ԿԻԲԵՐՏԻՐՈՒԹ

Տեղեկատվական անվտանգություն և իրավունք

ԼՐԱԳՐՈՂՆԵՐ ՀԱՆՈՒՆ ԱՊԱԳԱՅԻ

«Կիբերտիրույթ. տեղեկատվական անվտանգություն եւ իրավունք» ձեռնարկը պատրաստվել եւ լույս է ընծայվել «Լրագրողներ հանուն ապագայի» ՀԿ կողմից «Ազատ, վստահելի եւ անվտանգ առցանց տեղեկատվություն բոլորի համար» ծրագրի շրջանակներում, որն իրականացվել է ԵԱՀԿ երեւանյան գրասենյակի ֆինանսական աջակցությամբ: Ձեռնարկում արտահայտված տեսակետները հեղինակներինն են, եւ պարտադիր չէ, որ արտահայտեն ԵԱՀԿ-ի կամ ԵԱՀԿ երևանյան գրասենյակի տեսակետները:

The handbook entitled “Cyberspace: Information Security and Rights” has been published by the Journalists for the Future NGO within the framework of the “Free, Reliable and Secure Internet Information for All” project supported by the Organization for Security and Co-operation in Europe Office in Yerevan. The views and conclusions expressed in the handbook are those of the authors and do not necessarily reflect the views of the OSCE or OSCE Office in Yerevan.

OSCE Organization for Security and Co-operation in Europe Office in Yerevan

ISBN 978-92-9235-102-1

«Կիբերտիրույթ. տեղեկատվական անվտանգություն եւ իրավունք» ձեռնարկը նախատեսված է տեղեկատվական անվտանգության ուղղությամբ մասնագիտացող ուսանողների, դասախոսների, իրավաբանների, լրագրողների, SS մասնագետների, իրավապաշտպանների եւ քաղաքացիական հասարակության ներկայացուցիչների համար: Այն կարող է հետաքրքրել նաեւ ընթերցողների լայն շրջանակներին: Ձեռնարկը տրամադրում է ե՛ւ տեսական, ե՛ւ գործնական գիտելիքներ կիբերտիրույթում տեղեկատվական անվտանգությունը պատշաճ ձեւով կազմակերպելու եւ սեփական իրավունքները ճանաչելու համար: Ձեռնարկի տպագիր տարբերակի օժանդակ մասը նրա էլեկտրոնային տարբերակն է՝ տեղադրված մեր էլեկտրոնային գրադարանում: Այն հնարավորություն է տալիս օգտվելու ձեռնարկում առկա հղումներից՝ դեպի հավելյալ էլեկտրոնային գրականություն: Ձեռնարկը բաղկացած է 7 մասից՝ գրված ոլորտի բարձրակարգ մասնագետների կողմից, որոնք անդրադառնում են կիբերտիրույթին վերաբերող ամենահաճախ բարձրացվող հարցերին:

“Cyberspace: Information Security and Rights” is a handbook intended for students specializing in journalism and information security, lecturers, lawyers, journalists, IT specialists, internet advocates as well as for CSO representatives. It may also interest a wide circle of readers. The handbook provides both with theoretical and practical knowledge on how to decently organize information security in cyberspace and to recognize one’s own rights. An auxiliary part of the handbook’s print version is its e-release posted on our e-library website. It consists of 7 parts, regarding the most frequently raised issues on cyberspace, prepared by experts of the field.

ՀԵՂԻՆԱԿՆԵՐԻ ՄԱՍԻՆ

Սուրեն Դեհերյան. նախագծի հեղինակ եւ տնօրեն, «Լրագրողներ հանուն ապագայի» ՀԿ նախագահ եւ Վրաստանի հանրային կապերի ինստիտուտի դասախոս: Մասնագիտական հետաքրքրությունների շրջանակն է՝ ԶԼՄ փոխակերպումը, համացանցում հայկական բովանդակության ստեղծումը, ժամանակակից տեխնոլոգիաների ազդեցությունը լրատվական հոսքերի կառավարման վրա եւ հեռարձակվող ԶԼՄ-ների թվայնացումը: «Լրագրության եւ զանգվածային հաղորդակցության կրթության ամերիկյան ընկերակցության» անդամ:

Արա Ղազարյան. «Արնի քնսալթ» փաստաբանական գրասենյակի եւ «Իրավունքի գերակայություն» հասարակական կազմակերպության հիմնադիր անդամ: Անդամակցում է տեղեկատվական վեճերի հարցերով զբաղվող Տեղեկատվական վեճերի խորհրդին եւ ԶԼՄ-ների էթիկայի հարցերով զբաղվող Դիտորդ մարմնին:

Սամվել Մարտիրոսյան. «Նորավանք» հիմնադրամի տեղեկատվական անվտանգության փորձագետ եւ iDitord.org կայքի տնօրեն: Դասավանդում է «Արեգնազան» կրթահամալիրում, Երեւանի պետական համալսարանի ժուռնալիստիկայի ֆակուլտետում եւ Երեւանի Վ. Բրյուսովի անվան պետական լեզվաբանական համալսարանի «Տեղեկատվության եւ հանրային հաղորդակցման տեխնոլոգիաների» գիտաուսումնական կենտրոնում: Մասնագիտական հետաքրքրությունների շրջանակը՝ տեղեկատվական անվտանգություն, սոցիալական մեդիա եւ առցանց լրատվություն: Անձնական կայք՝ Banman.am

Սարգիս Դարբինյան. իրավունքի մագիստրոս, ռուսական «Տրուևով, Այվար եւ գործընկերներ» փաստաբանական կոլեգիայի SS եւ IP ոլորտների փաստաբան, միեւնույն ժամանակ ակտիվ հասարակական գործիչ, Ռուսաստանի բնական գիտությունների ակադեմիայի իրավունքի հարցերով բաժանմունքի խորհրդական, «Համացանցից օգտվողների ասոցիացիայի» խորհրդի անդամ, «ՌոսԿոմՍվոբոդա» նախագծի իրավապաշտպան, «Ռուսաստանի ցանցահեների կուսակցության» անդամ, թվային տիրույթում հեղինակային իրավունքի իրավական կարգավորման փորձագետ, «Ժամանակն է փոխել հեղինակային իրավունքը» նախագծի ղեկավար, բլոգեր: Անձնական կայք՝ Dss-advokat.com

ԲՈՎԱՆԴԱԿՈՒԹՅՈՒՆ

ՆԱԽԱԲԱՆ

Սույն ձեռնարկով «Լրագրողներ հանուն ապագայի» (ԼՀԱ) ՀԿ նպատակն է մեկտեղել կիբերտիրույթին վերաբերող մեր փորձագետների դասախոսություններն ու 2014 թ. ընթացքում իրականացրած ուսումնասիրությունները: Հանձնելով այն ընթերցողի դատին՝ ցանկանում ենք, որ ձեռնարկը կիբերտիրույթին վերաբերող արդիական թեմաների քննարկման հիմք դառնա շահագրգիռ կողմերի շրջանում:

«Լրագրողներ հանուն ապագայի» կազմակերպությունը 2014 թ. ընթացքում կազմակերպել է նմանատիպ դասընթաց-քննարկումների շարք «Ազատ, վստահելի եւ անվտանգ առցանց տեղեկատվություն բոլորի համար» ծրագրի շրջանակներում, որի գլխավոր աջակիցն էր ԵԱՀԿ երեւանյան գրասենյակը: Ծրագրին աջակցել է նաեւ «Քաուսթերփարթ ինթերնեշնլի» հայաստանյան ներկայացուցչությունը:

