ՀՏԴ 004.056:32.001

ՀԱՅԱՍՏԱՆԻ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ ԵՎ ԿՐԻՏԻԿԱԿԱՆ ԵՆԹԱԿԱՌՈՒՑՎԱԾՔՆԵՐԸ

Սամվել Մարտիրոսյան[*]

Բանալի բառեր՝ տեղեկատվական անվտանգություն, կրիտիկական ենթակառուցվածքներ, կիբեռանվտանգություն, Հայաստան, ազգային անվտանգություն։

Տեղեկատվական անվտանգությանը վերաբերող խնդիրներն օրեցօր դառնում են ավելի վտանգավոր և հանդես են գալիս որպես ազգային մակարդակի սպառնալիքներ։ Ոլորտի բարդ խնդիրներից մեկն այն է, որ դրանք անընդհատ ձևափոխման մեջ են գտնվում, մարտահրավերներն ավելի արագ են զարգանում, քան դրանց ուղղված կանխարգելիչ գործողությունները։ Ավելին, տեղեկատվական անվտանգության խնդիրներն արդեն անմիջական կապ են ունենում կրիտիկական ենթակառուցվածքների հետ, և դրանք կարող են հանգեցնել երևույթների, որոնք կարող են դիտվել որպես ազգային մակարդակի անվտանգության սպառնալիքներ։ Խոսքն ինչպես զանգվածային խուճապ հրահրելու հնարավորությունների, ընտրական և այլ տիպի քաղաքական ու հասարակական գործընթացների վրա ներազդեցության հնարավորությունների, այնպես էլ գործարանների, էներգահամակարգերի, ջրամատակարարման և այլ ենթակառուցվածքների վրա հարձակումների մասին է։

Հայաստանի Հանրապետության տեղեկատվական անվտանգության համակարգը. Հայաստանի Հանրապետությունում տեղեկատվական անվտանգության խնդիրները կարելի է բաժանել երկու մասի՝ տեխնիկական, որն աշխարհի շատ երկրներում ընդունված է կոչել կիբեռանվտանգություն, և բովանդակային, որը քարոզչական, հակաքարոզչական, զանգվածային լրագրության, տեղեկատվական հոսքերի հետ կապված խնդիրների հետ է կապված։ Այս խնդիրները նկարագրվում են Հայաստանի Հանրապետության Տեղեկատվական անվտանգության հայեցակարգում[1]։

---

[*] «Նորավանք» ԳԿՀ Տեղեկատվական հետազոտությունների կենտրոնի փորձագետ։

[1] Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգ, 2009թ. հունիսի 26, http://www.arlis.am/DocumentView.aspx?DocID=52559

2011-ից տեղեկատվական անվտանգության տեխնիկական բաղադրիչի համակարգողը Ազգային անվտանգության ծառայությունն է[1]: Բովանդակային հատվածով տեղեկատվական անվտանգության գործառույթները բաշխված են մի շարք կառույցների միջև, բազմաթիվ գործառույթներ իրականացնում են պաշտպանության նախարարությունը, արտգործնախարարությունը և այլն: Համակարգող դեր ունի ՀՀ Նախագահի աշխատակազմի հանրային կապերի և տեղեկատվության կենտրոնը:

Բացի այդ, գոյություն ունի ոլորտային մոտեցում: Խոսքը բանկային ոլորտի մասին է: Այստեղ 2013թ. ընդունվել է որոշում Կենտրոնական բանկի խորհրդի «Տեղեկատվական անվտանգության ապահովման նվազագույն պահանջների սահմանման վերաբերյալ կարգի» մասին, որը նախատեսում է անցում բանկային համակարգի տեղեկատվական անվտանգության ստանդարտներին[2]: 2015թ. ստեղծվեց ՀՀ արդարադատության նախարարության Անձնական տվյալների պաշտպանության գործակալությունը[3]:

