ԿԻԲԵՐԱՆՎՏԱՆԳՈՒԹՅՈՒՆԸ՝ ԱԶԳԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԱՐԵՎՈՐԱԳՈՒՅՆ ԲԱՂԱԴՐԻՉ

Աղայան Նարինե
ՀՀ ԳԱԱ Փիլիսոփայության, սոցիոլոգիայի և իրավունքի ինստիտուտի կրտսեր գիտաշխատող

Տեղեկատվական և հաղորդակցական տեխնոլոգիաները (ՏՀՏ) աշխարհում զարգանում են սրընթաց արագությամբ: Դեռ չհարմարված առաջին ալիքին՝ անհրաժեշտություն է ծագում հետևելու և յուրացնելու հաջորդները՝ ժամանակի պահանջներից ետ չմնալու համար: Դրանց ազդեցությունը մեր ժամանակներում խիստ զգալի է քաղաքացիների, կազմակերպությունների և պետության գործունեության բոլոր հիմնական ոլորտների վրա: Համացանցի և կիբերտարածքի ընձեռած հնարավորությունները պետության քաղաքական, տնտեսական, պաշտպանական և այլ ոլորտների զարգացման լայն հեռանկարներ են ստեղծում: Սակայն, միևնույն ժամանակ կտրուկ մեծանում են վտանգները, սպառնալիքները վերոնշյալ և մյուս բոլոր ոլորտներում:

Կիբերտարածքի անդրսահմանային բնույթը, դրա կախվածությունը բարդ տեղեկատվական տեխնոլոգիաներից, վիրտուալ տարածքի հարթակների և ծառայությունների ակտիվ օգտագործումը քաղաքացիների զանազան խմբերի կողմից առաջացնում են նոր ռիսկեր անհատի, կազմակերպության, պետության շահերի ոտնահարման առումով[1]:

21-րդ դարում մարդկությունն առաջին անգամ բախվեց հանցագործության նոր՝ նախկինում անհայտ տեսակի՝ կիբերհանցագործության հետ: «Կիբերհանցագործությունը հիմնված է համացանցային էջերի կոտրման, վնասակար ծրագրերի և անօրինական տեղեկատվության տարածման վրա այն մարդկանց կամ խմբերի կողմից, ովքեր

[1] Տե՛ս **Даненьян А. А.** Международное правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 261 - 269:

հանցավոր գործունեություն են իրականացնում վիրտուալ տարածքում՝ օգտագործելով տեղեկատվական տեխնոլոգիաները»[2] :

Կիբերհանցավորության աճը աշխարհում վկայում է, որ կիբերսպառնալիքները համացանցում ավելի ու ավելի են մեծանում և իրապես լուրջ վտանգներ են պարունակում պետությունների ազգային անվտանգության համար[3]: Կիբերհարձակումների կատարելագործումը հետևում է տեղեկատվական տեխնոլոգիաների զարգացման արագ տեմպերին, ինչի արդյունքում կատարելագործվում են նմանատիպ հարձակումները և փոփոխվում են իրականացման եղանակներն ու միջոցները: Այն, որ նշյալ սպառնալիքները բնավ չափազանցված չեն, դրա ամենավառ ապացույցները տարբեր ինտերնետային ռեսուրսների, տեղային ցանցերի, տվյալների պահոցների և կառավարական կազմակերպությունների վրա հաքերային գրոհների աճող քանակն ու որակն են: Ըստ ՄԱԿ-ի մասնագետների՝ 2021 թվականի սկզբին կիբերհանցավորությունից տնտեսական վնասը հասել է 3 տրիլիոն դոլարի[4]:

Ներկայումս շուրջ 130 երկրներում գործում են ցանցահեների խմբեր, որոնք ամեն ամիս միլիոնավոր նոր վնասակար ծրագրեր են մշակում և տարեկան կատարում են մի քանի հարյուր միլիոն կիբերհարձակում[5]: Դրանց նպատակն է ֆինանսական – տնտեսական վնաս պատճառել «պայմանական հակառակորդներին»՝ մրցակից բիզնես կազմակերպություններին, կամ էլ ուղղակի անձնական շահույթ ստանալ:

Կիբերհանցավորության մասին Եվրոպայի խորհրդի կոնվենցիան (Հայաստանի Հանրապետությունում սույն կոնվենցիան ուժի մեջ է մտել 2007 թվականից) այն բաժանում է հինգ խմբի:

Առաջին խմբին դասվում են «համակարգչային հանցագործությունները»՝ ուղղված համակարգչային տվյալների ու համակարգերի գաղտնիության, ամբողջականության ու հասանելիության դեմ: Դրան-

---

[2] **Тимофеев А.В., Комолов А.А.** Киберпреступность как социальная угроза и объект правового регулирования, Вестник Московского государственного областного университета. Серия: Философские науки, 2021, № 1, с. 96. – с. 95-101.