Դասընթացներին մասնակցել են ՁԼՄ եւ քաղաքացիական հասարակության ավելի քան 60 ներկայացուցիչներ Երեւանից եւ Հայաստանի այլ մարզերից՝ տեղի ու միջազգային լավագույն մասնագետների օգնությամբ ծանոթանալով կիբերտիրույթում անվտանգությանը եւ իրավունքին վերաբերող հիմնարար խնդիրներին՝ այդպիսով բարձրացնելով ցանցային գրագիտության մակարդակը:

Նույն ծրագրի շրջանակներում ԼՀԱ-ն ստեղծել է «Համացանց եւ իրավունք» էլեկտրոնային տեղեկագիրը (տե՛ս www.jnews.am/internetrights), որտեղ կարելի է գտնել օգտակար նյութեր կիբերտիրույթի վերաբերյալ:

Բացի վերը նշված նախաձեռնություններից, ԼՀԱ-ն անցկացրել է նաեւ հարցում դասընթացներին մասնակցած լրագրողների եւ քաղաքացիական հասարակության ներկայացուցիչների շրջանում՝ որոշակի պատկերացում կազմելու Հայաստանում կիբերհանցագործության եւ տեղեկատվական անվտանգության կանոնների պահպանման վերաբերյալ: Հարցման արդյունքները ներառված են այս ձեռնարկում:

Այստեղ կարելի է ծանոթանալ նաեւ համացանցի կառավարման միջազգային սկզբունքներին, տեղեկանալ կիբերտիրույթում անձնական եւ ընտանեկան կյանքի իրավունքների մասին,

ուսումնասիրել կիբերհանցագործության իրավական կողմը, ընթերցել միջազգային կիբերհետապնդումներին եւ գաղտնալսումներին վերաբերող նյութեր, որտեղ անմասն չի մնում նաեւ Հայաստանը: Ձեռնարկի վերջին մասը համացանցի ռուսական տիրույթին առնչվող օրենսդրական եւ իրավական իրավիճակի մասին է՝ պատրաստված հատուկ այս ձեռնարկի համար: Ներկայացված է նյութի ռուսերեն բնօրինակը:

Սույն ձեռնարկում, ամփոփելով «Ազատ, վստահելի եւ անվտանգ առցանց տեղեկատվություն բոլորի համար» ծրագիրը, ընթերցողին հնարավորություն է տրվում անցնելու այն նույն ճանապարհով, որով անցել է ձեռնարկը հեղինակած անձնակազմը ողջ 2014 թ. ընթացքում:

Սուրեն Դեհերյան

«Լրագրողներ հանուն ապագայի» ՀԿ նախագահ

ՄԱՍ 1

ՀԱՄԱՅԱՆՑԻ ԿԱՌԱՎԱՐՄԱՆ ՄԻՋԱԶԳԱՅԻՆ ՍԿԶԲՈՒՆՔՆԵՐ

ՀԱՄԱՑԱՆՑԻ ԱԶԱՏՈՒԹՅՈՒՆ. ԻՆՉՈ՞Ւ Է ԱՅՆ ԿԱՐԵՎՈՐ

ԵԱՀԿ մամուլի ազատության հարցերով ներկայացուցչի հանձնարարականը

«Համացանցն առաջարկում է գաղափարների փոխանակման եւ տեղեկատվության ազատ հոսքի աննախադեպ հնարավորություն ամբողջ աշխարհում: Ժամանակակից տեղեկատվական հասարակությունում ազատ համացանցը նպաստում է ազատ արտահայտվելու հիմնարար իրավունքի եւ դրանից բխող ԶԼՄ-ների ազատության իրավունքի իրացմանը: 21-րդ դարում համացանցի հասանելիությունը, ինչպես նաեւ նրա բոլոր ծառայությունների գործածումը համարվում են մարդու իրավունք»,- նշված է ԵԱՀԿ մամուլի ազատության հարցերով ներկայացուցչի պաշտոնական էջում:

Համացանցը միավորում եւ լրացնում է ավանդական ԶԼՄ-ներին, ստեղծում տեղեկատվության փոխանակման նոր հնարավորություններ, որոնցից շատերի մասին մի քանի տարի առաջ հնարավոր չէր նույնիսկ պատկերացնել, իսկ շատերն էլ, որոնց մասին հնարավոր չէ պատկերացնել այսօր, դեռ ի հայտ են գալու:

Համացանցն աստիճանաբար դառնում է տեղեկատվություն ստանալու, փնտրելու եւ հաղորդելու ավելի անհրաժեշտ գործիք բոլորի համար:

Կառավարությունները պարտավորություն ունեն իրենց քաղաքացիներին թույլ տալու անարգել մուտք գործել համացանց: Ժողովրդավարական կառավարությունների պարտավորությունն է՝ մշակել օրենսդրություն եւ կանոնակարգեր, որոնք հնարավորություն կտան ունենալու անկախ եւ բազմակարծիք ԶԼՄ-ներ, տեղեկատվության ազատ հոսք առանց սահմանների, անարգել մուտք համացանց եւ ցանցային գրագիտության զարգացում:

ՀԱՄԱՑԱՆՑԻ ԿԱՌԱՎԱՐՈՒՄ

Կառավարությունները պետք է մեծ դերակատարում ունենան, երբ խոսքը ցանցային բովանդակության եւ երեխաների պաշտպանության, ռասիզմի դեմ պայքարի, ատելության եւ կիբերհանցագործության հրահրման մասին է: Հարցն այն չէ՝ արդյոք կառավարությունները պե՞տք է կարգավորեն համացանցը, թե՞ ոչ, այլ թե ինչպե՞ս, ի՞նչ եւ ի՞նչ ծավալով բովանդակություն պետք է կարգավորվի: Արդյոք պետական կարգավորումն արդյունավե՞տ է, եթե ոչ, ապա կա՞ն այնպիսի մեթոդներ, որոնք կարող են ավելի արդյունավետ լինել:

Համացանցի օգտագործման ցանկացած սահմանափակում օրինական է, եթե համապատասխանում է միջազգային նորմերին եւ չափանիշներին, որոնք անհրաժեշտ են ժողովրդավարական հասարակությանը եւ սահմանված են օրենքով: Պարտադիր զտումը եւ արգելափակումը համարվում են գերսահմանափակում:

ՄԱԿ-ի Համացանցի կառավարման ֆորումի, որում ընդգրկված են նաև քաղաքացիական հասարակության ներկայացուցիչներ, եւ որը հաշվի է առնում բոլոր շահագրգիռ կողմերի մասնակցությունը, որդեգրած մոտեցումը համացանցի կառավարման տեսանկյունից կարող է գործնական լավ օրինակ ծառայել ԵԱՀԿ տարածաշրջանի համար:

ԲԱԶՄԱԿԱՐԾՈՒԹՅՈՒՆ

Թվային լրատվամիջոցներն ավելի շատ են բազմազանության եւ բազմակարծության հնարավորություն տալիս, քան ավանդական-ները. հաճախականությունների կամ այլ ռեսուրսների սակավություն չի նկատվում: Համացանցը, այնուամենայնիվ, զերծ չէ գրաքննությունից եւ, ըստ էության, ազատ չէ իր բնույթով եւ կառուցվածքով:

Կառավարությունները պետք է հաշվի առնեն սա համացանցին վերաբերող այնպիսի օրենքներ ընդունելիս, որոնք, թեկուզ պատահական, բայց կողմնակի ազդեցություն կարող են ունենալ:

Այսօր միայն կառավարությունները չէ, որ ձեւավորում են ցանցային իրականությունը: Քաղաքացիական հասարակությունը, արդյունաբերությունը, մեդիա ընկերությունները, լրագրողները եւ բլոգերները, իրենց հասանելիք դերակատարմամբ, ձեւավորում են վաղվա համացանցը: Անհատների իրավունքների, ներառյալ ազատ արտահայտվելու իրավունքի դիտարկումը, պետք է լինի հավաքական պատասխանատվության մաս, միեւնույն ժամանակ օգտատերերի տվյալների գաղտնիությունն ու անհատական հաղորդակցությունները պետք է երաշխավորվեն կազմակերպությունների կողմից:

ՀԱՍԱՆԵԼԻՈՒԹՅՈՒՆ

ԵԱՀԿ մասնակից երկրները պետք է վստահեցնեն, որ համացանցը մնում է բաց եւ հանրային հարթակ՝ համահունչ ԵԱՀԿ ԶԼՄ-ների ազատությանը վերաբերող հանձնառություններին եւ ազատ արտահայտվելուն վերաբերող այլ միջազգային պայմանագրերին: Անհրաժեշտ է անխոչընդոտ, ոչ խտրական մուտք թվային ցանցեր եւ ծառայություններ, ինչպես նաեւ ցանցի չեզոքության ապահովում: Առցանց տեղեկատվությունը եւ թրաֆիկը պետք է մատուցվեն հավասարապես՝ անկախ սարքից, բովանդակությունից, հեղինակից, ծագումից եւ նշանակությունից:

ԵԱՀԿ ոչ բոլոր երկրներում է դեռեւս լայնաշերտ համացանցը մատչելի եւ հասանելի: Կառավարությունները պետք է միջոցներ ձեռնարկեն հաղթահարելու այս «թվային անհավասարությունը»՝ խթանելու մուտքը համացանց եւ վերացնելու խոչընդոտները բոլոր մակարդակներում՝ տեխնիկական, կառուցվածքային եւ կրթական:

Թեեւ երկրները հետաքրքրված են օրենսդրական պայքար մղելու ցանցահենության դեմ, օգտվողների համար համացանցի հասանելիության սահմանափակումը կամ արգելումը (երեք հարվածի մոտեցում) անհամաչափ պատասխան է, որն անհամատեղելի է ԵԱՀԿ հանձնառությունների հետ: Հանրային տիրույթի հասանելիությունը կարեւոր է ե՛ւ տեխնիկական, ե՛ւ մշակութային նորարարության համար եւ այն չպետք է վտանգվի արտոնագրին ու հեղինակային իրավունքին առնչվող ավելորդ դրույթների ընդունմամբ:

ՑԱՆՑԱՅԻՆ ԳՐԱԳԻՏՈՒԹՅՈՒՆ

Ցանցային գրագիտությունը մեդիա կրթության արդյունք է, որն օգտատերերին հնարավորություն է տալիս ողջամիտ որոշումներ կայացնելու համացանցի օգտագործման վերաբերյալ, գնահատելու առցանց տեղեկատվության ճշգրտությունն ու հնարավոր շեղումը եւ պաշտպանելու անչափահասներին հնարավոր վնասակար բովանդակությունից:

Մասնագետներն էական դեր ունեն ավանդական մեդիա կրթությունը ցանցային գրագիտությանը կամրջելու գործում, հատկապես որ հասարակությունը գնում է դեպի մեդիա հարթակների միավորում: Ոչ պաշտպանական մոտեցումը կարեւոր նշանակություն ունի ուսանողներին մեդիա գրագիտության ապահովման աշխատանքում ներգրավելու համար:

Երիտասարդությունը պետք է հզորացնի ցանցում սեփական գործողությունների մասին խելամիտ դատողություններ անելու կարողությունները: Կրթված ուղեղը լավագույն զտիչն է:

ՍՈՑԻԱԼԱԿԱՆ ՄԵԴԻԱ

Պաշտպանված չէ մեդիա ընկերությունների կամ խմբագրությունների ՁԼՄ-ների ազատության իրավունքը: Այս իրավունքը վերաբերում է հանրային տարածման համար նախատեսված լրագրության բոլոր տեսակներին՝ ինչպես պրոֆեսիոնալ, այնպես էլ՝ քաղաքացիական: Դա մարդու հիմնարար իրավունքն է եւ չի կարող բաժանվել ավանդական եւ նոր մեդիայի: Այսօրվա լուրը սոցիալական է: Սոցիալական մեդիան եւ սոցիալական ցանցերը փոխում են լուրի ստեղծման եւ տարածման ձեւը: Դրանք ազդում են ՁԼՄ-ների վրա երեք ձեւով. որպես բովանդակության ստեղծման, տեղեկատվության տարածման, հաղորդման եւ որոնման եւ որպես տեղեկատվության ստացման ու հասանելիության գործիք: Սոցիալական մեդիան եւ սոցիալական ցանցերը աստիճանաբար ավելի են նպաստում ՁԼՄ-ների ազատության եւ ազատ արտահայտվելու իրավունքների իրականացմանը:

«Չկա անվտանգություն առանց ազատ ԶԼՄ-ների եւ ազատ արտահայտվելու, եւ չկա ազատ արտահայտում եւ ազատ ԶԼՄ առանց անվտանգության: Այս երկու հասկացությունները պետք է ձեռք ձեռքի տված առաջ ընթանան եւ ոչ թե պայքարեն միմյանց դեմ, ինչպիսին ականատես ենք աշխարհի շատ վայրերում»,- ասել է ԵԱՀԿ մամուլի ազատության հարցերով ներկայացուցիչ Դունյա Միյատովիչը, ով այս պաշտոնին է 2010 թ.-ից:

«Անվտանգությունը եւ մարդու իրավունքները Հելսինկյան գործընթացի, Աստանայի գագաթնաժողովի, ինչպես նաեւ ԵԱՀԿ սկզբունքների ու հանձնառությունների հիմքում են: Համացանցն հրաշալի ռեսուրս է, որը հիմնովին փոխել է մեր հասարակությունները դեպի ավելի լավը: Այն կշարունակի դրական ազդեցություն ունենալ, եթե թույլ տանք: Դասը պարզ է՝ համացանցը պետք է մնա ազատ»:

Նյութի օժանդակ աղբյուրը ԵԱՀԿ պաշտոնական կայքն է՝ www.osce.org/fom

ՀԱՄԱՑԱՆՑԻ ԿԱՌԱՎԱՐՄԱՆ ՍԿԶԲՈՒՆՔՆԵՐԸ՝ ԸՍՏ ԵՎՐՈՊԱՅԻ ԽՈՐՀՐԴԻ ՆԱԽԱՐԱՐՆԵՐԻ ԿՈՄԻՏԵԻ

2003 թ. Ժնեւում եւ 2005 թ. Թունիսում տեղի ունեցած տեղեկատվական հասարակության համաշխարհային գագաթնաժողովների շնորհիվ աշխարհի ուշադրությունը բեւեռվեց դեպի «համացանցի կառավարում» եզրույթը: Տեղեկատվական հասարակությունը լիովին ներգրավված էր համացանցի կառավարման բանավեճում:

Համացանցի կառավարումը բարդ գործընթաց է, որն իրականացվում է բազմաթիվ շահագրգիռ կողմերի մասնակցությամբ՝ ընկերություններ, պետություններ, միջկառավարական կազմակերպություններ, քաղաքացիական հասարակության ներկայացուցիչներ (ներառյալ՝ տեխնիկական փորձագետներ): Նրանք համագործակցում են՝ իրենց ներդրումն ունենալով ընդհանուր քաղաքականություն եւ ստանդարտներ ստեղծելու գործում, որոնք կապահովեն համացանցի գլոբալ փոխգործունակությունը՝ հանուն հանրության բարօրության:

Ժնեւում տեղի ունեցած համաշխարհային գագաթնաժողովը ներկայացրեց սկզբունքներ տեղեկատվական հասարակության համար, ներառյալ համացանցի կառավարման սկզբունքը, որում ասվում էր. «Համացանցի միջազգային կառավարումը պետք է լինի բազմակողմ, թափանցիկ եւ ժողովրդավարական՝ կառավարությունների, մասնավոր հատվածի, քաղաքացիական հասարակության եւ միջազգային կազմա-կերպությունների լիակատար ներգրավվածությամբ»:

Թունիսի գագաթնաժողովում պետությունների ղեկավարները համաձայնության եկան համացանցի կառավարման հետևյալ սահմանման շուրջ. «Համացանցի կառավարումն ընդհանուր սկզբունքների, նորմերի, կանոնների, որոշումների կայացման ընթացակարգերի ու ծրագրերի մշակում եւ կիրառում է, որը ձեւավորվում է համացանցի զարգացմամբ եւ գործածմամբ»:

Իսկ 2011 թ. սեպտեմբերի 21-ին Եվրոպայի խորհրդի

նախարարների կոմիտեն ընդունեց համացանցի կառավարման սկզբունքների մասին ստորեւ ներկայացված 10 կետից բաղկացած հռչակագիրը:

1. Մարդու իրավունքներ, ժողովրդավարություն եւ օրենքի գերակայություն

Համաձայն մարդու միջազգային իրավունքների՝ համացանցի կառավարման կարգավորումները պետք է երաշխավորեն բոլոր հիմնարար իրավունքների եւ ազատությունների պաշտպանություն եւ հաստատեն իրենց համընդհանրությունը, անքակտելիությունը, փոխկախվածությունը եւ փոխշաղկապվածությունը: Դրանք պետք է խոր հարգանք երաշխավորեն նաեւ ժողովրդավարության եւ օրենքի գերակայության հանդեպ եւ խթանեն կայուն զարգացումը: Հանրային եւ մասնավոր բոլոր դերակատարները պետք է ընդունեն եւ պաշտպանեն մարդու հիմնարար իրավունքներն ու ազատություններն իրենց գործողություններում եւ գործունեության շրջանակներում, ինչպես նաեւ նոր տեխնոլոգիաների, ծառայությունների եւ դրանց կիրառության համատեքստում: Նրանք պետք է իրազեկ լինեն այն զարգացումներին, որոնք հանգեցնում են հիմնարար իրավունքների եւ ազատությունների ընդլայնմանը, ինչպես նաեւ դրանց վտանգներին եւ իրենց լիարժեք մասնակցությունն ունենան այն գործին, որի նպատակը նոր ձեւավորվող իրավունքների ընդունումն է:

2. Կառավարում բոլոր շահագրգիռ կողմերի մասնակցությամբ

Համացանցի կառավարման կարգավորումների զարգացումը եւ իրականացումը պետք է բաց, թափանցիկ եւ պատասխանատու կերպով ապահովեն կառավարությունների, մասնավոր հատվածի, քաղաքացիական հասարակության, տեխնիկական համայնքի եւ օգտատերերի լիակատար մասնակցություն՝ հաշվի առնելով նրանց հատուկ դերակատարությունն ու պարտավորությունները: Համացանցին առնչվող միջազգային հանրային քաղաքականության եւ համացանցի կառավարման կարգավորումների զարգացումը պետք է լիակատար եւ հավասար մասնակցության հնարավորություն տա բոլոր երկրների բոլոր շահագրգիռ կողմերին:

3. Պետությունների պարտավորությունները

Պետություններն ունեն իրավունքներ եւ պարտավորություններ՝ կապված համացանցին առնչվող միջազգային հանրային քաղաքականության հարցերի հետ: Ըստ միջազգային իրավունքի՝ իրենց ինքնիշխանության իրավունքների շրջանակներում, պետությունները պետք է զերծ մնան որեւէ գործողությունից, որն ուղղակիորեն կամ անուղղակիորեն կարող է վնասել անձանց՝ իրենց տարածքային իրավազորությունից դուրս: Բացի այդ, հիմնարար իրավունքները սահմանափակող որեւէ ազգային որոշում կամ գործողություն պետք է ենթարկվի միջազգային պարտավորություններին եւ, մասնավորապես, հիմնված լինի իրավունքի վրա, անհրաժեշտ լինի ժողովրդավարական հասարակությանը եւ լիովին հարգի համաչափության եւ ազատ բողոքարկման իրավունքի սկզբունքները՝ ներկայացված համապատասխան իրավական եւ գործընթացներով պայմանավորված երաշխիքներով:

4. Համացանցից օգտվողների լիազորությունները

Օգտվողները պետք է լիովին իրացնեն իրենց հիմնարար իրավունքները եւ ազատությունները, կայացնեն իրազեկված որոշումներ եւ մասնակցեն համացանցի կառավարման կարգավորման գործընթացին, մասնավորապես՝ կառավարման մեխանիզմներին եւ համացանցին առնչվող հանրային քաղաքականության մշակմանը՝ լիովին վստահ եւ ազատ:

5. Համացանցի համընդհանրությունը

Համացանցին առնչվող քաղաքականությունը պետք է ընդունի համացանցի գլոբալ բնույթը եւ համընդհանուր հասանելիության նպատակը: Դա չպետք է բացասաբար ազդի անդրսահմանային համացանցային թրաֆիկի անարգել հոսքի վրա:

6. Համացանցի հստակությունը

Համացանցի անվտանգությունը, կայունությունը, հուսալիությունը, ճկունությունը, ինչպես նաեւ զարգանալու հնարավորությունը պետք է լինեն համացանցի կառավարման առանցքային նպատակները: Համացանցի ենթակառուցվածքների հստակությունը եւ շարունակական գործառնությունը պահպանելու նպատակով անհրաժեշտ է խթանել ազգային եւ միջազգային շահագրգիռ կողմերի համագործակցությունը:

7. Ապակենտրոնացված կառավարում

Պետք է պահպանվի համացանցի ամենօրյա կառավարման համար պատասխանատվության ապակենտրոնացված բնույթը: Համացանցի տեխնիկական եւ կառավարման ոլորտների պատասխանատու մարմինները, ինչպես նաեւ մասնավոր հատվածը, պետք է պահպանեն իրենց առաջատար դերը տեխնիկական եւ գործնական հարցերում՝ ապահովելով թափանցիկություն եւ պատասխանատվություն գլոբալ հանրության առջեւ այն գործողությունների համար, որոնք ազդեցություն ունեն հանրային քաղաքականության վրա:

8. Կառուցվածքային սկզբունքները

Պետք է պահպանվեն համացանցի բաց ստանդարտները եւ փոխգործունակությունը, ինչպես նաեւ՝ անսահմանափակ բնույթը: Բոլոր շահագրգիռ կողմերը, համացանցի կառավարման վերաբերյալ որոշումներ կայացնելիս, պետք է ղեկավարվեն այս սկզբունքներով: Չպետք է լինեն նոր օգտատերերի մուտքի եւ համացանցի օրինական օգտագործման անխոհեմ արգելքներ կամ ավելորդ բեռ, որոնք կարող են ազդել նորարարության ներուժի վրա՝ կապված տեխնոլոգիաների եւ ծառայությունների հետ:

9. Բաց ցանց

Օգտատերերին պետք է հնարավորինս հասանելի լինեն առցանց բովանդակությունը, իրենց ընտրած ծառայությունները՝ անկախ այն բանից, դրանք անվճա՞ր են, թե՞ ոչ՝ գործածելով իրենց ընտրած հարմարավետ սարքերը: Թրաֆիկի կառավարման միջոցառումները, որոնք ազդում են հիմնարար իրավունքների եւ ազատությունների, մասնավորապես, ազատ արտահայտվելու, տեղեկատվության հաղորդման եւ ստացման, ինչպես նաեւ անձնական կյանքը հարգելու իրավունքները իրականացնելու վրա, պետք է համընկնեն ազատ արտահայտման եւ տեղեկատվության հասանելիության պաշտպանության, անձնական կյանքը հարգելու միջազգային իրավունքների պահանջներին:

10. Մշակութային եւ լեզվական բազմազանություն

Մշակութային եւ լեզվական բազմազանության պահպանությունը եւ տեղական բովանդակության զարգացման խթանումը, անկախ լեզվից կամ ձեռագրից, պետք է լինեն համացանցին առնչվող

քաղաքականության եւ միջազգային համագործակցության, ինչպես նաեւ նոր տեխնոլոգիաների զարգացման առանցքային նպատակները:

Նյութի օժանդակ աղբյուրը Եվրոպայի խորհրդի պաշտոնական կայքն է:

Պատրաստեց Հասմիկ Փայտյանը

ՄԱՍ 2

ԱՆՁՆԱԿԱՆ ԵՎ ԸՆՏԱՆԵԿԱՆ ԿՅԱՆՔԻ ԻՐԱՎՈՒՆՔԸ ՀԱՄԱՑԱՆՑՈՒՄ

ԱՆՁՆԱԿԱՆ ԵՎ ԸՆՏԱՆԵԿԱՆ ԿՅԱՆՔԻ ԻՐԱՎՈՒՆՔԸ ՀԱՄԱՑԱՆՑՈՒՄ

Արա Ղազարյան

Վեբ տեխնոլոգիաների զարգացումը ստիպում է մեզ շարունակ փոփոխել մեր պատկերացումները այս տիրույթում անձնական եւ ընտանեկան կյանքի նկատմամբ հարգանքի իրավունքի պաշտպանվածության շրջանակների ու հիմքերի մասին: Համացանցը մի տիրույթ է, որը չունի աշխարհագրական սահմաններ, եւ կարգավորող մարմիններին դժվար է կիրառել իրավազորություն անձանց իրավունքները պաշտպանելու նկատառումով: Այս իմաստով շատ կարեւոր են միջպետական ու միջազգային համաձայնագրերը, իրավական կառուցակարգերը: Այդուհանդերձ, փորձը ցույց է տալիս, որ գիտությունն ու տեխնոլոգիաներն այս ոլորտում առավել արագ են զարգանում, քան իրավական կարգավորումները, եւ մինչ նոր իրավական կառուցակարգերը ստեղծվում ու հարմարեցվում են նոր պայմաններին, դրանք արագորեն հնանում են, քանի որ ստեղծվում են նոր տեխնոլոգիաներ, որոնք հնարավորություն են տալիս սպառողներին արդյունավետորեն շրջանցելու այդ կառուցակարգերը:

Վաղ համացանցի դարաշրջանում (անցյալ դարի 90-ական թվականներ) տեղեկատվությունը հոսում էր մեկ ուղղությամբ՝ արտադրողից սպառողին: Վերջինս չէր կարող գեներացնել ստացված տեղեկատվական նյութը (քոնթենթը) եւ տարածել դա կոճակի մեկ հարվածով՝ «հասանելի է բոլորին» ռեժիմով՝ այնպես, ինչպես անում էր տեղեկատվության աղբյուրը՝ տարածողը:

2005-2006 թվականներից նոր տեխնոլոգիաները հնարավորություն տվեցին տեղեկատվություն սպառողին դառնալ միեւնույն ժամանակ տեղեկատվություն արտադրող. համացանցը դարձավ ինտերակտիվ, եւ բոլոր տեսակի տեղեկությունները, այդ թվում՝ անձնական ու ընտանեկան կյանքի մասին, հնարավորություն ստացան արագորեն ու գրեթե անկառավարելի եղանակով գեներացվելու եւ տարածվելու: «Ֆեյսբուքի» մեկ օգտատերն այսու - հետ կարող էր տեղեկությունը տարածել հազարավոր օգտատերերի շրջանում՝ այնպես, ինչպես նախկինում դա անում էին ավանդական ՁԼՄ-ները՝ տպագիր մամուլը, հեռուստատեսությունը, ռադիոն:

Նման ինտերակտիվ համացանցը խառնաշփոթ առաջացրեց

արդեն գոյություն ունեցող եւ հարմարեցված իրավական կառուցակարգերում: Անձնական կյանքի մասին ինֆորմացիան այսուհետ համացանցի տիրույթ մուտք գործելիս արագորեն գեներացվում ու տարածվում էր, եւ այն հեռացնելը համացանցի տիրույթից դառնում գրեթե անհնար կամ մեծ ջանքեր պահանջող:

Այս ամենին գումարվեց եւս մեկ երեւույթ՝ տեղեկատվական տեխնոլոգիաների կոնվերգենցիան՝ համացանցը, հեռուստատեսությունը, ռադիոն, բջջային կապը եւ այլ տեխնոլոգիաներ, որոնք ավանդաբար գտնվում էին տարբեր տիրույթներում, զուգամիտվեցին մեկ ենթակառույցի վրա: Գրպանում ունենալով բջջային հեռախոս՝ օգտատերը կարող է այսուհետ մուտք ունենալ հեռուստատեսություն, տպագիր մամուլ, ռադիո, էլեկտրոնային փոստ, հեռակապ, առցանց ինտերակտիվ ծառայություններ, խաղեր եւ այլն, եւ ոչ միայն մուտք ունենալ, այլ նաեւ գեներացնել տեղեկությունը բոլոր այս տիրույթներում: Հասկանալի է, որ անձնական կյանքի մասին տեղեկության տարածումը նման միջավայրում դառնում է առավել անվերահսկելի:

Համացանցի վերը նշված հատկանիշները հաշվի առնելով՝ իրավական կառուցակարգերում ամրագրվեցին անձնական եւ ընտանեկան կյանքի նկատմամբ հարգանքի իրավունքի պաշտպանության համար նոր մոտեցումներ՝ նյութաիրավական նոր հիմքեր եւ պաշտպանության նոր մեխանիզմներ:

1. Անձնական կյանքի տիրույթները համացանցում

Անձնական ու ընտանեկան կյանքի նկատմամբ հարգանքի իրավունքի միջամտությունը համացանցում կարող է տեղի ունենալ հետեւյալ պաշտպանված հիմքերի շրջանակներում.