Տեղեկատվական անվտանգության անվերահսկելի հատվածները. Հայաստանի Հանրապետությունում մի շարք բնագավառներ տեղեկատվական անվտանգության առումով դուրս են մնում ընդհանուր և մասնավոր վերահսկումից: Հայաստանում գոյություն չունի ազգային կիբեռանվտանգության պատասխանատու մարմին: ԱԱԾ-ի կողմից վերահսկվում է միայն պետական ցանցը, այն էլ՝ ոչ ամբողջությամբ: Այսպես, կառավարությանը կից մի շարք մարմինների կայքերը չեն վերահսկվում: Բացի այդ, Արցախի պետական կայքերի մեծ մասը շարունակում է մնալ խոցելի և պարբերաբար ենթարկվում է հաքերային հարձակումների, հիմնականում ադրբեջանական ցանցահենների խմբերի կողմից[4]:

[1] Տեղեկատվական անվտանգության ապահովման ոլորտում լիազոր և ազգային համակարգող մարմին նշանակելու մասին, 2011թ. մարտի 9, http://www.arlis.am

[2] «Տեղեկատվական անվտանգության ապահովման նվազագույն պահանջների սահմանման վերաբերյալ կարգը» հաստատելու մասին, 9 հուլիսի 2013թ., http://www.arlis.am/DocumentView.aspx?DocID=84836

[3] ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալություն ստեղծելու, ՀՀ արդարադատության նախարարության աշխատակազմի անձնական տվյալների պաշտպանության գործակալությունը լիազոր մարմին ճանաչելու, ՀՀ կառավարության 2002 թվականի նոյեմբերի 28-ի N 1917-ն որոշման մեջ լրացումներ կատարելու և ՀՀ արդարադատության նախարարության անձնական տվյալների պաշտպանության գործակալության կանոնադրությունը և կառուցվածքը հաստատելու մասին, 2 հուլիսի 2015, http://www.arlis.am/documentview.aspx?docid=98941

[4] Օրինակ, Արցախի Հանրապետության գյուղատնտեսության նախարարության կայքը (http://minagro.nkr.am/) ենթարկվեց հաքերային հարձակման արդրբեջանական Anti-Armenia Team ցանցահենային խմբի կողմից 2016թ. մայիսի 15-ին. http://zone-h.org/mirror/id/26268331; Արցախի վերասկիչ պալատի կայքը (http://www.cocnkr.am/) ենթարկվել է հաքերային հարձակման 2017թ. մարտի 22-ին արգենտինյան ցանցահենի կողմից, http://zone-h.org/mirror/id/28914827

Բացի այդ, բացարձակ անվերահսկելի դաշտում են գտնվում մի շարք կրիտիկական ենթակառուցվածքներ, որոնք պետության անմիջական վերահսկողության տակ չեն գտնվում: Նման կրիտիկական հանգույցները, գտնվելով մասնավոր կամ օտարերկրյա կազմակերպությունների վերահսկողության տակ, չունեն ըստ օրենսդրության հստակ պարտավորություններ ապահովելու տեղեկատվական անվտանգության հստակ ստանդարտները: Նաև չկան մեխանիզմներ, որոնք թույլ կտան որևէ պետական կամ անկախ մարմնի իրականացնել աուդիտ և վերհանել համակարգային թույլ կետերը, որոնք կարող են կիբեռհարձակումների համար խոցելի լինել: Այսպես, եթե Մեծամորի ատոմակայանը գտնվում է պետության վերահսկողության տակ և այստեղ կարող են լինել հստակ պահանջներ տեղեկատվական անվտանգության վերաբերյալ, որոնք կարող են վերահսկվել պետական գործակալությունների կողմից, ապա մնացած էներգահամակարգը գտնվում է լրիվ ազատ գոտում:

Պետության կողմից անվերահսկելի և տեղեկատվական անվտանգության կողմից չկարգավորվող դաշտում են գտնվում մի շարք կրիտիկական ենթակառուցվածքային տիրույթներ.

