ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԱՊԱՀՈՎՄԱՆ ԲՆԱԳԱՎԱՌՈՒՄ ԱՄՆ-Ի ԵՎ ՌԴ-Ի ՄԻՋԱԶԳԱՅԻՆ ՀԱՄԱԳՈՐԾԱԿՑՈՒԹՅԱՆ ՀԻՄՆԱԽՆԴԻՐՆԵՐԸ

ՀԱՅԿՈՒՀԻ ՄԿՐՏՉՅԱՆ

ԱՄՆ-ն տեղեկատվական անվտանգության քաղաքականություն մշակող առաջին երկրներից է: Դեռևս 1990-ական թվականների կեսերին ամերիկյան կառավարությունը սկսել է ուշադրություն դարձնել տեղեկատվական տեխնոլոգիաների միջոցով կատարվող հանցագործություններին: Ամերիկյան փորձագետները նշում էին, որ կիբեռահաբեկչությունն ու կիբեռհանցագործությունները բավականին լուրջ մարտահրավերներ են երկրի համար:

Թեպետ տեղեկատվական անվտանգության ապահովման վերաբերյալ 1990-ական թվականներից ի վեր ընդունվել են մի շարք փաստաթղթեր, սակայն ոլորտում միջազգային համագործակցության տեսանկյունից հատկանշական է 2009 թ. մայիսին պատրաստված «Կիբեռտարածությունում քաղաքականության ակնարկ»[1] փաստաթուղթը, որում առաջարկվում էին կիբեռանվտանգության ապահովման համակարգի հետագա քայլերը: Փաստաթղթի հիմնական բնութագրական կողմն այն էր, որ ԱՄՆ-ն միայնակ չի կարող ապահովել կիբեռանվտանգությունը: Անհրաժեշտ է համագործակցել հատկապես այն երկրների հետ, որոնք խնդրի լուծման ժամանակ նմանատիպ մոտեցումներ ունեն, կիսում են ԱՄՆ-ի մոտեցումը կիբեռտարածության անվտանգության ապահովման տեխնիկական չափորոշիչների, ազգային օրենսդրության ընդունելի իրավական նորմերի, ինչպես նաև կիբեռհանցագործություններին և կիբեռհարձակումներին ի պատասխան գործողությունների կազմակերպման ժամանակ օրենսդրական բազայի մշակման հարցերում: Ավելին, կիբեռտարածությունում անվտանգության ապահովման ոլորտում համագործակցությունը օտարերկրյա գործընկերների հետ աշխուժացնելու նպատակով 2011 թ. մայիսին ԱՄՆ-ում մշակվեց և հրապարակվեց «Կիբեռտարածության միջազգային ռազմավարությունը», որտեղ ձևակերպված էին երկրի կիբեռանվտանգության ապահովման համընդհանուր մոտեցումները և հակազդեցության բոլոր հնարավոր միջոցները՝ դիվանա-

[1] Տե՛ս «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՝ 15.10.2011):

գիտական, ռազմական, տնտեսական[2]:

Այդ ռազմավարության համաձայն՝ ԱՄՆ հիմնական խնդիրը տեղեկատվական ու հաղորդակցային բաց, փոխգործակցող, անվտանգ ու հուսալի ենթակառուցվածքի ստեղծումն էր, որի համար անհրաժեշտ էին տեղեկատվական և հաղորդակցային տեխնոլոգիաների՝ բազմակողմ փոխհամաձայնեցված միջազգային չափորոշիչների մշակում ու ընդունում[3]:

Կիբեռտարածության միջազգային ռազմավարությունը որակապես նոր ծրագրային փաստաթուղթ էր և տարբերվում էր բոլոր նախորդներից: Մասնավորապես, եթե նախորդ փաստաթղթերում առաջնային էր կրիտիկական կարևոր ենթակառուցվածքի պաշտպանությունը, ապա վերջինում հստակ նշվում էր, որ գոյություն ունի վնասակար տեղեկատվություն, որը պետության, հասարակության ու անհատի վրա կարող է ունենալ խիստ բացասական ազդեցություն:

Փաստաթղթում նշվում էր, որ ԱՄՆ-ի հիմնական նպատակը առաջնորդության ապահովումն է խաղաղ ու կայուն կիբեռտարածության ստեղծման բազմակողմ գործընթացում, որի նպատակն է 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-ն ուշադրություն էր դարձնում Ռուսաստանի ու Չինաստանի հետ համագործակցության ընդլայնմանը, որտեղից գալիս էին տեղեկատվական հիմնական սպառնալիքները:

Ռուս-ամերիկյան համագործակցության առաջին փուլը սկսվել է նախագահ Օբամայի կառավարման ժամանակ. 2009 թ. նոյեմբերին Ռուսաստանի անվտանգության խորհրդի քարտուղարի՝ Վաշինգտոն կատարած այցի ժամանակ ԱՄՆ ազգային անվտանգության խորհրդի ներկայացուցիչները քննարկել են համացանցի զինաթափման վերաբերյալ ռուս-ամերիկյան հնարավոր պայմանագրի ստորագրման հարցը: Երկու երկրների միջև համագործակցության իրական պայմանավորվածություն ձեռք է բերվել 2013 թ. հունիսի 17-ին «Մեծ ութնյակի» գագաթնաժողովի շրջանակում կայացած հանդիպումների ժամանակ, որտեղ ԱՄՆ և ՌԴ նախագահները հանդես են եկել նոր ոլորտում վստահությունն ամրապնդելու մասին հայտարարությամբ: Ձեռք է բերվել պայմանավորվածություն ռուս-ամերիկյան նախագահական հանձնաժողովի շրջանակում ստեղծելու երկկողմ աշխատանքային խումբ, որը կզբաղվի տեղեկատվական տեխնոլոգիաների կիրառման, ինչպես նաև միջազգային անվտանգության բնագավառում տեղեկատվական

[2] Տե՛ս «International Strategy for Cyberspace» // White House. (http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (վերջին մուտքը՝ 15.10.2015)):

[3] Տե՛ս նույն տեղը, էջ 5:

տեխնոլոգիաներից բխող սպառնալիքների հարցերով[4]:

Չինաստանի հետ համագործակցության առաջին քայլերը դարձյալ արվել են 2013թ., երբ երկու երկրների աշխատանքային խմբերը պայմանավորվել են կիբեռտարածությունում անվտանգության խնդիրներին, կիբեռլրտեսությանը և մտավոր սեփականությանը վերաբերող հարցերի շուրջ[5]: Սակայն հարկ է նշել, որ ներկայումս տեղեկատվական անվտանգության ապահովման հարցերում Չինաստանի մոտեցումը էականորեն հակասում է համացանցում թափանցիկության ամերիկյան ընկալմանը[6]: Չինաստանում համացանցի վերահսկողության նպատակը անցանկալի տեղեկատվության ներթափանցումը կանխելն է երկիր, ինչպես նաև տեղեկատվության արտահոսքը կանխելը երկրից:

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

ԱՄՆ-ն ՆԱՏՕ-ն դիտում է 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 ներուժը, որը կբարելավի ԱՄՆ-ի հնարավորությունը՝ հակազդելու պետական ու ոչ պետական կառույցների գործողություններին:

Կիբեռպաշտպանության ապահովմանն ուղղված խնդիրներին հատուկ ուշադրություն է դարձվել 2014 թ. Ուելսի գագաթնաժողովում, երբ ընդունվել է ՆԱՏՕ-ի նոր կիբեռքաղաքականությունը: Գագաթնաժողովի հայտարարության մեջ նշվում էր, որ կիբեռպաշտպանությունը ՆԱՏՕ-ի առանցքային խնդիրներից է[7]:

Ընդհանուր առմամբ, վերջին տարիներին ՆԱՏՕ-ն բավականին առաջ է անցել կիբեռանվտանգության ոլորտում: Ընդ որում, հարկ է նշել, որ ԱՄՆ-ն դաշինքի կիբեռքաղաքականության մշակման ու կիրառման մեջ առաջատարներից է: Նա ակտիվորեն շարունակում է համագործակցությունը նաև «Մեծ ութնյակի» հետ, որի շրջանակում հատկանշական էր 2011 թ. մայիսին ընդունված «Նորացված ընտրություն հա-

---

[4] Տե՛ս «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՝ 20.05.2016)):

[5] Տե՛ս **Farnsworth T**. «U.S., China Meet on Cybersecurity». (http://www.armscontrol.org/act/2013_09/US-China-Meet-on-Cybersecurity (վերջին մուտքը՝ 20.05.17)):