- արժանապատվության նկատմամբ հարգանքի իրավունք
  - վիրավորանք
  - զրպարտություն
- հեղինակային եւ հարակից իրավունքներ
  - քաղվածքներ
  - գրագողություն
- անձնական տվյալների հրապարակում

- անուն, ազգանուն
- աուտենտիկական տվյալների հրապարակում

• անձնական եւ ընտանեկան կյանքի վերաբերյալ տեղեկությունների հրապարակում

- ինտիմ կյանքի վերաբերյալ տվյալներ
- բժշկական տվյալներ

2. Հրապարակային հայտարարությունը համացանցում

Համացանցում անձնական կյանքի իրավունքն առավել հաճախ խախտվում է վիրավորական կամ զրպարտող բնույթի խոսքի տարածման հիմքով: ՀՀ-ում այս իրավունքի պաշտպանության համար գործում է ՀՀ քաղաքացիական օրենսգրքի 1087.1-րդ հոդվածը, որի բազմաթիվ դրույթներով սահմանված պաշտպանության միջոցները հավասարապես գործում են նաեւ համացանցի առումով: Այս կապակցությամբ ՀՀ դատարանները կայացրել են մի շարք որոշումներ, որոնցով սահմանել են մի շարք պաշտպանական համակարգեր: Օրինակ՝ որպեսզի հնարավոր լինի կիրառել վերը նշված 1087.1-րդ հոդվածով սահմանված իրավական պաշտպանության միջոցները, անհրաժեշտ է առաջին հերթին ցույց տալ, որ անձական կյանքի իրավունքի միջամտությունը տեղի է ունեցել **հրապարակային** եղանակով: «Հրապարակային» արտահայտությունը դատարանները մեկնաբանել են որպես մի հայտարարություն, որը կատարվում է առնվազն մեկ երրորդ անձի **ներկայությամբ**, իսկ եթե հայտարարությունը կատարվել է համացանցի կամ կապի այլ միջոցներով՝ երրորդ անձին **հաղորդակից** դարձնելով: Այս մեկնաբանությունը հնչել է ՀՀ Վճռաբեկ դատարանի թիվ ԵԿԴ/2293/02/10 գործով որոշման մեջ[1]: Զարգացնելով սույն մեկնաբանությունը համացանցի առումով՝ դատարանները (տե՛ս թիվ ԵԱԴԴ/0074/02/12 քաղաքացիական գործով Աջափնյակ եւ Դավթաշեն վարչական շրջանների ընդհանուր իրավասության դատարանի որոշումը) սահմանել են «հասանելի է բոլորին» եզրույթը,

1. Տե՛ս առավել մանրամասն Վճռաբեկ դատարանի թիվ ԵԿԴ/2293/02/10 որոշման 8-րդ էջի վերջում եւ 9-րդ էջի սկզբում, ինչպես նաեւ 9-րդ էջի 2-րդ պարբերության հստակ ձեւակերպումը:

ըստ որի՝ սոցիալական ցանցում բոլորին հասանելի եղանակով տարածված հայտարարությունը հրապարակային հայտարարություն է[2]: Այսինքն՝ «Ֆեյսբուք» սոցիալական ցանցի անձնական էջում status post եղանակով ուրիշի անձնական կյանքի վերաբերյալ տեղեկության տեղադրումը public կամ friends ռեժիմով, կամ տեղեկության տարածումը share եղանակով համարվում է անձնական կյանքի վերաբերյալ **հրապարակային** հայտարարություն՝ իր բոլոր հետեւանքներով:

3. Պատկերը պաշտպանելու իրավունքը

Մարդու իրավունքների եվրոպական դատարանը սահմանել է, որ անձն իրավունք ունի վերահսկելու իր լուսանկարի հրապարակումը՝ ընդհուպ դրա հրապարակումը մերժելը.

> *«Անձի պատկերը համարվում է իր անհատականության գլխավոր հատկանիշներից, քանի որ այն ի ցույց է դնում անձի ուրույն հատկանիշները եւ տարբերակում է անձին իր նմաններից: Անձի պատկերի պաշտպանությունը, այդպիսով, անձնական զարգացման էական բաղադրիչներից է: Այն առավելապես ենթադրում է անձի՝ այդ պատկերի օգտագործումը հսկելու, ներառյալ դրա հրապարակումն արգելելու իրավունքը»[3]:*

Անկասկած, վերը նշվածը վերաբերում է նաեւ պատկերի օգտագործմանը առցանց միջավայրում: Այստեղից հարց է ծագում՝ արդյոք վերը նշվածից բխո՞ւմ է, որ անձն իրավունք ունի ոչ միայն արգելելու իր նկարի հրապարակումը, այլ նաեւ պահանջելու, որ նկարը հեռացվի համացանցից: Ավելին՝ արդյոք նշանակո՞ւմ է նաեւ, որ անձն իրավունք ունի պահանջելու, որ իր մասին որոշակի տեղեկատվությունը հեռացվի համացանցից: Սա մի խնդիր է, որն իր վերջնական լուծումը դեռ չի ստացել միջազգային իրավունքում եւ

2. Աջափնյակ եւ Դավիթաշեն վարչական շրջանների ընդհանուր իրավասության դատարան թիվ ԵԱԴԴ/0074/02/12 քաղաքացիական գործով վճիռ, էջ 8, պարբ. 2:
3. Ֆոն Հաննովերն ընդդեմ Գերմանիայի (2), թիվ *40660/08 եւ 60641/08)*, ՄԻԵԴ, 7/02/2012, § 96

պետությունների ազգային իրավական համակարգերում, սակայն որոշակի քայլեր արդեն արվել են, որոնցից է մոռացված լինելու իրավունքը:

4. Անոնիմ մնալու իրավունքը

Համացանցում անոնիմ (անանուն) մնալը աստիճանաբար ճանաչվում է որպես ինքնուրույն իրավունք: Եվրոպայի խորհրդի Նախարարների կոմիտեի՝ 28/05/2003թ. «Համացանցում հաղորդակցության ազատության» մասին հռչակագրի 7-րդ սկզբունքում սահմանվում է.

> *«Առցանց միջավայրում գաղտնի միջոցների դեմ պաշտպանության միջոցներ ապահովելու եւ տեղեկությունների ու գաղափարների ազատ արտահայտման հնարավորությունը մեծացնելու նպատակով անդամ պետությունները պետք է հարգեն համացանցի բոլոր օգտատերերի՝ իրենց անձնական տվյալները չբացահայտելու իրավունքը: Սա չի արգելում անդամ պետություններին կիրառել միջոցներ եւ համագործակցել միմյանց հետ՝ հանցագործություն կատարած անձանց հայտնաբերելու նպատակով՝ արդարադատության եւ ոստիկանության ոլորտներում ազգային օրենքների, Մարդու իրավունքների եւ հիմնարար ազատությունների մասին կոնվենցիայի եւ այլ միջազգային համաձայնագրերի հիման վրա:*

Վերը նշվածից ակնհայտ է, որ այս իրավունքը չի կարող գործել քրեաիրավական տիրույթում, երբ համացանցի տիրույթում անձնական տվյալները չբացահայտելով՝ անանունությունը օգտագործվում է հանցագործության, կիբերհանցագործության կատարման նպատակով: Սակայն մնացած դեպքերում, այսինքն՝ քաղաքացիաիրավական եւ վարչաիրավական հարաբերություններում, անանունության իրավունքն աստիճանաբար ընդունվում է: Օրինակ՝ այդպիսի ոլորտներ են լրագրողական աղբյուրների գաղտնիությունը (որը նաեւ անձնական կյանքի տիրույթ է),