- Էլեկտրաէներգետիկա
- Գազամատակարարում
- Ջրմուղ-կոյուղի
- Հեռահաղորդակցություն:

Այս ոլորտներում ոչ միայն հստակ կարգավորում չկա՝ տեղեկատվական անվտանգության առումով, այլև չի տրված գնահատական, թե որքանով են տվյալ ենթակառուցվածքները պոտենցիալ խոցելի կիբեռհարձակումների տեսանկյունից: Հաշվի առնելով այն հանգամանքը, որ թվայնացումը համակարգերի անընդհատ իրականացվող գործընթաց է, վերոնշյալ ենթակառուցվածքների հնարավոր խոցելիությունները և դրանց վրա կիբեռհարձակումների միջոցով ներազդելու հնարավորությունն անընդհատ մեծանում են:

Հայաստանի հասարակությունը՝ կրիտիկական ենթակառուցվածք. Հայաստանում կիբեռանվտանգությունը տարբեր բնագավառներում դառնում է ազգային մակարդակի խնդիր: Հասարակությունն արագ տեմպերով մտնում է համացանց, շարժական կապի ներթափանցումը նույնպես շարունակում է աճել[1]: Բջջային կապի բաժանորդների թվաքանակը Հայաս-

[1] *Սամվել Մարտիրոսյան,* Համացանցը Հայաստանում. 2016 թվականի ամփոփում, http://www.noravank.am/arm/articles/detail.php?ELEMENT_ID=15344&sphrase_id=58069

տանում 2016թ. երրորդ եռամսյակում հասել է 3 486 480-ի, ինչը նախորդ եռամսյակի համեմատ 52 084 բաժանորդով ավելի է (2015թ. այս ցուցանիշը 3 424 236 էր)։ Ինչ վերաբերում է ինտերնետ կապի հասանելիությանը, ապա այստեղ նույնպես դիտվում է աճ բոլոր ցուցանիշներով։

2016թ. երրորդ եռամսյակի տվյալներով.

- լայնաշերտ ինտերնետ կապի բաժանորդագրությունների թիվը հասել է 265 480-ի (+4 835)
- շարժական լայնաշերտ ինտերնետ կապի բաժանորդագրությունների թիվը՝ 247 140-ի (+15 442)
- բջջային հեռախոսներով ինտերնետ կապից օգտվող բաժանորդների թիվը՝ 1 891 078-ի (+ 229 132)։

Հասարակությունը սկսում է օգտվել բազմաթիվ էլեկտրոնային ծառայություններից, օնլայն բանկային ծառայություններից և այլն, ինչի շնորհիվ Հայաստանը դառնում է ավելի հրապուրիչ զանազան կիբեռհանցագործների համար։ Մյուս կողմից՝ Հայաստանում դեռևս չկա կիբեռանվտանգության վերաբերյալ ուսուցման հստակ մոտեցում։ Ոչ միջնակարգ, ոչ բարձրագույն ուսուցումը չի տրամադրում այն հմտությունները, որոնք պահանջված են այսօր արդիական վտանգներին դիմակայելու համար։ Նաև չկան ծրագրեր՝ ուղղված կրթական տարիքից դուրս քաղաքացիների իրազեկմանը։ Չկա ազգային մակարդակի իրազեկման կենտրոն, որը տեղյակ կպահեր հանրությանը կոնկրետ տվյալ պահին վերաբերող լայն տարածում ստացած կիբեռվտանգների վերաբերյալ։ Այս ամենը Հայաստանի հասարակությունը դարձնում է բավական խոցելի կիբեռհարձակումների տեսանկյունից։

Հայաստանը կիբեռանվտանգության տեսանկյունից ամենախոցելի երկրներից մեկն էր համարվում։ Ըստ *Kaspersky Lab* տվյալների, մեր երկիրը 2016թ. վարակված համակարգիչների քանակով միջին ռիսկայնության երկրների ցանկում է հայտնվել. վարակված է, ըստ հակավիրուսային լաբորատորիայի տվյալների, համակարգիչների 40,4%-ը[1]։

Համացանցում վարակվելու ռիսկայնության տեսանկյունից Հայաստանը նույնպես դուրս է եկել ամենավտանգավոր երկրների տասնյակից և զբաղեցնում է 14-րդ տեղը 33,01% ցուցանիշով (տե՛ս *Աղյուսակ 1*)[2]։

[1] Kaspersky security bulletin 2016: Статистика, https://kasperskycontenthub.com/securelist-russia/files/2016/12/KASPERSKY_SECURITY_BULLETIN_2016_Statistics_RUS.pdf

