ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԲՆԱԳԱՎԱՌՈՒՄ ԱՄՆ ՄԻՋԱԶԳԱՅԻՆ ՀԱՄԱԳՈՐԾԱԿՑՈՒԹՅԱՆ ՓՈՐՁԻՑ*

Հայկուհի Մկրտչյան

Բանալի բառեր՝ *տեղեկատվական անվտանգություն, տեղեկատվական սպառնալիքներ, միջազգային համագործակցություն, կիբեռտարածություն, կիբեռհանցագործություն:*

20-րդ դարի երկրորդ կեսին տեղեկատվության ծավալն ու նշանակությունն ակնհայտորեն աճեցին: Տեղեկատվությունն սկսեց մեծ դեր խաղալ մարդկային կենսագործունեության բոլոր բնագավառներում: Այդ է վկայում նաև այն հանգամանքը, որ հաճախ զանգվածային լրատվամիջոցներն անվանվում են չորրորդ իշխանություն՝ օրենսդիր, գործադիր և դատական իշխանությունների կողքին: Պատահական չէ նաև այսօր լայն կիրառում ստացած «ով տիրապետում է տեղեկատվությանը, նա տիրում է աշխարհին» արտահայտությունը: Ավելին՝ 1994 թվականից սկսած՝ Տեղեկատվության միջազգային ակադեմիայի նախաձեռնությամբ նոյեմբերի 26-ը աշխարհի շատ երկրներում նշվում է որպես տեղեկատվության համաշխարհային օր:

Տեղեկատվության դերի ու ծավալի աճի պայմաններում, ինչպես նաև տեղեկատվական տեխնոլոգիաների զարգացմանը զուգահեռ բարդացել են նաև տեղեկատվական անվտանգության սպառնալիքները: Ավելին՝ միջազգային անվտանգության օրակարգ են ներթափանցել անհամաչափ սպառնալիքները և դրանց հիմնական աղբյուր հանդիսացող ահաբեկչական խմբավորումներն ու անդրազգային հանցավոր խմբերը [1]: Ուստի տեղեկատվության պաշտպանությունը դարձել է շատ պետությունների ներքին ու արտաքին քաղաքականության առաջատար ուղղություններից մեկը:

Գլոբալացման արդյունքում ձևավորված համաշխարհային նոր քաղաքական համակարգի առաջնային դիրքերում ոչ թե ռազմական կամ տնտեսական ներուժ ունեցող երկրներն են, այլ նրանք, որոնք կարողանում են տնտեսական ներուժն օգտագործել սեփական ազդեցության գոտիների ընդլայնման և դրա անքակտելի բաղադրիչը հանդիսացող տեղեկատվական քաղաքականության մշակման և իրականացման գործում:

Այժմ անդրադառնանք տեղեկատվական անվտանգության ապահովման ոլորտում աշխարհի առաջատար երկրներից մեկին՝ ԱՄՆ-ին:

ԱՄՆ-ն իրավամբ համարվում է տեղեկատվական անվտանգության քաղաքականության մշակման առաջին երկրներից: Դեռևս 1990-ական թվականների կեսերին ամերիկյան կառավարությունն սկսել է ուշադրություն դարձնել տեղեկատվական տեխնոլոգիաների միջոցով իրականացվող հանցագործություններին: Ամերիկյան փորձագետները նշում էին, որ կիբեռահաբեկչությունն ու կիբեռհանցագործությունները բավականին լուրջ մարտահրավերներ են երկրի համար:

Տեղեկատվական անվտանգության ապահովման խնդիրը հատկապես կարևոր է հենց ԱՄՆ-ի համար, որտեղ առաջին անգամ զգացվել է տեղեկատվական հեղաշրջման ազդեցությունը: Այստեղ են ի հայտ եկել առաջին համակարգիչները: ԱՄՆ-ում է, որ տեղեկատվական-հաղորդակցային տեխնոլոգիաները դիտվել են որպես ռազմավարական ռեսուրս: Դրանք բավականին զարգացել ու ներդրվել են հասարակության ու պետության կենսագործունեության գրեթե բոլոր ոլորտներում:

---

* Հոդվածն ընդունվել է 03.09.19:
Հոդվածը տպագրության է երաշխավորել ԵՊՀ քաղաքական ինստիտուտների և գործընթացների ամբիոնի վարիչ, ք.գ.դ., պրոֆեսոր Գ. Քեռյանը: 27. 09. 19:

Ի դեպ, Ռազմավարական և միջազգային հետազոտությունների կենտրոնը նշում է ոլորտում «ճիշտ» մարդիկ ունենալու անհրաժեշտությունը՝ կիբեռանվտանգության հուսալի ու պատշաճ ռազմավարություն ունենալու համար: Դրա համար, ըստ Էվանսի և Ռիդերի, անհրաժեշտ են հետևյալ չորս տարրերը՝

- *Խթանել և ֆինանսավորել դպրոցներում ավելի ճշգրիտ ուսումնական ծրագրերի մշակումը,*
- *Աջակցել մասնագետների այնպիսի տեխնիկապես խստապահանջ հավաստագրման մշակմանը և ընդունմանը, որը ներառի հաստատուն կրթական և վերահսկելի գործնական բաղադրատարրեր,*
- *Պետական համակարգեր կառուցող, գործարկող և պաշտպանող մարդկանց տեխնիկական պատրաստականության մակարդակը բարձրացնելու համար կիրառել աշխատանքի ընդունման գործընթացի, գիտելիքների ձեռքբերման պրոցեսի և ուսումնավարժեցման ռեսուրսների համակցությունը,*
- *Բարձր մակարդակի տեխնիկական հմտություններ ունեցողներին խրախուսելու և պահելու նպատակով երաշխավորել նրանց պաշտոնական առաջխաղացումը, ինչպես այլ բնագավառներում է, օրինակ՝ քաղաքացիական շինարարության կամ բժշկության ոլորտներում [2]:*

Թեպետ տեղեկատվական անվտանգության ապահովման համար 1990-ական թվականներից ի վեր ընդունվել են մի շարք փաստաթղթեր, սակայն ոլորտում միջազգային համագործակցության տեսանկյունից հատկանշական է 2009թ-ի մայիսին պատրաստված «Կիբեռտարածությունում քաղաքականության ակնարկ» փաստաթուղթը, որում առաջարկվում էին կիբեռանվտանգության ապահովման համակարգի հետագա քայլերը: Ընդհանուր առմամբ, վերջինս 2008թ-ի Կիբեռանվտանգության ազգային համալիր նախաձեռնության[3] լրացումն էր: Վերջինս կիբեռանվտանգության հարցերի հետ կապված մի շարք խնդիրներ էր լուծում, մասնավորապես՝

- *«Պաշտպանական գծի» ստեղծում՝ ամերիկյան տվյալների բազայի վրա հնարավոր հակառակորդների կողմից գրոհներից պաշտպանելու համար, ինչպես նաև դաշնային կառավարության մասնագետների համար պայմաններ ստեղծել ազգային համակարգչային ցանցերի կախվածության մասին տեղեկացվածության ապահովման համար,*
- *ԱՄՆ հակահետախուզական մարմինների տեխնիկական ու օպերատիվ հնարավորությունների ընդլայնման հաշվին տեղեկատվության պաշտպանության ապահովում հնարավոր սպառնալիքների բոլոր ոլորտներում,*
- *Տեղեկատվական անվտանգության ոլորտում մասնագետների պատրաստման համար համալիր միջոցառումների իրականացում, ոլորտում հետազոտությունների իրականացում ու մշակում, ինչպես նաև ռազմավարական մոտեցումների մշակում՝ ԱՄՆ կիբեռտարածության մեջ իրականացվող չարամիտ գործողություններին արդյունավետ հակազդելու համար [4] :*