հեղինակային իրավունքը (որը թույլ է տալիս ճանաչել անոնիմ կամ կեղծանունով հանդես եկող հեղինակի իրավունքը ստեղծագործության նկատմամբ), որոշ խոցելի խմբերի անձնական տվյալները չբացահայտելու պարտավորությունը (օրինակ՝ սեռական բռնության զոհերի) եւ այլն: Վիրավորանքի եւ զրպարտության դեպքերում 1087.1-րդ հոդվածի 6-րդ եւ 9-րդ մասն ապահովում է տեղեկատվության հեղինակի անձնական տվյալների գաղտնիությունն այն դեպքում, երբ հրապարակային հայտարարություն կատարողն օգտվել է անանուն աղբյուրից եւ որոշել է չբացահայտել իր աղբյուրը: Նման դեպքերում պատասխանատվության սուբյեկտ է դառնում հրապարակային հայտարարություն կատարողը, եւ քաղաքացիական դատարանները, սովորաբար, չեն պարտադրում նրանց պատասխանողին բացահայտել իրենց անանուն աղբյուրը: Վերը նշվածը մանրամասնորեն բացատրել ու մեկնաբանել է ՀՀ Վճռաբեկ դատարանն իր թիվ ԵԿԴ/2293/02/10 եւ թիվ ԼԴ/0749/02/10 գործերով կայացված որոշումներում:

5. Մոռացված լինելու իրավունքը

Եվրոպայի արդարադատության դատարանը 2014 թ. մայիսի 13-ին կայացրեց աննախադեպ որոշում[4], որով սահմանեց, որ համացանցում որոնողական համակարգի օպերատորը (տվյալ դեպքում՝ Google ընկերությունը) կարող է պատասխանատվություն կրել այն անձանց անհատական տվյալների շրջանառության համար, որոնք հրապարակվում են երրորդ անձանց ինտերնետ էջերում: Գործնականում դա նշանակում է, որ եթե անձի անունով կատարվում է որոնում, եւ դրա արդյունքում ցուցադրվում են բոլոր այն համացանցային էջերի հղումները, որոնք պարունակում են տեղեկություն այդ անձի մասին, տվյալ անձը կարող է դիմել որոնողական համակարգի օպերատորին եւ պահանջել հանել բոլոր հղումները, որոնք ստացվում են որոնման արդյունքում, կամ, եթե օպերատորը մերժում է խնդրանքը, նույն պահանջով դիմել պատկան

4. Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Dators and Mario Costeja Gonzalez. Եվրոպայի արդարադատության դատարան, թիվ C-131/12, 13/05/2014թ.

մարմիններին: Այլ կերպ, այս իրավունքը կոչվեց մոռացված լինելու իրավունք: Այս իրավունքը, փաստորեն, գործում է դեռ միայն Եվրոպական միության պետություններում: Իսկ մնացած պետություններում այն ամրագրված չէ, եւ այդ դեպքում դիմողը կարող է հույսը դնել միայն տվյալ կայքի սեփականատիրոջ բարի կամքի վրա:

ՀՀ-ում համացանցից որոշակի քոնթենթ հեռացնելու իրավունքը չի գործում: Դա նշանակում է, որ անձնական կյանքի մասին վիրավորական կամ զրպարտող բնույթի տեղեկությունը կարող է մնալ համացանցում նույնիսկ այն դեպքում, երբ անձը շահել է դատական գործը դատարանում եւ ստացել արդարացի փոխհատուցում՝ ներողության հայցում, հերքում կամ բարոյական վնասի դիմաց նյութական փոխհատուցում: Ակնհայտ է, որ իրավական պաշտպանության նման եղանակներն անարդյունավետ են, եթե վիճահարույց տեղեկությունը շարունակում է մնալ ու տարածվել համացանցում:

Չի բացառվում, որ ապագայում օրենսդիրը վերանայի իր մոտեցումը եւ Քաղաքացիական օրենսգրքի 1087.1-րդ հոդվածում ավելացնի համացանցից քոնթենթը հեռացնելու իրավունքը սահմանող առանձին դրույթ: Տեխնոլոգիաների զարգացումը դա է պահանջում: Դրա համար արդեն կան նախադրյալներ: Առաջինը վերը նշված ԵՄ դատարանի որոշումն է, որ աննախադեպ խոսք էր համացանցի տիրույթում անձնական կյանքի պաշտպանվածության մասին: Երկրորդը Դելֆիի[5] գործով Մարդու իրավունքների եվրոպական դատարանի հետեւյալ դիրքորոշումներն են.

> • Համացանցում կատարված հրապարակային արտահայտությունների առումով պետությունը կրում է անձանց արժանապատվության եւ անձնական կյանքի նկատմամբ հարգանքի իրավունքները պաշտպանելու նպատակով արդյունավետ իրավական կառուցակարգեր մշակելու պոզիտիվ պարտականություն[6],

5. «Դելֆին ընդդեմ Էստոնիայի», թիվ 64569/09, ՄԻԵԴ, 10/10/2013:

• Համացանցում կատարված հրապարակային արտահայտության առումով միշտ չէ, որ հեղինակ(ներ)ի դեմ քաղաքացիական հայցը արդյունավետ իրավական պաշտպանության միջոց է՝ հաշվի առնելով այն հանգամանքը, որ համացանցում հեղինակների համար համեմատաբար հեշտ է հանդես գալ անոնիմ եղանակով, մինչդեռ տուժողներից նկատելիորեն մեծ ջանքեր են պահանջվում հեղինակներին հայտնաբերելու եւ նրանց դեմ քաղաքացիական հայց ներկայացնելու համար[7],

• Համացանցի օգտատերերին անոնիմ մնալու եւ իրենց ինքնությունը չբացահայտելու հնարավորություն տալը խիստ կարեւոր է նրանց ազատ արտահայտվելու իրավունքի իրականացման համար: Այդուհանդերձ, համացանցի զարգացումը, ինչպես նաեւ հնարավորությունը, իսկ որոշ դեպքերում նաեւ վտանգը, որ համացանցում մեկ անգամ հրապարակայնորեն տարածված խոսքը կարող է ընդմիշտ մնալ որպես այդպիսին եւ անդադար տարածվել, պահանջում է ցուցաբերել զգոնություն[8],

• Համացանցում տեղեկության տարածման դյուրինությունը, ինչպես նաեւ այդ տիրույթում մեծ քանակությամբ տեղեկությունների առկայությունը հանգամանքներ են, որոնց արդյունքում շատ դժվար է համացանցում հայտնաբերել վիրավորական կամ զրպարտող բնույթի հայտարարությունները եւ հեռացնել դրանք: Դա շատ դժվար խնդիր է առցանց լրատվամիջոցների օպերատորների համար եւ առավել մեծ դժվարություն է ներկայացնում վիրավորանքի կամ զրպարտության զոհ դարձած սովորական քաղաքացիների համար, ովքեր մեծ մասամբ չունեն համացանցը մոնիթորինգ անելու համար բավարար ռեսուրսներ[9]:

6. Կետ 91:
7. Նույն տեղում:
8. Կետ 92:

Վերը նշված մոտեցումների արդյունքում Եվրոպական դատարանը «Դելֆիի» գործով» փոքր-ինչ նեղացրեց ազատ խոսքի պաշտպանության սահմանները համացանցում՝ Կոնվենցիայի խախտում չարձանագրելով «Դելֆի» ընկերությանը պատասխանատվության ենթարկելու մասին ազգային մարմինների որոշումը: Այս որոշումը, սակայն, քննադատության արժանացավ ազատ խոսքի ակտիվիստների կողմից:

9. Նույն տեղում:

ՄԱՍ 3

ԿԻԲԵՐՀԱՆՑԱԳՈՐԾՈՒԹՅԱՆ ԻՐԱՎԱԿԱՆ ԿԱՐԳԱՎՈՐՈՒՄԸ ՀԱՅԱՍՏԱՆՈՒՄ

ԿԻԲԵՐՀԱՆՑԱԳՈՐԾՈՒԹՅԱՆ ԻՐԱՎԱԿԱՆ ԿԱՐԳԱՎՈՐՈՒՄԸ ՀԱՅԱՍՏԱՆՈՒՄ

Արա Ղազարյան

Կիբերհանցագործությունները համակարգչային համակարգերի միջոցով կատարված հանցագործություններ են: «Համակարգչային համակարգեր» ասելով հասկանում ենք համակարգչային սարք կամ ցանցով միմյանց փոխկապակցված սարքերի խումբ, որոնք կատարում են համակարգչային տվյալների ավտոմատ մշակում: Համաձայն Կիբերհանցագործության մասին եվրոպական կոնվենցիայի (այսուհետ Կոնվենցիա)՝ կիբերհանցագործությունները բաժանվում են հանցագործությունների չորս խմբի.