[2] Նույն տեղում։

Աղյուսակ 1

Համացանցում հարձակման ենթարկվելու ամենամեծ ռիսկերն ունեցող երկրներն ըստ Kaspersky Lab-ի (տվյալ երկրում հարձակման ենթարկվող համակարգիչների տոկոսը)

1	Ռուսաստան	42,15%
2	Ղազախստան	41,22%
3	Իտալիա	39,92%
4	Ուկրաինա	39,00%
5	Բրազիլիա	38,83%
6	Ադրբեջան	38,81%
7	Իսպանիա	38,21%
8	Բելառուս	38,04%
9	Ալժիր	37,11%
10	Վիետնամ	36,77%
14	Հայաստան	33,01%

Իրավիճակի ուսումնասիրությունը թույլ է տալիս ասել, որ այն պահանջում է անհապաղ գործողություններ ազգային մակարդակով: Խնդիրը միայն վտանգների քանակական աճը չէ, ոչ էլ ինտերնետից օգտվողների աճը, այլ նաև վտանգների որակական փոփոխությունը, ինչը պահանջում է պարբերաբար հանրային մակարդակով իրազեկում և նույնիսկ կրթում: Այսպես, աշխարհում տարածում են գտնում այսպես կոչված կրիպտովիրուսները: Դրանք այն վիրուսներն են, որոնք, ներթափանցելով համակարգիչ, կոդավորում են դրանում առկա ֆայլերն ու ապակոդավորման համար գումար պահանջում[1]: Տվյալ վիրուսների տեսակները կտրուկ աճ են գրանցում ողջ աշխարհում. եթե 2015թ. կրիպտովիրուսների միջոցով շորթված գումարի չափը գնահատվում էր մոտ $24 մլն, ապա 2016թ. այն արդեն հասավ $1 մլրդ-ի[2]:

Ընդհանուր վարակումների մեջ կրիպտովիրուսներն արդեն բավական մեծ տոկոս են կազմում: Հնդկաստանում, օրինակ, ամեն տասներորդ վարակված սարքը հենց կրիպտովիրուս է պարունակում[3] (տե՛ս *Նկար 1*).

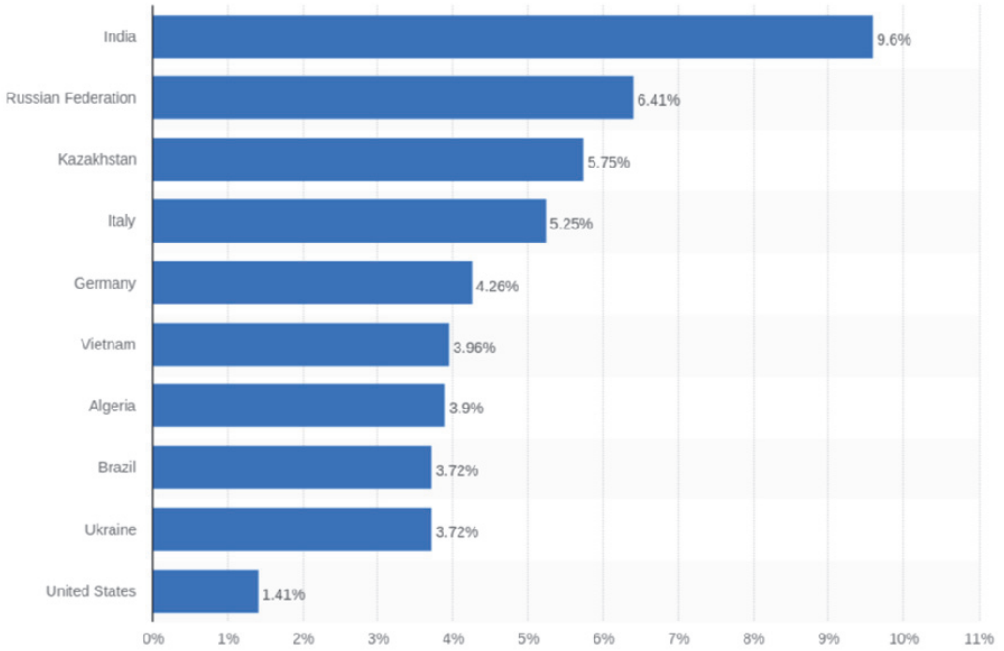
[1] Կրիպտովիրուսներ. տարածումը, կանխումն ու բուժումը, http://vavati.am/AM/news/6-Cryptoviruses.html

