«ՏԵՂԵԿԱՏՎԱԿԱՆ ԱՆՎՏԱՆԳՈՒԹՅՈՒՆ» ՀԱՍԿԱՑՈՒԹՅԱՆ ՋԱՐԳԱՑՈՒՄԸ

ՀԱՅԿՈՒՀԻ ՄԿՐՏՉՅԱՆ

20-րդ դարի կեսերին տեղեկատվության դերի ու ծավալի աճին, ինչպես նաև տեղեկատվական տեխնոլոգիաների զարգացմանը զուգահեռ՝ ավելացել են նաև տեղեկատվական անվտանգության սպառնալիքները, ուստի տեղեկատվության պաշտպանությունը դարձել է շատ պետությունների ներքին ու արտաքին քաղաքականության առաջնային ուղղություններից մեկը:

Հարկ է նկատել, որ համաշխարհայնացման նոր պայմաններում ի հայտ են գալիս անհամաչափ սպառնալիքներ, որոնք տեղեկատվական անվտանգության համար նոր մարտահրավերներ են ստեղծում: Նման սպառնալիքների դեմ մղվող պայքարում տեղեկատվական անվտանգությանը տրվում է կարևոր նշանակություն:

Եթե նախկինում գիտության ու քաղաքականության մեջ անվտանգությունն ընկալվում էր միայն ռազմական առումով, իսկ անվտանգության միջոցառումները «հոմանիշ» էին ռազմական գործողություններին, ապա ներկայումս առավելապես ուշադրություն է դարձվում հենց անվտանգության ոչ ռազմական կողմին: Այս պարագայում պետությունների ու միջազգային կազմակերպությունների համար հրամայական է դառնում կոլեկտիվ անվտանգության ապահովումը բոլոր՝ քաղաքական, տնտեսական, սոցիալական, էկոլոգիական, ռազմական ուղղություններում: Ընդ որում՝ երկրներն ըստ իրենց ռեժիմի բնույթի խնդիրը լուծում են տարբեր կերպ. մի մասը տեղեկատվական դաշտը փակում է՝ արգելելով նույնիսկ սոցիալական ցանցերի օգտագործումը, մյուսներն ավելի լիբերալ մեթոդներ են փնտրում:

Հարկ է նկատել, որ «տեղեկատվական անվտանգություն» հասկացության հստակ սահմանում մինչ օրս չկա, ավելին՝ եղածներն այնքան տարբեր են, որ երբեմն նույնիսկ հակասում են միմյանց: Հասկացության սահմանման բարդությունը առաջին հերթին հետևանք է այն բանի, որ այն շրջանառվում է տեղեկատվական հասարակության համատեքստում, որը դեռևս գտնվում է ձևավորման փուլում և կարիք ունի մանրամասն ուսումնասիրությունների: Նշենք, որ տեղեկատվական հասարակության ձևավորումը հնարավոր է դարձել քսաներորդ դարի երկրորդ կեսին՝ տեղեկատվական հեղափոխության շնորհիվ: Դա բացատրվում է որակապես նոր տեխնոլոգիաների առաջացմամբ ու արա-

գընթաց զարգացմամբ, ինչը մարդկությանը թույլ է տալիս ստեղծել, պահել, մշակել ու փոխանցել գրեթե ցանկացած ծավալի տեղեկատվություն՝ իրական ժամանակում:

Տեղեկատվական հասարակությունը սահմանվում է որպես հասարակական և արտադրական հարաբերությունների զարգացման վիճակ, որտեղ արտադրանքի հիմնական մասը արդյունք է ոչ թե նյութական արտադրության, այլ բարձր տեխնոլոգիաների՝ տեղեկատվական արտադրանք ստեղծելու և վաճառելու միջոցով, այսինքն՝ խոսքը քաղաքացիների մտավոր աշխատանքով ստեղծված արդյունքի մասին է[1]:

«Տեղեկատվական անվտանգություն» հասկացության սահմանման մյուս բարդությունը կապված է «տեղեկատվական անվտանգություն» երևույթի տարբեր հայեցակետերի՝ տեխնիկական, սոցիալական, հոգեբանական, քաղաքական և այլն ուսումնասիրության հետ, ուստի տարբեր է հասկացության ընկալումը սոցիոլոգների, փիլիսոփաների, հոգեբանների, քաղաքագետների կողմից:

Տեղեկատվական անվտանգության խնդրի մեկնաբանման քաղաքագիտական մոտեցումը առաջին հերթին կարևորում է տվյալ ոլորտում տարատեսակ սպառնալիքներին հակազդելու համար մասնավոր սեկտորի և պետական ինստիտուտների ջանքերի համախմբումը:

Տեղեկատվական անվտանգության ապահովման տեխնիկական մոտեցումը ենթադրում է առաջին հերթին մշակել կայքերի անվտանգության պահանջները, ինչպիսիք են՝ սերվերների պաշտպանությունը, լիցենզավորումը և այլն:

Ամփոփելով «տեղեկատվական անվտանգություն» հասկացության շուրջ արտահայտված տեսակետների քննությունը՝ Ա. Ա. Մալյուկը տարբերակում է երեք հիմնական մոտեցում[2].

- Էմպիրիկ, որը ենթադրում է տեղեկատվության նոր սպառնալիքներին անընդհատ հետևելու գործընթաց, նոր սպառնալիքներից պաշտպանական մեթոդների մշակում, նախորդ փորձի հիման վրա նոր մեթոդների ընտրություն,
- Հայեցակարգային-էմպիրիկ, որը փորձի հիման վրա պաշտպանության ընդհանուր հայեցակարգի ձևավորումն է, տեղեկատվության և դրա պաշտպանության արդյունավետ մեխանիզմները գնահատող մոտեցումների մշակումն ու գիտական հիմնավորումը,
- Տեսական-հայեցակարգային, որը ենթադրում է տեղեկատվության պաշտպանության հիմնական տեսությունների մշակում, պաշտպանության ռազմավարության հասկացության ներմուծում:

---

[1] Տե՛ս **Емельянов Г. В., Стрельцов А. А.** Проблемы обеспечения безопасности информационного общества // Распределенная конференция «Технологии информационного общества 98 – Россия» (http://www.iis.ru/events/19981130/streltsov.ru.html, վերջին մուտքը՝ 11.04.2017 թ.):

[2] Տե՛ս **Малюк А. А.** Информационная безопасность: концептуальные и методологические основы защиты информации. М., 2004, էջ 12-22:

Մեր կարծիքով, տեղեկատվական անվտանգության սահմանման այս մոտեցումները ուղղված են երևույթի միայն առանձին բաղկացուցիչների ուսումնասիրությանը, հստակ չեն և չեն արտահայտում հասկացության իրական բովանդակությունը:

Հիմնահարցով զբաղվող արտասահմանյան գործակալություններում «տեղեկատվական անվտանգությունը» դիտվում է որպես ընդհանուր անվտանգության առանձին բաժին այնպիսի հասկացությունների կողքին, ինչպիսիք են «համակարգչային անվտանգությունը», «ցանցի անվտանգությունը», «հեռահաղորդակցության անվտանգությունը», «տվյալների անվտանգությունը» և այլն:

Ուստի կարող ենք ասել, որ տեղեկատվական անվտանգությունը հասարակության տեղեկատվական միջավայրի պաշտպանվածությունն է և ավելի լայն հասկացություն է, քան միայն ցանցի կամ համակարգչի անվտանգությունը:

Տարբեր է հասկացության բովանդակությունը նաև անգլալեզու, ռուսերեն ու հայերեն գրականության մեջ, ինչպես նաև հայեցակարգային փաստաթղթերում:

Այսպես, անգլալեզու գրականության մեջ «տեղեկատվական անվտանգություն» (information security) հասկացությունը սահմանվում է որպես տեղեկատվության և աջակցող ենթակառուցվածքների պաշտպանվածություն բնական կամ արհեստական բնույթի պատահական կամ կանխամտածված ազդեցություններից, որոնք տեղեկատվական հարաբերությունների սուբյեկտներին, այդ թվում՝ տեղեկատվությունը տիրապետողին ու օգտագործողին, ինչպես նաև աջակցող ենթակառուցվածքին կարող են անուղղելի վնաս հասցնել: Հասկացության մեկ այլ սահմանմամբ՝ «Տեղեկատվական անվտանգությունը տեղեկույթի և տեղեկատվական համակարգերի՝ չարտոնված մուտքից, օգտագործումից, հրապարակումից, փոփոխակումից կամ ոչնչացումից պաշտպանությունն է, որպեսզի ապահովված լինեն գաղտնիությունը, ամբողջականությունը և մատչելիությունը»[3]: Այս իմաստով տեղեկատվական անվտանգության հոմանիշներն են «կիբեռանվտանգությունը» (Cybersecurity) և «համակարգչային անվտանգությունը» (Computer security):