[3] Տե՛ս **Աթոյան Վ.Կ.,** Ազգային անվտանգության հիմնախնդիրներ, Եր., 2014, 154 էջ:

[4] Տե՛ս Կիբերհանցավորություն (համակարգչային տեղեկությունների անվտանգության դեմ ուղղված հանցավորություն),
http://www.un.am/up/file/Crime%20Congress_Cybercrime_Arm_Final.pdf

[5] Ըստ Allianz Global Corporate & Specialty տվյալների, http://www.agcs.allianz.com/

ցից են՝ ապօրինաբար մուտք գործելը, ապօրինաբար տեղեկություններ ձեռք բերելը, տվյալներին միջամտելը, համակարգին միջամտելը և այլն:

Երկրորդ խմբում տեղ են գտել համակարգչային միջոցների գործադրմամբ հակաօրինական արարքները, որոնցից են՝ համակարգչային տեխնոլոգիաների կիրառությամբ զեղծարարությունները, տնտեսական շահ կորզելու նպատակով կատարվող խարդախությունները և այլն:

Երրորդ խումբը կազմում են բովանդակային ուղղվածության հետ կապված չարագործությունները, առաջին հերթին մանկական պոռնոգրաֆիայի քարոզչությունը:

Չորրորդը հեղինակային և այլ իրավունքների խախտումներն են:

Հինգերորդ խումբը ներառում է հետևյալ հանցագործությունները՝ ռասիստական և համանման բնույթի տեղեկատվության տարածումը, որը դրդում է բռնի գործողությունների, սերմանում ատելություն, խտրականություն որևէ անձի կամ անձանց խմբի նկատմամբ՝ հիմք ընդունելով նրանց ազգային, ռասայական, կրոնական պատկանելությունը[6]:

Կիբերհանցագործները օգտվում են երկրների օրենսդրական սողանցքներից և անվտանգությանն ուղղված միջոցառումների անբավարարությունից: Պարարտ հող է ստեղծում նաև համակարգչային գրագիտության և այսպես կոչված «համակարգչային հիգիենայի» անմխիթար վիճակը: Զարգացած և զարգացող երկրների միջև համագործակցության պակասը նույնպես նպաստավոր պայման է կիբերհանցագործների համար[7]:

Հաշվի առնելով այն, որ արդի աշխարհում քաղաքացիների, երկրների և պետությունների կենսագործունեության մեծ մասը կառավարվում է ցանցերի և ծրագրերի միջոցով, էականորեն բարձրացնում են դրանց խոցելիությունը կիբերհարձակումների նկատմամբ: Օրինակ՝ ներկայումս ՀՀ-ում լայնորեն ներդրված են էլեկտրոնային փաստաթղթաշրջանառության, բնակչության պետական ռեգիստրի,

[6] Տե՛ս Конвенция Совета Европы о киберпреступности, www.coe.int/t/DC/Files/Source/FS_cybercrime_ru.doc

[7] Տե՛ս Կիբերհանցավորություն (համակարգչային տեղեկությունների անվտանգության դեմ ուղղված հանցավորություն) http://www.un.am/up/file/Crime%20Congress_Cybercrime_Arm_Final.pdf

սոցիալական ապահովության ոլորտի, անշարժ գույքի գրանցման, հարկային հաշվետվությունների և մի շարք այլ համակարգեր, որոնց խափանումը կարող է հանգեցնել պետության կարևորագույն գործառույթների իրականացման ժամանակավոր արգելափակման, ինչն իր հերթին կհանգեցնի փոխկապակցված այլ ոլորտներում կաթվածահար վիճակի: Այս ամենը հղի է նաև երկրների ազգային անվտանգությանը սպառնացող վտանգներով, որոնց մեջ հենց կիբերհանցավորությունն է ծավալներով ամենամեծը: Այն անդրազգային հանցավորության ամենից արագ զարգացող տեսակներից է:

Աչքի առաջ ունենալով կիբերհանցավորության աճի միտումները՝ կասկածից դուրս է, որ կիբերանվտանգությունը կարևորագույն բաղադրիչ է դառնում ոչ միայն անձնական, այլև ազգային անվտանգության ապահովման համակարգում:

Հայաստանի պարագայում լուրջ վտանգ են ներկայացնում ոչ բարեկամական մի շարք երկրների, հատկապես Ադրբեջանի և Թուրքիայի հատուկ ծառայությունները: Արդյունքում՝ հազարավոր հայաստանցիներ և սփյուռքահայեր շարունակաբար տուժում են ադրբեջանա-թուրքական հաքերների գործողություններից:

Մասնավորապես, Հայաստանի և Ադրբեջանի միջև կիբերպատերազմները երկու տասնամյակի պատմություն ունեն:

Դրանք փոխադարձ բնույթ են կրել և ուղեկցվել կայքերի վրա հարձակումներով:

2016-ի Ապրիլյան քառօրյայի և դրան մերձակա օրերին կտրուկ սաստկացել են ադրբեջանական կիբերհարձակումները, ընդ որում, ի համերաշխություն նրանց, ակտիվացել են նաև թուրք հաքերները: Ի պատասխան ակտիվ են եղել հայ հաքերային խմբերը, մասնավորապես կոտրելով Ադրբեջանի կառավարության կայքը և հրապարակելով այդ երկրի զինված ուժերի 25 հազար զինծառայողի անհատական տվյալները:

Ապրիլյան պատերազմից հետո ընկած ժամանակահատվածում ադրբեջանական հաքերները ավելի շատ սկսել են թիրախավորել Ֆեյսբուքի հայկական օգտատերերին՝ կոտրելով պրոֆիլներ, էլեկտրոնային փոստեր և ֆեյսբուքյան հաշիվների մուտքային տվյալներ և այլն:

Ադրբեջանի հաքերային թիմերը կտրուկ ակտիվացել են 2020 թվականի ամառվանից, դեռ մինչև Տավուշի սահմանին ռազմական

բախումները (հուլիսի 12-16): Հունիսի և հուլիսի ընթացքում տասնյակ հազարավոր մարդկանց անձնական տվյալների արտահոսքեր են տեղի ունեցել ադրբեջանական հաքերային թիմերի կողմից թիրախավորված հարձակումների հետևանքով:

Նույն թվականի հուլիսի 14-ին ադրբեջանական հաքերները կիբերհարձակում են գործել gov.am, e-gov.am և primeminister.am պաշտոնական կայքերի վրա: Ի պատասխան՝ հայկական հաքերային թիմերից մեկը հարձակում է գործել և կոտրել Ադրբեջանի մոտ երկու հազար տնային տնտեսությունների և օֆիսների WiFi սարքեր, փոխել դրանց DNS կարգավորումները:

Արդեն Արցախյան 44-օրյա պատերազմի ընթացքում ադրբեջանական հաքերներին հաջողվել է կոտրել մի շարք պետական կայքեր, ինչպես նաև ներթափանցել պետական փաստաթղթերի շրջանառության համակարգ, տիրանալ մի շարք բարձրաստիճան պաշտոնյաների էլեկտրոնային փոստերին և այլն: Բացի դրանից, մի շարք լրատվամիջոցներ են կոտրվել, իսկ գրեթե ողջ լրատվական և պետական հատվածը գտնվում էր անընդհատ և ուժգին DDoS հարձակումների տակ[8]:

Խնդրի կարևորությունը հաշվի առնելով, ՀՀ-ում վերջին մեկուկես տասնամյակում որոշակի քայլեր կատարվել են:

Հայաստանի Հանրապետության Ազգային ժողովը 2007 թ. վավերացրել է «Կիբերհանցագործությունների մասին» Եվրախորհրդի կոնվենցիան և նույն կոնվենցիայի «Համակարգչային համակարգերի միջոցով կատարվող ռասիստական և քսենոֆոբիական բնույթի արարքների քրեականացման մասին» լրացուցիչ արձանագրությունը:

2009 թ. ընդունվել է ՀՀ տեղեկատվական անվտանգության հայեցակարգը[9], որում ձևակերպվել են Հայաստանի Հանրապետության տեղեկատվական անվտանգության սպառնալիքների տեսակները, որոնց շարքում է նաև կիբերահաբեկչությունը, և նշվել դրանց դիմակայելու առաջնահերթ միջոցառումներն ու դրանց իրականացման առաջնահերթությունները:

[8] Ոչ միայն վարչապետինը, https://armeniasputnik.am/society/ 20200714/23724247/Voch-miayn-varchapetiny-HH-um-petakan-vor-karuycneri-kayqern-en-kotrel-adrbejancinery.html