Իսկ արդեն 2009թ-ի «Կիբեռտարածությունում քաղաքականության ակնարկ» փաստաթղթի հիմնական բնութագրական հանգամանքն այն էր, որ ԱՄՆ-ը, մեծապես կախված լինելով ցանցերից, միայնակ չի կարող ապահովել կիբեռանվտանգությունը: Անհրաժեշտ է համագործակցել հատկապես այն երկրների հետ, որոնք խնդիրի լուծման ժամանակ նմանատիպ մոտեցումներ ունեն, կիսում են ԱՄՆ մոտեցումը կիբեռտարածության անվտանգության ապահովման ժամանակ տեխնիկական չափորոշիչների, ազգային օրենսդրության հարցերը շոշափող ընդունելի իրավական նորմերի, ինչպես նաև կիբեռհանցագործությունների և կիբեռհարձակումներին ի պատասխան գործողությունների կազմակերպման ժամանակ օրենսդրական բազայի մշակման հարցերում:

Ավելին՝ կիբեռտարածությունում անվտանգության ապահովման հարցերի հետ կապված համագործակցությունը օտարերկրյա գործընկերներ հետ աշխուժանցելու նպատակով 2011թ-ի մայիսին ԱՄՆ-ում մշակվեց և հրապարակվեց «Կիբեռտարածության միջազգային ռազմավարությունը», որտեղ ձևակերպված էին գլոբալ մակարդակում ԱՄՆ կիբեռանվտանգության ապահովման հիմնական մոտեցումները, որի համար կարող էին կիրառվել ազդեցության բոլոր հնարավոր միջոցները՝ դիվանագիտական, ռազմական, տնտեսական[5]:

Ռազմավարության համաձայն, ԱՄՆ հիմնական խնդիրը բաց, փոխգործակցող, անվտանգ ու հուսալի տեղեկատվական ու հաղորդակցային ենթակառուցվածքի ստեղծումն է, որի նպատակով անհրաժեշտ է տեղեկատվական և հաղորդակցային տեխնոլոգիաների համար բազմակողմ փոխհամաձայնեցված միջազգային չափորոշիչների մշակում ու ընդունում[6]:

Կիբեռտարածության միջազգային ռազմավարությունը որակապես նոր ծրագրային փաստաթուղթ է և տարբերվում է այդ բնագավառում գոյություն ունեցած բոլոր նախորդ փաստաթղթերից: Մասնավորապես, եթե նախորդ փաստաթղթերում առաջնային էր դիտվում կրիտիկական կարևոր ենթակառուցվածքի պաշտպանությունը, ապա վերջինում հստակ նշվում էր, որ գոյություն ունի վնասակար տեղեկատվություն, որի ազդեցությունը պետության, հասարակության ու անհատի վրա կարող է ունենալ ամենաբացասական ազդեցությունը:

Փաստաթղթում նշվում է, որ ԱՄՆ հիմնական նպատակը առաջնորդության ապահովումն է խաղաղ ու կայուն կիբեռտարածության ստեղծման բազմակողմ գործընթացում: ԱՄՆ նպատակ ունի զարգացնել համագործակցությունը երկու ուղղություններով՝ միջպետական (երկկողմ ու բազմակողմ հիմքերով) և պետական-մասնավոր (ինտերնետ ծառայություն տրամադրողներ, ծրագրային ապահովումը մշակողներ, համակարգչային տեխնիկա արտադրողներ):

Երկկողմ համագործակցության համար ԱՄՆ-ը ուշադրություն է դարձնում Ռուսաստանի ու Չինաստանի հետ համագործակցության ընդլայնմանը, որտեղից գալիս էին տեղեկատվական հիմնական սպառնալիքները:

Ռուս-ամերիկյան համագործակցության առաջին փուլն սկսվել է Օբամայի կառավարման ժամանակ, երբ 2009թ-ի նոյեմբերին Ռուսաստանի Անվտանգության խորհրդի քարտուղարի՝ Վաշինգտոն կատարած այցի ժամանակ ԱՄՆ ազգային անվտանգության խորհրդի ներկայացուցիչները քննարկեցին ռուս-ամերիկյան հնարավոր պայմանագրի ստորագրումը՝ համացանցի զինաթափման վերաբերյալ: Երկու երկրների միջև համագործակցության իրական պայմանավորվածություն ձեռք է բերվել 2013թ-ի հունիսի 17-ին «Մեծ ութնյակի» գագաթնաժողովի շրջանակում կայացած հանդիպումների արդյունքում, որտեղ երկու երկրների նախագահները հանդես են եկել համագործակցության նոր ոլորտում վստահության ամրապնդման հայտարարությամբ: Ձեռք է բերվել պայմանավորվածություն՝ ռուս-ամերիկյան նախագահական հանձնաժողովի շրջանակում երկկողմ աշխատանքային խումբ ստեղծելու, որը կզբաղվի տեղեկատվական տեխնոլոգիաների կիրառման, ինչպես նաև միջազգային անվտանգության բնագավառում տեղեկատվական տեխնոլոգիաներից բխող սպառնալիքների հարցերով[7]:

Չինաստանի հետ համագործակցության հաստատման առաջին քայլերը դարձյալ կատարվել են 2013թ-ին, երբ երկու երկրների աշխատանքային խմբերը պայմանավորվել են կիբեռտարածությունում անվտանգության խնդիրների ապահովման, կիբեռշպիոնաժի և ինտելեկտուալ սեփականության հետ կապված հարցերի շուրջ[8]: Չնայած հարկ է նշել, որ ներկայումս տեղեկատվական անվտանգության ապահովման հարցերում Չինաստանի մոտեցումը էականորեն հակասում է համացանցում թափանցիկության ամերիկյան ընկալմանը[9]: Չինաստանում համացանցի վերահսկողության

նպատակը անցանկալի տեղեկատվության ներթափանցման կանխումն է երկիր, ինչպես նաև տեղեկատվության արտահոսքի կանխումը երկրի սահմաններից դուրս [10]::

Բացի Ռուսաստանի ու Չինաստանի հետ համագործակցելուց և ոլորտում երկկողմ համագործակցությունն ընդլայնելուց՝ ԱՄՆ-ը փորձում է ընդլայնել նաև բազմակողմ համագործակցությունը, որը հիմնականում կատարում է ՆԱՏՕ-ի, ԵԱՀԿ-ի և ԵՄ-ի շրջանակում:

ԱՄՆ-ը ՆԱՏՕ-ն դիտարկում է որպես տեղեկատվական օպերացիաների ու կիբեռպատերազմների իրականացման բնագավառում ամերիկյան ձեռքբերումների առաջխաղացման հարթակ: ՆԱՏՕ-ի նման ռազմական միավորումները և դրանց շրջանակում պետությունների միջև համագործակցությունը թույլ են տալիս ուժեղացնել համատեղ պոտենցիալը և կբարելավեն ԱՄՆ-ի հնարավորությունը՝ հակազդելու պետական ու ոչ պետական կառույցների գործողություններին:

Կիբեռպաշտպանության ապահովմանն ուղղված խնդիրներին ՆԱՏՕ-ի շրջանակում հատուկ ուշադրություն է դարձվել 2014թ-ին Ուելսի գագաթնաժողովի ժամանակ, որի ընթացքում ընդունվել է ՆԱՏՕ-ի նոր կիբեռքաղաքականությունը: Գագաթնաժողովի հայտարարության մեջ նշվում էր, որ Կիբեռպաշտպանությունը ՆԱՏՕ-ի առանցքային խնդիրներից է[11]:

Ընդհանուր առմամբ վերջին տարիներին ՆԱՏՕ-ն բավականին առաջ է անցել կիբեռանվտանգության հետ կապված հարցերում: Ընդ որում, հարկ է նշել, որ ԱՄՆ-ը միության կիբեռքաղաքականության մշակման ու կիրառման մեջ առաջատար դերակատարներից է:

Խնդրո առարկայի հետ կապված՝ ԱՄՆ-ն ակտիվորեն շարունակում է համագործակցությունը նաև «Մեծ ութնյակի» հետ, որի շրջանակում հատկանշական էր 2011թ-ի մայիսին ընդունված «Նորացված ընտրություն հանուն ազատության ու ժողովրդավարության»[12] փաստաթուղթը: Փաստաթղթում նշվում էր միջազգային համագործակցության անհրաժեշտությունը՝ կրիտիկական ռեսուրսների, տեղեկատվական-հաղորդակցային տեխնոլոգիաների, տեղեկատվական ենթակառուցվածքի պաշտպանություն ապահովելու, տեղեկատվական տեխնոլոգիաների կիրառմամբ իրականացվող ահաբեկչական ու հանցավոր գործողություններին հակազդելու համար:

Կիբեռանվտանգության հարցերի հետ կապված՝ ԱՄՆ-ը ակտիվորեն համագործակցում է նաև Եվրամիության, ԵԱՀԿ-ի հետ:

Տեղեկատվական անվտանգության ապահովման ամերիկյան փորձը ցույց է տալիս, որ ԱՄՆ տեղեկատվական անվտանգության և 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՝ հարկ է առանձնացել՝

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

ԱՄՆ օրինակը խոսուն է և ՀՀ համար կարող է ուսուցողական լինել տեղեկատվական անվտանգության կառուցակարգերի մշակման և անհրաժեշտ գործիքարանի հստակեցման հարցում: Մասնավորապես, անհրաժեշտ է լրամշակել ՀՀ տեղեկատվական անվտանգության հայեցակարգը՝ այն համապատասխանեցնելով ժամանակի ար-

դի պահանջներին, որում տեղեկատվական անվտանգությունը կդիտվի երկրի կրիտիկական ենթակառուցվածքների շարքին, առանձին բաժին կհատկացվի կիբեռանվտանգությանը[13]: ԱՄՆ օրինակը ուսուցողական կարող է լինել նաև ոլորտում միջազգային համագործակցության ընդլայնման տեսանկյունից, որը կարող է իրականացվել թե՛ երկկողմ, թե՛ բազմակողմ մասշտաբներով: Բացի այդ՝ անհրաժեշտ է բարձրացնել տեղեկատվական սպառնալիքների մասին հանրային իրազեկման մակարդակը, ինչը թույլ կտա խուսափել կամ ըստ արժանվույն արձագանքել տեղեկատվական տարածությունից բխող սպառնալիքներին: Հարկ է նաև կրթել հանրությանը, ինչի արդյունքում մեր երկիրը ոլորտում որակյալ մասնագետներ կունենա, ովքեր կարող են ոչ միայն պաշտպանողական, այլև անհրաժեշտության դեպքում հարձակողական միջոցառումներ իրականացնել:

Ավելին՝ անհրաժեշտ է հատուկ կարևորել տեղեկատվական անվտանգությունը հանրային անվտանգության ապահովման համատեքստում: Հանս Մորգենթաուն հասարակության բարոյահոգեբանական վիճակը համարում էր պետական հզորության կարևորագույն բաղադրիչներից մեկը: Ուստի այս շրջանակում կարևոր է հանրության բարոյահոգեբանական անվտանգության ապահովումը տեղեկատվական ներքին և արտաքին սպառնալիքներից:

ԾԱՆՈԹԱԳՐՈՒԹՅՈՒՆՆԵՐ

1. Панарин И.Н. Информационная война и геополитика. – М.: Поколение, 2006, стр 56.
2. Evans K., Reeder F.. A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters. Washington: CSIS, 2010.
3. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (issued on 29.05.2009) // The White House. URL: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_ fi nal.pdf (վերջին մուտքը՝ 15.10.2011թ):
4. The Comprehensive National Cybersecurity Initiative//The White House. (http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (վերջին մուտքը՝ 15.10.2015թ.)).
5. International Strategy for Cyberspace // White House. (http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Վերջին մուտքը՝ 15.10.2015թ.)):
6. Տե՛ս նույն տեղը, էջ 5:
7. О новой области сотрудничества в укреплении доверия. Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки. 17 июня 2013 г. (http://news.kremlin.ru/ref_notes/1479 (Վերջին մուտքը՝ 20.05.16թ.).
8. Farnsworth T. U.S., China Meet on Cybersecurity. (http://www.armscontrol.org/act/2013_09/US-China-Meet-on-Cybersecurity(Վերջին մուտքը՝ 20.05.17թ.).
9. Старкин С.В. Влияние геополитической среды на трансформацию контрразведывательной парадигмы спецслужб США // Вестник Брянского государственного университета. 2011. № 2. С. 130–134.
10. Манойло А.В. Культурно-цивилизационные модели и технологии психологического разрешения международных конфликтов//Право и политика.2008, N4. стр. 914-926.

11. Section 72. Wales Summit Declaration. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales. September 5, 2014.
12. Deauville G8 Declaration. Renewed Commitment for Freedom and Democracy. Section II. – P.6
13. Հարությունյան Գ., Կրիտիկական ենթակառուցվածքներն ու ազգային անվտանգությունը, Երևան, 2018. http://www.noravank.am/upload/pdf/CRITICAL_STRUCTURES_book.pdf (Վերջին մուտքը՝ 20.05.16թ.).

ԱՄՓՈՓԱԳԻՐ

Տեղեկատվական անվտանգության ապահովման բնագավառում ԱՄՆ միջազգային համագործակցության փորձից

Հայկուհի Մկրտչյան

Տեղեկատվության դերի ու ծավալի աճի պայմաններում, ինչպես նաև տեղեկատվական տեխնոլոգիաների զարգացմանը զուգահեռ բարդացել են նաև տեղեկատվական անվտանգության սպառնալիքները: Ոխստի տեղեկատվության պաշտպանությունը դարձել է շատ պետությունների ներքին ու արտաքին քաղաքականության առաջատար ուղղություններից մեկը:

ԱՄՆ օրինակը խոսուն է և կարող է ուսուցողական լինել տեղեկատվական անվտանգության կառուցակարգերի մշակման հարցում: ԱՄՆ օրինակը ուսուցողական կարող է լինել նաև ոլորտում միջազգային համագործակցության ընդլայնման տեսանկյունից, որը կարող է իրականացվել թե՛ երկկողմ, թե՛ բազմակողմ մասշտաբներով:

РЕЗЮМЕ

Из опыта международного сотрудничества США в области информационной безопасности

Айкуи Мкртчян

Ключевые слова: информационная безопасность, информационные угрозы, международное сотрудничество, киберпространство, киберпреступления.

Учитывая возрастающую роль и объем информации, а также развитие информационных технологий, угрозы информационной безопасности также стали более значимыми. Защита информации стала одним из ведущих направлений внутренней и внешней политики многих государств.

Пример США является полезным для разработки систем информационной безопасности, а также может быть поучительным в расширении международного сотрудничества в этой области, которое может быть реализовано как в двустороннем, так и в многостороннем масштабе.

SUMMARY

From the USA International Cooperation Experience in the Field of Information Security

Haykuhi Mkrtchyan

Keywords: information security, information threats, international cooperation, cyberspace, cyber-attacks.

Considering the increasing role and volume of information, as well as the development of information technologies, information security threats have also become more complex. Information protection has become one of the leading domestic and foreign policy issues of many states.

The US example can be instructive in developing information security systems. The US example can also be instructive in expanding international cooperation in the field, which can be implemented on both a bilateral and multilateral scale.