանվտանգության գլոբալ ինդեքս. Հայաստանը 111-րդն է 193 երկրների շարքում (https://news.am/arm/news/399731.html, վերջին մուտքը՝ 10.08.2017 թ.):
13. Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգ (http://www.arlis.am/DocumentView.aspx?DocID=52559, վերջին մուտքը՝ 11.05.2017 թ.)

АЙКУИ МКРТЧЯН
Преподаватель кафедры политических институтов и процессов факультета международных отношений ЕГУ

Внешние угрозы информационной безопасности РА и меры их предотвращения. – В контексте новых геополитических событий двадцать первого века масштабы и характер предыдущих опасностей и угроз изменились. В таких условиях одним из приоритетов информационной безопасности РА является выявление внешних угроз и осуществление превентивных мер.

Ключевые слова: *информационная безопасность, информационные угрозы, внешние информационные угрозы, информационные войны.*
JEL: C80, C89, L86

HAYKUHI MKRTCHYAN
Lecturer at the Department of Political Institutes and Processes, Faculty of International Relations at YSU

External Threats of the Information Security of the RA and Their Prevention Measures. – In the context of the new geopolitical events of the twenty-first century, the extent and nature of previous dangers and threats have changed. In such circumstances, one of the priorities of the information security of the Republic of Armenia is the identification of external threats and the implementation of preventive measures.

Key words: *information security, information threats, external information threats, information wars.*
JEL: C80, C89, L86