[9] Հայաստանի Հանրապետության ազգային անվտանգության ռազմավարություն, http://www.mfa.am/u_files/file/doctrine/Doctrinearm.pdf

Կիբերանվտանգության ապահովման նպատակ է հետապնդում նաև Հայաստանի Հանրապետությունում կազմակերպված հանցավորությունների դեմ պայքարի արդյունավետության բարձրացման ազգային ծրագիրը (2011թ.)[10]:

Հաշվի առնելով կիբերհանցավորության աճի միտումները՝ 2012թ. ընդունվել է Հայաստանի Հանրապետությունում ահաբեկչության դեմ պայքարի ազգային ռազմավարությունը[11]: Այստեղ կիբերահաբեկչությունը հստակորեն սահմանվել է որպես «ահաբեկչության տարատեսակ»:

Հետագա տարիներին ևս քայլեր են արվել այս ոլորտին վերաբերող ՀՀ օրենսդրությունը միջազգային իրավունքի պահանջներին, գործող կոնվենցիաներին համապատասխանեցնելու ուղղությամբ՝ գիտակցելով, որ տեղեկատվական ներգործության նորագույն միջոցների առաջացումն ու կիրառումը աշխարհում շարունակ նոր սպառնալիքներ են ծնում և հետագայում էլ կծնեն, ուստի պետք է դրանց արագ արձագանքելու տեսական, իրավական, օրենսդրական հիմքերը անընդհատ կատարելագործել:

Մշակվել է Տեղեկատվական անվտանգության ապահովման և տեղեկատվական քաղաքականության հայեցակարգի նախագիծը: Այն հավանության է արժանացել Ազգային անվտանգության խորհրդի 27.09.2017 թ. նիստում:

2017 թ. տարեվերջին (20.12.2017) **Հայաստանի Հանրապետության կառավարությունը մշակել է** Կիբերանվտանգության ռազմավարության նախագիծը և դրանից բխող միջոցառումների ժամանակացույցը[12]: Նման ռազմավարություններ ունեն բազմաթիվ երկրներ, քանի որ դրանց անհրաժեշտությունը բխում է ֆիզիկական և վիրտուալ տարածքներում ենթակառուցվածքների ապահով և հուսալի գործունեության անհրաժեշտությունից: Հաշվի առնելով աշխարհա-

[10] Տե՛ս Հայաստանի Հանրապետությունում կազմակերպված հանցավորության դեմ պայքարի արդյունավետության բարձրացման ազգային ծրագիր,
http:/www.arlis.am /documentview.aspx?docid=73264

[11] Տե՛ս «Հայաստանի Հանրապետությունում ահաբեկչության դեմ պայքարի ազգային ռազմավարություն»
http://www.arlis.am/DocumentView.aspx?DocID=75353

[12] ՀՀ կառավարության «Կիբերանվտանգության ռազմավարությունը հաստատելու մասին» արձանագրային որոշման նախագիծ,
https://www.e-draft.am/projects/581/about

քաղաքական ներկա զարգացումների արագությունն ու անկանխատեսելիությունը՝ անհրաժեշտ է լրամշակել և ընդունել վերոնշյալ օրինագիծը՝ սահմանելով ՀՀ ներքին և արտաքին քաղաքականության ոլորտում կիբերհանցավորության դեմ պայքարի առաջնահերթությունները, սկզբունքները և իրականացվելիք միջոցառումները:

Ներկայումս արդիական է նաև պետության հովանավորությամբ Կիբերանվտանգության ռազմավարական հետազոտությունների կենտրոն ստեղծելու հարցը, որտեղ գիտական-տեսական հետազոտությունների մակարդակով կմշակվեն կիբերհանցավորության դեմ պայքարի մեխանիզմներ, մոդելներ, որոնցից կօգտվեն թե՛ պետական գերատեսչությունները, թե՛ մասնավոր ընկերությունները: Ի դեպ, Կիբերանվտանգության ռազմավարության վերոնշյալ նախագծում այս մասին կա համապատասխան գլուխ (գլուխ V):

Կիբերհանցավորության դեմ պայքարը մարտահրավեր է ինչպես ամբողջ աշխարհում, այնպես էլ Հայաստանում: Այդ պայքարը հնարավոր չէ արդյունավետ կազմակերպել առանց որակյալ և բանիմաց հասարակության առկայության: Այս խնդրի լուծման լավագույն տարբերակը ոլորտի զարգացման համապատասխան կրթական ծրագրեր մշակելն ու իրականացնելն է, ինչպես նաև հանրային իրազեկման միջոցառումներ անցկացնելը:

ԱՄՓՈՓՈՒՄ

21-րդ դարում մարդկությունն առաջին անգամ բախվեց հանցագործության նոր տեսակի՝ կիբերհանցագործությանը: Կիբերտարածքի անդրսահմանային բնույթը, դրա կախվածությունը բարդ տեղեկատվական տեխնոլոգիաներից, վիրտուալ տարածքի հարթակների և ծառայությունների ակտիվ օգտագործումը քաղաքացիների զանազան խմբերի կողմից առաջացնում են նոր ռիսկեր անհատի, կազմակերպության, պետության շահերի ոտնահարման առումով:

Կիբերհանցավորության աճը աշխարհում վկայում է, որ կիբերսպառնալիքները համացանցում ավելանալու են և ավելի մեծ վտանգներ են ստեղծելու պետությունների, այդ թվում և մեր երկրի ազգային անվտանգության համար:

Հաշվի առնելով աշխարհաքաղաքական ներկա զարգացումների արագությունն ու անկանխատեսելիությունը՝ անհրաժեշտ է Հայաստանի Հանրապետությունում ունենալ կիբերանվտանգության ռազմա-

վարություն, որտեղ կսահմանվեն ներքին և արտաքին քաղաքականության ոլորտում առաջնահերթությունները, սկզբունքները և իրականացվելիք միջոցառումները:

Ներկայումս հրատապ է նաև պետության հովանավորությամբ Կիբերանվտանգության ռազմավարական հետազոտությունների կենտրոն ստեղծելու հարցը, որտեղ գիտատեսական հետազոտությունների մակարդակով կմշակվեն կիբերհանցավորության դեմ պայքարի մեխանիզմներ, մոդելներ, որոնցից կօգտվեն թե՛ պետական գերատեսչությունները, թե՛ մասնավոր ընկերությունները:

Բանալի բառեր. կիբերհանցագործություն, տեղեկատվական տեխնոլոգիաներ, տեղեկատվական անվտանգություն, կիբերահաբեկչություն, կիբերսպառնալիքներ, կիբերտարածք, կիբերանվտանգության ռազմավարություն:

КИБЕРБЕЗАПАСНОСТЬ - ВАЖНЕЙШИЙ КОМПОНЕНТ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Агаян Нарине
Младший научный сотрудник Института философии, социологии и права НАН РА

РЕЗЮМЕ

В 21 веке человечество впервые столкнулось с новым видом преступности – киберпреступностью. Трансграничный характер киберпространства, его зависимость от сложных информационных технологий, активное использование виртуальных платформ и сервисов различными группами граждан создают новые риски с точки зрения нарушения интересов личности, организаций и государств.

Рост киберпреступности в мире свидетельствует о том, что киберугрозы в Интернете будут усиливаться и создадут еще большие угрозы национальной безопасности государств.

Учитывая скорость и непредсказуемость текущих геополитических событий, необходимо иметь стратегию кибербезопасности в Республике Армения, где будут определены приоритеты, принципы и меры, реализуемые в области внутренней и внешней политики.

В настоящее время также актуален вопрос создания под эгидой государства центра стратегических исследований кибербезопасности, где на уровне научно-теоретических исследований будут разрабатываться механизмы и модели противодействия киберпреступности, которые будут использованы как государственными ведомствами , так и частными компаниями.

Ключевые слова: киберпреступности, информационные технологии, информационная безопасность, кибертерроризм, киберугрозы, кибеространство, стратегия кобербезопасности.

CYBER SECURITY IS THE MOST IMPORTANT COMPONENT OF NATIONAL SECURITY

Aghayan Narine
Junior Researcher of the Institute of Philosophy, Sociology and Law of NAS RA

SUMMARY

In the 21st century, humanity first encountered a new type of crime-cybercrime. Cross-border nature of cyberspace, its dependence on complex information technologies, the active use of virtual platforms and services by various groups of citizens creates new risks in terms of violating the interests of individuals, organizations and states. The growth of cybercrime in the world indicates that cyber threats on the Internet will increase and create even greater threats to the national security of states. Given the speed and unpredictability of surrent geopolitical events, it is necessary to have a cybersecurity strategy in the Republic of Armenia, which will define priorities, principles and measures implemented in the field of domestic and foreign policy. At present, the issue of creating a center for strategic research on cybersecurity under the auspices of the state is also relevant, where mechanisms and models for combating cybercrime will be developed at the level of scientific and theoretical research, which will be used by both government departments and private companies.

Key words: cybercrime, information technology, information security, cyberterrorism, cyber threats, cyberspace, cybersecurity strategy.