[6] Տե՛ս **Старкин С. В.** Влияние геополитической среды на трансформацию контрразведывательной парадигмы спецслужб США // Вестник Брянского государственного университета. 2011, № 2, էջ 130–134:

[7] Տե՛ս «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» (http://www.nato.int/cps/en/natohq/official_texts_112964.htm (Վերջին մուտքը՝ 11.09.16)):

նուն ազատության ու ժողովրդավարության»[8] փաստաթուղթը: Այստեղ նշվում էր միջազգային համագործակցության անհրաժեշտությունը՝ կրիտիկական ռեսուրսների, տեղեկատվական-հաղորդակցային տեխնոլոգիաների, տեղեկատվական ենթակառուցվածքի պաշտպանությունն ապահովելու, տեղեկատվական տեխնոլոգիաների կիրառմամբ իրականացվող ահաբեկչական ու հանցավոր գործողություններին հակազդելու համար:

Կիբեռանվտանգության հարցերով ԱՄՆ-ն ակտիվորեն համագործակցում է նաև Եվրամիության, ԵԱՀԿ-ի հետ: Իսկ տեղեկատվական անվտանգության ապահովման ոլորտում ՌԴ-ի հետ գործունեությունը հետևյալ հիմնական ուղղություններով է՝ երկկողմ համագործակցության, ՄԱԿ-ի և տարածաշրջանային կազմակերպությունների, մասնավորապես՝ Շանհայի համագործակցության կազմակերպության (ՇՀԿ) և Հավաքական անվտանգության պայմանագրի կազմակերպության հետ (ՀԱՊԿ): Ռուսաստանի Դաշնության պետական քաղաքականության խնդիրները, որոնք ամրագրված են «Միջազգային տեղեկատվական անվտանգության բնագավառում պետական քաղաքականության հիմքերը մինչև 2020 թ.»[9] փաստաթղթում, համահունչ են շատ երկրների՝ միջազգային համագործակցության ամրապնդման միջոցով տեղեկատվական սպառնալիքներին հակազդելու ձգտումներին:

Այս առումով ռուսական նախաձեռնությունների հիմնական հակառակորդը ԱՄՆ-ն է, որն առաջատար է տեղեկատվական-հաղորդակցային համակարգերի և տեղեկատվական զենք մշակելու ոլորտներում, որոնցում նպատակ է հետապնդում համաշխարհային առաջատարի դիրքերում մնալ: Երկու երկրների միջև համագործակցության իրական պայմանավորվածություն ձեռք է բերվել 2013 թ. հունիսի 17-ին, երբ երկրների ղեկավարները պայմանավորվեցին ռուս-ամերիկյան նախագահական հանձնաժողովի ձևաչափով երկկողմ աշխատանքային խումբ ստեղծել, որը կզբաղվի տեղեկատվական տեխնոլոգիաների կիրառման, ինչպես նաև միջազգային անվտանգության բնագավառում տեղեկատվական տեխնոլոգիաներից բխող սպառնալիքների հարցերով[10]:

ՌԴ-ն ակտիվորեն համագործակցում է նաև երկկողմ ձևաչափով: Հատկանշական են հատկապես ՌԴ-ի և Կուբայի Հանրապետության կառավարությունների միջև միջազգային տեղեկատվական անվտանգության ապահովման բնագավառում 2014 թ. Հավանայում ստորա-

[8] Տե՛ս «Deauville G8 Declaration. Renewed Commitment for Freedom and Democracy». Section II, էջ 6:

[9] Տե՛ս «Основы государственной политики в области международной информационной безопасности на период до 2020 года. Утверждены Президентом РФ 24 июля 2013 г.» (http://www.scrf.gov.ru/security/information/document114/, վերջին մուտքը՝ 06.08.2017):

[10] Տե՛ս «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՝ 20.05.16)):

գրված համաձայնագիրը[11], ՌԴ-ի և Բելառուսի Հանրապետության կառավարությունների միջև 2013 թ. Մոսկվայում ստորագրված համաձայնագիրը[12]: Նշված համաձայնագրերում տեղեկատվական անվտանգություն ասելով հասկացվում է անձի, հասարակության ու պետության շահերի պաշտպանվածությունը սպառնալիքներից, ապակառուցողական և տեղեկատվական տարածության մեջ այլ բացասական ազդեցությունից: Տեղեկատվական տարածությունն իր հերթին սահմանվում է որպես գործունեություն տեղեկատվության ստեղծման, մշակման, փոխանցման, օգտագործման, պահպանման ոլորտներում և ազդում է նաև անհատական ու հասարակական գիտակցության, տեղեկատվական ենթակառուցվածքի և հենց տեղեկատվության վրա:

ՄԱԿ-ում դեռևս 1998 թ. Ռուսաստանի նախաձեռնությամբ հարց էր բարձրացվել տեղեկատվական անվտանգության ապահովման մասին՝ դրանով իսկ խնդիրը միջազգային մակարդակ տեղափոխելով: ՌԴ-ն առաջարկել էր որոշումների փաթեթի նախագիծ, որով նպատակահարմար էր համարվում ոլորտի անվտանգության միջազգային-իրավական մեխանիզմների մշակումը: Հետագայում ՄԱԿ-ում ՌԴ-ն տարբեր նախագծերով է հանդես եկել, որոնց մի մասը անդամ երկրները քննադատության էին արժանացրել: Առարկությունները հիմնականում վերաբերում էին այն բանին, որ առաջարկվում էր արգելել համացանցի կիրառումը ռազմական քարոզչության և այլ երկրների ռեժիմները տապալելու նպատակներով[13]:

Հետագայում թեման պարբերաբար քննարկվել է կազմակերպության հանձնաժողովներում, ստեղծվել է կառավարական փորձագետների խումբ՝ միջազգային տեղեկատվական անվտանգության առավել կարևոր սպառնալիքներն ուսումնասիրելու ու դրանց գնահատական տալու համար, ինչպես նաև մշակելու հակազդման անհրաժեշտ միջոցառումներ: Սակայն, հաշվի առնելով այն հանգամանքը, որ ՄԱԿ-ի անդամ պետությունները տեղեկատվական անվտանգության ապահովման հարցում տարբեր, հաճախ իրարամերժ մոտեցումներ ունեն, ՄԱԿ-ի շրջանակում ՌԴ-ն լուրջ հաջողությունների չհասավ: Փոխարենը նա զգալի դեր խաղաց տարածաշրջանային կազմակերպությունների մակարդակով հիմնահարցի ապահովման կանոններ մշակելու գործում: Եթե ՆԱՏՕ-ում թելադրող դիրք ունի ԱՄՆ-ն, ապա ՀԱՊԿ-ում նման որոշիչ ձայն ունի Ռուսաստանը: Վերջին տարիներին ՀԱՊԿ-ում

---

[11] Տե՛ս «Соглашение между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности» (http://www.mid.ru/foreign_policy/international_contracts/2_contract/-/storage-viewer/bilateral/page-33/44171, վերջին մուտքը՝ 10.07.2017):

[12] Տե՛ս «Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности» (http://base.spinform.ru/show_doc.fwx?rgn=66855, 10.07.2017):

[13] Տե՛ս **Демидов О. В.** Проект доклада для сборника «Научные записки ПИР-центра» (http://www.pircenter.org/ kosdata/page_doc/p2713_1/pdf (վերջին մուտքը՝ 25.03.2017):

արդիական են դարձել միջազգային համագործակցության զարգացման խնդիրները՝ տեղեկատվական սպառնալիքներին և վտանգներին հավաքական ուժերով հակազդելու համար:

ՀԱՊԿ-ի գլխավոր քարտուղար Ն. Բորդյուժան «Նորարարական լուծումներ Ռուսաստանի անվտանգության համար» տասներորդ ազգային համաժողովում նշեց, որ կազմակերպությունը խիստ շահագրգիռ է նման սերտ համագործակցության և դրա արդյունքները գործնական կիրառելու համար, քանի որ ՀԱՊԿ-ի գլխավոր խնդիրն է հավաքական անվտանգության համակարգի կառուցումը, որը կհակազդի առկա բոլոր սպառնալիքներին և վտանգներին[14]:

Կազմակերպության շրջանակում փորձագետներն առանձնացնում են ռազմական համագործակցության հետևյալ մասնավոր ուղղությունները՝

- տեղեկատվական տարածության մշտադիտարկման մեխանիզմների ու մեթոդաբանության մշակում,
- միջազգային տեղեկատվական անվտանգության բնագավառում սպառնալիքներին հակազդելու համատեղ միջոցառումների մշակում և իրականացում,
- մեխանիզմների ստեղծում, որոնք կհամակարգեն կազմակերպության պատասխանատվության տակ գտնվող տարածաշրջանում տեղեկատվական անվտանգության ապահովմանը վերաբերող գործողությունները[15]:

ՌԴ-ի դիրքորոշումը զգալի նշանակություն ունի նաև Շանհայի համագործակցության կամակերպության (ՇՀԿ) մեջ՝ ի տարբերություն ՄԱԿ-ի:

Միջազգային տեղեկատվական անվտանգության ապահովման բնագավառում ՇՀԿ-ի անդամ պետությունների կառավարությունների միջև 2009 թ. Եկատերինբուրգում ստորագրված համաձայնագիրը ուժի մեջ է մտել 2011 թ. և կամավոր հիմունքներով ոլորտում սերտ համագործակցության հիմք է[16]:

Փաստաթղթի յուրահատկությունն այն է, որ միջազգային-իրավական մասշտաբով առաջին անգամ հստակ սահմանվել են տեղեկատվական անվտանգության սպառնալիքները, ինչպես նաև այդ բնագավառում կողմերի համագործակցության հիմնական ուղղությունները, սկզբունքները, ձևերն ու մեխանիզմները: Ի դեպ, չնայած տարածաշրջանային բնույթին, կազմակերպությանն անդամակցությունը բաց է

---

[14] Տե՛ս **Бордюжа Н. Н.** Приветствие участников Десятого национального форума. “Инновационные решения для безопасности России” (ИНФОРУМ-10), М., 31 января-1 февраля, 2008 (http://www.infoforum.ru/news/?p=591&n=1025, վերջին մուտքը՝ 13.06.2017):

[15] Տե՛ս «Международная информационная безопасность: проблемы и решения» / под общ. ред. С. А. Комова. М., 2011, кн. 1, էջ 113:

[16] Տե՛ս «О вступлении в силу Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности» (http://www.mid.ru/mezdunarodnaa-informacionnaa-bezopasnost/-/asset_publisher/UsCUTiw2pO53/content/id/203770, վերջին մուտքը՝ 10.05.2017):

նաև այլ պետությունների համար: Սա վկայում է նաև տեղեկատվական անվտանգության ապահովման միջազգային համընդգրկուն համակարգ ստեղծելու գաղափարի և սկզբունքների մասին: Ինչ վերաբերում է ոլորտում միջազգային համագործակցությանը, ապա ՌԴ-ն նույնպես հիմնահարցի արդյունավետ լուծման համար կարևորում է համագործակցության ընդլայնումը:

Մեր կարծիքով, 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): Արդյունավետ կարող է լինել նաև այնպիսի նորմատիվային փաստաթղթերի մշակումը, որոնք, բացի պաշտպանողական բնույթից, Ռուսաստանին նաև հարձակողական միջոցներով ոլորտում գերակա դիրք զբաղեցնելու հնարավորություն կտան:

Բանալի բառեր – *տեղեկատվական անվտանգություն, կիբեռտարածություն, կիբեռլրտեսություն, տեղեկատվական պատերազմ*

АЙКУИ МКРТЧЯН – *Проблемы международного сотрудничества США и РФ в области информационной безопасности.* – В области информационной безопасности обе страны придают большое значение расширению международного сотрудничества. Но если НАТО – платформа, где США имеют главенствующие позиции, то Россия активна в рамках ОДКБ и ШОС. Для неё может быть эффективным сотрудничество с государственными и частными компаниями (провайдерами интернет-услуг, разработчиками программного обеспечения, производителями компьютеров). Также было бы полезно разработать нормативные документы, которые позволят России занять лидирующие позиции в ряде сфер.

Ключевые слова: *информационная безопасность, киберпространство, кибершпионаж, информационная война*

HAYKUHI MKRTCHYAN – *Issues of International Cooperation of the USA and the Russian Federation in the Field of Information Security*. – In the field of information security, the USA and RF attach great importance to expanding international cooperation. The main platform for the United States is NATO, where it has a dictating position, Russia is active in the framework of the CSTO and the SCO. In our opinion, cooperation with state-owned private companies (Internet service providers, software developers, computer manufacturers) can also be effective for Russia. It may also be useful to develop regulatory documents that will not only be defensive but will also allow Russia to take a leading position in the offensive actions.

Key words: *information security, cyberspace, cyber espionage, information war*

Ներկայացվել է՝ 23.09.2019, Գրախոսվել է՝ 15.01.2020, Ընդունվել է տպագրության՝ 25.05.2020