[2] Ransomware: Now a Billion Dollar a Year Crime and Growing, http://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646

[3] KSN Report: PC ransomware in 2014-2016, https://securelist.com/analysis/publications/75145/pc-ransomware-in-2014-2016/

Նկար 1

Կրիպտովիրուսներով վարակումը բոլոր վարակումների մեջ (%), 2015-2016թթ. տվյալներով: Տվյալները՝ Kaspersky Lab, պատկերը՝ Statista



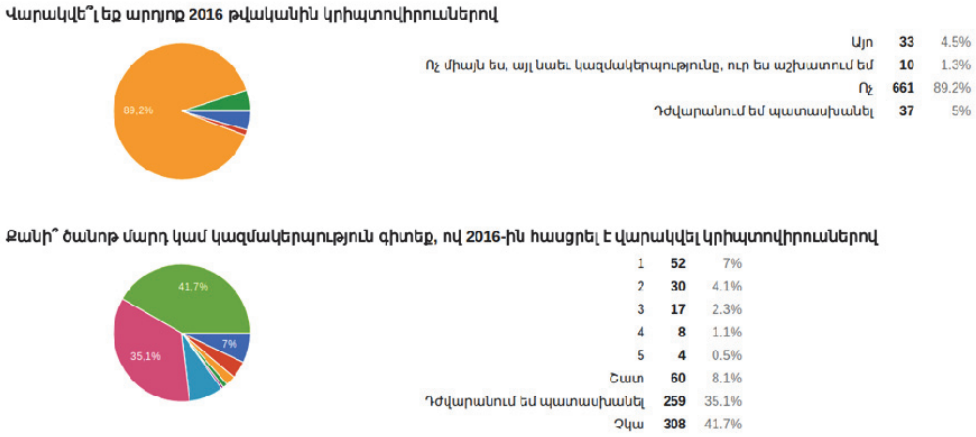
Հայաստանում իրավիճակը նույնպես մտահոգիչ է, սակայն քիչ ուսումնասիրված: Ըստ հեղինակի կողմից համացանցում իրականացված հարցման (իրականացվել է 2017թ. հունվարի 11-ին), Հայաստանում հարցման մասնակիցների 4,5%-ը դարձել է 2016թ. կրիպտովիրուսների զոհ, իսկ ևս 1,3%-ը ոչ միայն վարակվել է, այլ վարակման է ենթարկել նաև կազմակերպության համակարգիչը[1]: Բացի այդ, հարցման մասնակիցների 23%-ը տեղյակ է այլ անձանց կամ կազմակերպությունների մասին, որոնք հանդիսացել են կրիպտովիրուսների հարձակման զոհ (տե՛ս *Նկար 2*):

Նման վիճակագրությունները բավական մտահոգիչ են և նշանակում են, որ կիբեռհարձակումները ոչ միայն անձնական տվյալների արտահոսքի աղբյուր են, այլև սկսում են դառնալ նաև տնտեսական գործոն:

[1] Ինտերնետային հարցում Հայաստանում կրիպտովիրուսներով վարակումների մասին 2016թ. ընթացքում, https://docs.google.com/forms/d/e/1FAIpQLSdghL2HVSYnx7XI8jysmx4LOkEsmzuC1blmNJSMYRJbBn06sw/viewanalytics

Նկար 2

Ինտերնետային հարցում Հայաստանում կրիպտովիրուսներով վարակումների մասին 2016թ., տվյալներն՝ ըստ 744 հարցվողի