Ռուսալեզու գրականության մեջ տեղեկատվական անվտանգության ժամանակակից խնդիրների սահմանման համար հիմք են հանդիսացել Ի. Ա. Լազարևի, Վ. Ն. Լոպատինի, Յու. Ս. Ուֆիմցևի, Ե. Ա. Երոֆեևի համակարգային հետազոտությունները:

Այսպես, Վ. Ն. Լոպատինը առանձնացնում է տեղեկատվական – հոգեբանական անվտանգությունը և այն սահմանում որպես վնասակար տեղեկատվության ազդեցությունից անհատի, հասարակության ու պետության կենսական կարևոր շահերի պաշտպանության իրավիճակ[4]:

[3] «Glossary of Key Information Security Terms». Ed. by Richard Kissel. National Institute of Standards and Technology, May 2013, p. 94.

[4] Տե՛ս **Лопатин В. Н.** Информационное право: Учебник. СПб., 2005, էջ 474:

Տ. Ա. Պոլյակովան տեղեկատվական անվտանգությունը դիտում է որպես Ռուսաստանի Դաշնության ազգային շահերի պաշտպանության վիճակ և դա համարում անհատի, հասարակության ու պետության հավասարակշռված շահերի ամբողջություն[5], ինչը համապատասխանում է պետության տեղեկատվական անվտանգության ռազմավարական հայեցակարգում ամրագրված՝ տեղեկատվության բնագավառում անվտանգության ապահովման սկզբունքին:

Ա. Դ. Ուրսուլը տեղեկատվական անվտանգությունը սահմանում է որպես տեղեկատվական վտանգավոր ազդեցություններից կենսագործունեության հիմնական բնագավառների պաշտպանության վիճակ[6]:

Ինչ վերաբերում է հայալեզու գրականությանը, նշենք, որ ՀՀ ՊՆ ԱՌՀԻ-ի՝ արևմտյան ու ռուսաստանյան պաշտպանական-անվտանգային տերմինաբանական-հասկացութային համակարգերի համադրմամբ կազմված եռալեզու բացատրական բառարանում տեղեկատվական անվտանգությունը բացատրվում է որպես «սուբյեկտի (անհատի, հասարակության) այն վիճակը, որի դեպքում տեղեկույթի և սուբյեկտի փոխազդեցության հետևանքով սուբյեկտի մեջ առաջացած փոփոխությունը սպառնալիք չի հարուցում նրա ֆիզիկական ու հոգեկան առողջության, ինչպես նաև հասարակության ու պետության համար»[7]:

Տեղեկատվական անվտանգության հիմնահարցի ուսումնասիրության երկու հիմնական ուղղություն կարելի է առանձնացնել: Առաջինի համաձայն՝ հասկացությունը կարելի է սահմանել որպես հենց տեղեկատվական ռեսուրսների՝ տեղեկատվության ու տեխնոլոգիաների անվտանգություն: Այս դեպքում տեղեկատվական անվտանգության ապահովման համար կարևոր են տեղեկատվական ենթակառուցվածքի անխափան գործունեության ապահովումը, այն կանխամտածված կամ պատահական ազդեցությունից պաշտպանելը: Այլ կերպ ասած՝ այս ուղղությունը հիմնականում շոշափում է տեխնիկական խնդիրները:

Երկրորդ ուղղությունն ավելի լայն է և ընդգրկում է ընդհանուր անվտանգության ապահովման համար տեղեկատվական ռեսուրսների դերը, դրանց կիրառման արդյունավետությունը: Փաստորեն, այս դեպքում ուշադրություն են դարձվում ազգային անվտանգության ապահովման ժամանակ տեղեկատվական ռեսուրսների դերին ու նշանակությանը:

Այսպիսով, տեղեկատվական անվտանգությունը ուսումնասիրվում է նեղ և լայն առումներով: Առաջին դեպքում շեշտը դրվում է դրա տեխնիկական բաղադրիչի վրա, իսկ մյուս պարագայում ընդգրկվում են տեղեկատվական անվտանգության բոլոր սուբյեկտները, այդ թվում՝

---

[5] Տե՛ս նույն տեղը:

[6] Տե՛ս **Урсул А. Д.** Информатизация общества и безопасность развития цивилизации // "Социально-политические науки", 1990, № 10:

[7] **Դ. Ս. Չիլինգարյան, Ե. Լ. Երզնկյան**, Պաշտպանական-անվտանգային տերմինների բացատրական հայերեն-ռուսերեն-անգլերեն, ռուսերեն-հայերեն, անգլերեն-հայերեն մեծ բառարան, Եր. 2015, էջ 76:

տեղեկատվություն փոխանցողը, ստացողը, առկա ենթակառուցվածքները: Մեր կարծիքով, տեղեկատվական անվտանգությանը վերաբերող հարցերի ուսումնասիրության ժամանակ հարկ է կիրառել թե՛ մեկ և թե՛ մյուս մոտեցումները:

Այժմ անդրադառնանք հասկացության բովանդակությանը հայեցակարգային փաստաթղթերի շրջանակում:

Այսպես, Ռուսաստանի Դաշնության՝ 2000 թ. ընդունված տեղեկատվական անվտանգության հայեցակարգում հասկացությունն օգտագործվում է լայն իմաստով և սահմանվում որպես տեղեկատվության բնագավառում ազգային շահերի ապահովության վիճակ, այսինքն՝ անհատի, հասարակության ու պետության հավասարակշռված շահերի ամբողջություն[8], որտեղ անհատի շահերը տեղեկատվական ոլորտում մարդու և քաղաքացու՝ օրենքով չարգելված գործունեություն իրականացնելու, ֆիզիկական, հոգևոր և մտավոր զարգացման համար օգտագործվող տեղեկատվության հասանելիության սահմանադրական իրավունքի իրագործումն են, ինչպես նաև՝ շրջակա միջավայրի փոփոխությունների վերաբերյալ տեղեկատվության հասանելիությունը և անձնական անվտանգությունն ապահովող տեղեկատվության պաշտպանությունը:

Հասարակության շահերը տեղեկատվական ոլորտում ներառում են անձի շահերի ապահովումը, ժողովրդավարության ամրապնդումը, իրավական-սոցիալական պետության կառուցումը, Ռուսաստանի հոգևոր վերարտադրությունը:

Պետության շահերն ընդգրկում են ռուսական տեղեկատվական դաշտի ձևավորման, նրա ենթակառուցվածքների ներդաշնակ գործառման և զարգացման, սահմանադրական կարգի, Ռուսաստանի ինքնիշխանության և տարածքային ամբողջականության անխախտելիության, քաղաքական, տնտեսական և սոցիալական կայունության, օրինականության և իրավակարգի ապահովման նպատակով անձի և քաղաքացու տեղեկատվություն ստանալու և օգտագործելու բնագավառում նրա սահմանադրական իրավունքների և ազատությունների իրականացման, ինչպես նաև հավասարազոր և փոխշահավետ միջազգային համագործակցության զարգացման համար անհրաժեշտ պայմանների ստեղծումը[9]:

Հայաստանի Հանրապետության նախագահի՝ 2009 թ. հաստատած տեղեկատվական անվտանգության հայեցակարգում տեղ է գտել 2000 թ. ՌԴ ընդունած հայեցակարգի համարյա նույն սահմանումը: Միայն հասարակության շահերը թվելիս գումարվում են հայ ինքնության հիմնասյուների՝ բարոյահոգեբանական կերտվածքի, հայոց լեզվի և Հայաստանյայց ա-

[8] Տե՛ս «Доктрина информационной безопасности Российской Федерации» (Утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., № Пр-1895, http://www.scrf.gov.ru/documents/5.html (վերջին մուտքը՝ 15.10.2011)):

[9] Տե՛ս նույն տեղը:

ռաքելական սուրբ եկեղեցու դերի ամրապնդումը, Հայաստան-Արցախ-Սփյուռք եռամիասնության տեղեկատվական կապի ապահովումը[10]:

ԱՄՆ նորմատիվային փաստաթղթերում մինչև 2001 թվականը «տեղեկատվական անվտանգություն» հասկացությունը շատ քիչ էր օգտագործվում: Կարևորվում էր «Համակարգչային անվտանգության վերաբերյալ»[11] օրենքի դերը, որի նպատակն էր նվազագույն գործողություններով ապահովել երկրի համակարգչային ցանցերում տեղեկատվության անվտանգությունը:

Արդեն 2002 թվականին ԱՄՆ-ում ընդունվեց օրենք «Տեղեկատվական անվտանգության կառավարման վերաբերյալ», որտեղ այն սահմանվում էր որպես՝

- անթույլատրելի մուտքից, օգտագործումից, բացահայտումից, տարածումից, ձևափոխումից կամ ոչնչացումից տեղեկատվության և տեղեկատվական համակարգերի պաշտպանություն,
- ոչ իրավական փոփոխությունից կամ ոչնչացումից տեղեկատվության ամբողջականության ապահովում,
- գաղտնիության ապահովում, որը նշանակում է տեղեկատվության հասանելիության ու տարածման սահմանափակումների ապահովում, այդ թվում՝ անձնական կյանքի և սեփականության տվյալների գաղտնիություն,
- հասանելիություն, որը նշանակում է արագ և հուսալի մուտք տեղեկատվական բազա[12]:

ԱՄՆ 2015 թ. «Ազգային անվտանգության ռազմավարության» մեջ տեղեկատվական անվտանգության հիշատակումը համապատասխանում է նրա նեղ իմաստին, այն է՝ կիբեռանվտանգությանը, որի առանձին բաժնում մասնավորապես նշվում է. «Որպես համացանցի ծննդավայր՝ Միացյալ Նահանգներն ունի ցանցային աշխարհին առաջնորդելու հատուկ պատասխանատվություն: Ավելի ու ավելի է աճում բարեկեցության ու անվտանգության կախումը բաց, համագործակցելի, պաշտպանված և հուսալի համացանցից…Հենվելով կիբեռանվտանգության կամավոր հայեցակարգի վրա՝ մենք պաշտպանում ենք դաշնության ցանցերն ու մասնավոր հատվածի, քաղաքացիական հասարակության և այլ շահագրգիռ կողմերի հետ աշխատում ամրապնդել ԱՄՆ համար կենսականորեն կարևոր ենթակառուցվածքի անվտանգությունն ու կայունությունը»[13]: Նույն փաստաթղթի «Արժեքներ» բաժինը նվիրված է ներքին և արտաքին տեղեկատվաքարոզչական աշխատանքին, հա-

[10] Տե՛ս «Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգ» (http://www.arlis.am/DocumentView.aspx?docID=52559, վերջին մուտքը՝ 20.02.2017 թ.):

[11] Տե՛ս «Computer Security Act of 1987», Public Law 100-235 (H.R. 145), January 8, 1988.

[12] Տե՛ս «The Federal Information Security Management Act of 2002»:

[13] «National Security Strategy». The White House, February 2015, էջ 12–13 (https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf, վերջին մուտքը՝ 14.05.2017 թ.):

մընդհանուր տեղեկատվական դաշտում ամերիկյան տեղեկատվական միջոցների ներկայացվածությանը, «փափուկ ուժի» մշտական գործարկմանը: Այստեղ արդեն տեղեկատվական անվտանգության խնդիրները քննարկվում են լայն իմաստով:

Փաստորեն, ԱՄՆ հիմնական նորմատիվային փաստաթղթերում տեղեկատվական անվտանգությունը ցանցի կամ համակարգի կարողությունն է՝ հակազդելու այն չարամիտ գործողություններին, որոնք կարող են խախտել տեղեկատվության հասանելիությունը, ամբողջականությունն ու գաղտնիությունը: Իսկ անվտանգության ապահովումը սահմանվում է որպես տեղեկատվության հասանելիություն, ամբողջականություն, գաղտնիություն:

Այսպիսով, եթե Հայաստանի Հանրապետության տեղեկատվական անվտանգության հայեցակարգում հստակ նշվում է, որ այն տեղեկատվության բնագավառում պետության ազգային շահերի պաշտպանության վիճակն է, որը բնութագրվում է անհատի, հասարակության ու պետության հավասարակշռված շահերի ամբողջությամբ, ապա ԱՄՆ-ում տեղեկատվական անվտանգությունը ցանցի կամ համակարգի կարողությունն է՝ հակազդելու այն չարամիտ գործողություններին, որոնք կարող են խախտել տեղեկատվության հասանելիությունը, ամբողջականությունն ու գաղտնիությունը:

Փաստորեն, ի սկզբանե «տեղեկատվական անվտանգություն» հասկացությունը օգտագործվում էր տեղեկատվական-հաղորդակցային տեխնոլոգիաների զարգացման համատեքստում՝ համակարգչային ցանցերի միջոցով ծագած խնդիրները վերհանելու նպատակով, իսկ հետագայում արդեն ավելի ընդգրկուն դարձավ՝ դուրս գալով բացառապես տեխնոլոգիական բնագավառին առնչվող շրջանակներից:

Մեր կարծիքով, անհրաժեշտ է տալ «տեղեկատվական անվտանգության» այնպիսի սահմանում, որը կընդգրկի հասկացության սահմանման և՛ լայն, և՛ նեղ մոտեցումները: Ուստի այդ տեսակետից ավելի ընդունելի ենք համարում Ե. Ա. Ռոգովսկու հետևյալ սահմանումը. ««Տեղեկատվական անվտանգությունը» տեղեկատվական տարածքում անհատի, հասարակության ու պետության շահերի պաշտպանության վիճակն է կանխամտածված կամ պատահական ազդեցություններից, որոնք խախտում են տեղեկատվության կամ տեղեկատվական-հաղորդակցային ենթակառուցվածքի ամբողջականությունը, օբյեկտիվությունը, հասանելիությունը, գաղտնիությունը»[14]:

Այսպիսով, ամփոփելով վերը ասվածը, կարող ենք եզրակացնել, որ «տեղեկատվական անվտանգություն» հասկացության հիմնական էությունը տեղեկատվության անվտանգությունը ապահովելն է՝ տեղեկատվական փոխազդեցության սուբյեկտների պաշտպանվածությունը

[14] **Роговский Е. А.** США: информационное общество. М., 2008, с. 396.

բացասական ազդեցությունից, սոցիալական սուբյեկտների տեղեկատվական պահանջմունքների բավարարումը: Այդ ամենին հասնել հնարավոր է նախևառաջ հասարակության ու դրա սուբյեկտների համար տեղեկատվական տեխնոլոգիաների կիրառման գործընթացում բացասական ազդեցության ուսումնասիրմամբ, որը կնպաստի դրանց վնասակար ազդեցության հաղթահարմանը և ապահով տեղեկատվական միջավայրի ձևավորմանը:

Բանալի բառեր – *տեղեկատվական անվտանգություն, տեղեկատվական սպառնալիքներ, տեղեկատվական տեխնոլոգիաներ, ԱՄՆ, ՌԴ*

АЙКУИ МКРТЧЯН – ***Эволюция понятия “информационная безопасность”.*** **–** В середине XX века в условиях роста роли и объёма информации, а также развития соответствующих технологий значительно усложнились угрозы информационной безопасности. Само восприятие информационной безопасности также изменилось**.** Если раньше это понятие применялось в контексте развития информационных и коммуникативных технологий для выявления проблем, возникающих через компьютерные сети, то сейчас оно стало поистине всеобъемлющим.

Ключевые слова: *информационная безопасность, информационные угрозы, информационные технологии, США, РФ*

HAYKUHI MKRTCHYAN – ***The Evolution of the Concept of “Information Security”.*** **–** In the middle of the 20th century, in the context of increasing role and volume of information, as well as the development of information technology, the threats to information security became much more complicated. As a result, the perception of information security has changed. If previously, the concept of "information security" was used in the context of the development of information and communication technologies to identify problems that arise through computer networks, now it has become more comprehensive, referring not only to the scope of technology.

Key words: *information security, information threats, information technologies, USA, RF*