Հայ-ադրբեջանական հակամարտությունը՝ հասարակական գործոն. Ադրբեջանական հաքերային համայնքի հիմնական թիրախներից մեկը Հայաստանն ու հայերն են՝ անկախ բնակության վայրից: Հաքերային ամենամեծ ու ակտիվ խմբավորումը, որն արդեն 5 տարի գործում է, կոչվում է *Anti-Armenia Team*: Այս թիմն է հակահայկական կազմակերպված հաքերային հարձակումների հիմնական պատասխանատուն, չնայած պարբերաբար գործում են նաև նրանց հետ համագործակցող թուրքական խմբավորումներ[1]:

Ադրբեջանական հաքերները հիմնականում աշխատել և շարունակում են աշխատել հայկական կայքերը «կոտրելու» ուղղությամբ, ինչպես նաև պարբերաբար իրականացնում են DDoS տիպի հարձակումներ[2]: Սակայն 2016-2017թթ. ընթացքում նկատվում է ադրբեջանական հաքերների հարձակումների որակի փոփոխություն: Դեռ ապրիլյան պատերազմական գործողությունների ժամանակ նկատվեց, որ արդեն թիրախ են դառնում ոչ միայն կայքերը, ներքին ցանցերը, այլ նաև առանձին հայ օգտատերերը:

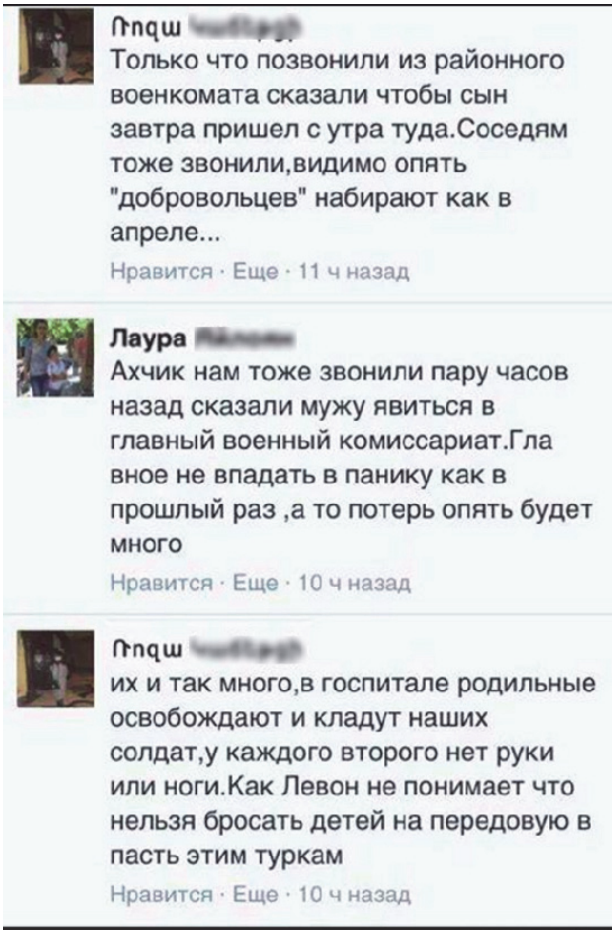
[1] Հայ-ադրբեջանական ապրիլյան պատերազմին ուղեկցող կիբեռհարձակումները, *Սամվել Մարտիրոսյան*, http://www.noravank.am/arm/articles/detail.php?ELEMENT_ID=14732&sphrase_id=59206

[2] DDOS հարձակումները Հայաստանի վրա դառնում են մտահոգիչ, *Սամվել Մարտիրոսյան*, http://www.noravank.am/arm/articles/detail.php?ELEMENT_ID=12704

2017թ. ադրբեջանցի հաքերները հայտարարեցին, որ իրենց հաջողվել է կոտրել հարյուրավոր հայկական ֆեյսբուքյան օգտատերերի[1]: Այդ օգտատերերի մուտքանունն ու գաղտնաբառերն էին հրապարակվել: Հետագայում անընդհատ հարձակումները հայկական օգտատերերի դեմ շարունակվում էին:

Նկար 3

Հայկական կոտրված ֆեյսբուքյան օգտատերերի կողմից տարածվող ապատեղեկատվության օրինակ



Եթե մինչև վերջերս օգտատերերի վրա հարձակումը հիմնականում հոգեբանական ճնշման միջոց էր, ապա վերջին զարգացումները ցույց են

[1] Facebook–ի էջերի ցանկ է ներկայացվել. ըստ ադրբեջանցի հաքերների, դրանք կոտրված են, http://newsarmenia.am/am/news/armenia/facebook-i-ejeri-cank-e-nerkayacvel-/

տալիս, որ դրանք օգտագործվում են նաև ապատեղեկատվություն տարածելու համար՝ որպես տեղեկատվական պատերազմի բաղադրիչ: Այսպես, 2017թ. փետրվարի 25-ի ադրբեջանական ձախողված դիվերսիոն գործողությունից հետո կոտրված ֆեյսբուքյան հաշիվներն օգտագործվում էին իբրև հայերի անունից ապատեղեկատվություն հայկական կողմի կորուստների վերաբերյալ տարածելու համար[1] (տե՛ս *Նկար 3*):

Հաշվի առնելով այն, որ ընդհանուր համակարգչային գրագիտությունը Հայաստանում բավական ցածր մակարդակի է, ադրբեջանական հաքերների (և ոչ միայն նրանց) համար հանրապետության բնակչության բավական լուրջ տոկոսը շարունակում է հարձակումների հեշտ թիրախ համարվել: Փաստացի, համակարգչային գրագիտություն չստացած հասարակության հատվածը դառնում է գործիք հակառակորդի տեղեկատվական գործողությունների համար, որոնք իրականացվում են հայաստանյան հասարակության դեմ ռազմական իրավիճակներում:

Համաշխարհային ներկա զարգացումները, որոնք տանում են դեպի հասարակությունների, պետությունների ավելի ու ավելի լայն թվայնացման, տեղեկատվական անվտանգության հարցերը դարձնում են առաջնայիններից մեկը: Կրիտիկական ենթակառուցվածքների վրա կիբեռհարձակումներն արդեն այսօր պետություններին լրջագույն հարված են հասցնում: Հայաստանը նման տեղեկատվական ագրեսիվ միջավայրում դիմակայելու համար պետք է կարողանա զարգանալ մարտահրավերներին համապատասխան, ունենա տեղեկատվական անվտանգության հստակ ռազմավարություն և մարտավարություն:

Մարտ, 2017թ.

ՀԱՅԱՍՏԱՆԻ ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ ԵՎ ԿՐԻՏԻԿԱԿԱՆ ԵՆԹԱԿԱՌՈՒՑՎԱԾՔՆԵՐԸ

Սամվել Մարտիրոսյան

Ամփոփագիր

Տեղեկատվական անվտանգության հետ կապված խնդիրներն այսօր լրջագույն մարտահրավեր են Հայաստանի համար: Մի շարք կրիտիկական ենթակառուցվածքներ կարող են կիբեռհարձակումների թիրախ դառնալ, ինչն էլ կարող է

[1] Ադրբեջանի ՊՆ-ն խոստովանել է 5 զինծառայողի կորուստ, http://razm.info/97043

ունենալ ազգային անվտանգության մակարդակի բացասական հետևանքներ: Նշված իրավիճակում Հայաստանը պետք է ունենա ավելի հստակ մոտեցումներ տեղեկատվական ավտանգության և կրիտիկական ենթակառուցվածքների պաշտպանության հարցերում:

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И КРИТИЧЕСКИЕ ИНФРАСТРУКТУРЫ АРМЕНИИ

Самвел Мартиросян

Резюме

Сегодня задачи информационной безопасности стали серьезным вызовом для Армении. Ряд критических инфраструктур может стать мишенью для кибератак, что может негативно сказаться на уровне национальной безопасности. В данной ситуации у Армении должны быть более четкие подходы в вопросах информационной безопасности и защиты критических инфраструктур.

INFORMATION SECURITY OF ARMENIA AND CRITICAL INFRASTRUCTURES

Samvel Martirosyan

Resume

The problems of information security are currently one of the most serious challenges for Armenia. A number of critical infrastructures may become targets for cyber-attacks, leaving negative impact on the level of the national security. Under such circumstances Armenia needs more clarity in approaches to the information security and protection of critical infrastructures.