1) համակարգչային համակարգերի եւ տվյալների գաղտնիության, միասնության եւ մատչելիության դեմ ուղղված հանցագործություններ,

2) համակարգչային միջոցների օգտագործմամբ կատարված հանցագործություններ,

3) մանկական պոռնոգրաֆիային վերաբերող հանցագործություններ,

4) հեղինակային իրավունքի եւ հարակից իրավունքների խախտման հետ կապված հանցագործություններ:

ՀՀ ազգային համակարգում կիբերհանցագործությունը կարգավորվում է Քրեական օրենսգրքի 24-րդ գլխով, որը պարունակում է համակարգչային համակարգի եւ տեղեկատվության անվտանգության դեմ ուղղված հանցագործությունների յոթ հոդվածներ:

Ներկայացնենք Կոնվենցիայի ներքո կիբերհանցագործության տեսակների չորս խմբերը.

1. Համակարգչային համակարգերի եւ տվյալների գաղտնիության, միասնության եւ մատչելիության դեմ ուղղված հանցագործություններ

1.1. Անօրինական մուտք գործելը

Այս խմբի հանցագործությունները ներառում են համակարգչային համակարգ առանց թույլտվության մուտք գործելը տվյալների ձեռքբերման կամ որեւիցե այլ անազնիվ նպատակով: ՀՀ ազգային համակարգում այս հանցակազմը սահմանված է Քրեական օրենսգրքի 254-րդ հոդվածով: Այս հոդվածի հիմքով հարուցված, հանրային մեծ հետաքրքրություն առաջացրած գործերից է Երեւանի պետական ճարտարագիտական համալսարանի ռեկտորի հայտարարության հիման վրա հարուցված քրեական գործը այն հիմքով, որ անհայտ անձինք անօրինական մուտք են գործել նրա ֆեյսբուքյան էջ եւ այդտեղից վարկաբեկիչ տեղեկատվություն են տարածել:

1.2. Անօրինական եղանակով հաղորդակցությունը գաղտնի որսալը

Այս խմբի հանցագործությունները ներառում են համակարգչային կապի միջոցների օգտագործմամբ համակարգչային համակարգ մտնող, դուրս եկող եւ համակարգ(չ)ի մեջ գտնվող տվյալների ոչ հրապարակավ կատարվող փոխանցումները որսալը տեխնիկական միջոցների կիրառմամբ: Այս հանցակազմը նույնպես սահմանված է ՀՀ քրեական օրենսգրքի 254-րդ հոդվածով: Այդուհանդերձ, այս հանցակազմի տարբերությունը վերը նշվածից այն է, որ այս դեպքում իրավունքի միջամտությունը կատարվում է ոչ թե համակարգ մուտք գործելու, այլ էլեկտրամագնիսական հոսքը որսալու եղանակով:

1.3. Միջամտություն տվյալների մեջ

Այս խմբի հանցագործությունները ներառում են այնպիսի գործողություններ, ինչպիսիք են համակարգչային տվյալները վնասելը, ոչնչացնելը, փչացնելը, փոփոխելը կամ արգելելը: ՀՀ քրեական օրենսգրքում նշված հանցագործությունը սահմանված է 251-րդ եւ 252-րդ հոդվածներով: Ընդ որում, 251-րդ հոդվածի

իմաստով (որը սահմանում է համակարգչային տվյալների փոփոխություն եւ ոչնչացում) պարտադիր չէ համակարգ մուտք գործելու դիտավորության առկայությունը, իսկ 252-րդ հոդվածի իմաստով (որը սահմանում է համակարգչային տվյալների փոփոխություն կամ գույքային վնասի պատճառում)՝ կարեւոր չէ գույքը հափշտակելու մտադրությունը: Այս հանցագործությունների օրինակ են տեղեկատվական պատերազմի շրջանակներում հայկական կայքերի վրա հաքերների հարձակումները, որոնք արվում են կայքերում տեղեկությունները զուտ փոփոխելու, վնասելու, ոչնչացնելու նպատակով՝ առանց գույքը հափշտակելու մտադրության:

1.4. Սարքերի չարաշահում

Ներառում է վերը շարադրված հանցագործությունների կատարման նպատակով սարքը, համակարգչային ծրագիր վաճառելը, օգտագործելը, ներմուծելը կամ այլ կերպ հայթայթելը: Ներառում է նաեւ համակարգչային համակարգ մուտք գործելու համար ծածկագրի, մուտքի կոդի տվյալները վաճառելը, օգտագործելը, ներմուծելը կամ այլ կերպ հայթայթելը: ՀՀ քրեական օրենսգրքում այս հանցագործությունները մասամբ սահմանված են 255-րդ եւ 256-րդ հոդվածներով: Այս հոդվածները կիրառվել են ՀՀ-ում եւ ամբողջ աշխարհում մեծ աղմուկ հանած հայտնի Բ. Ավանեսովի գործով, ով, օգտագործելով իր ստեղծած Bredolab «կոտրած» (hijacked) համակարգիչների ցանցը կամ բոթնեթը, օրական տարածում էր ավելի քան 3 մլրդ սփամ նամակներ՝ հարձակման թիրախ դարձնելով տարբեր երկրներում ֆիզիկական եւ իրավաբանական անձանց պատկանող կայքերն ու IP-հասցեները, խափանելով այդ կայքերի բնականոն աշխատանքը, ուղեփակելով այնտեղ պահվող համակարգչային տեղեկատվությունը, ոչ պիտանի դարձնելով այդ համակարգչային համակարգերը եւ դրանց արդյունքում հափշտակելով խոշոր չափի գույք[10]: Համակարգը Ավանեսովի համար գեներացնում էր ամսական շուրջ 100.000 եվրոյի եկամուտ:

10. Տե՛ս ԵԱՔԴ/0144/01/11 քրեական գործը www.datalex.am տվյալների բազայում:

2. Համակարգչին առնչվող հանցագործություններ

Ներառում է այնպիսի հանցագործություններ, որոնց արդյունքում միտումնավոր կերպով մուտք է արվում, փոփոխվում, ոչնչացվում կամ արգելափակվում համակարգչային տվյալներ՝ տվյալների **աուտենտիկության** խափանման նպատակով, որպեսզի մուտքագրված, տեղադրված կեղծ տվյալները գործեն օրինական կերպով՝ որպես իսկական տվյալներ:

Նաեւ ներառում է այնպիսի գործողություններ, ինչպիսիք են համակարգչային տվյալների մուտքագրումը, փոփոխումը, ոչնչացումը կամ արգելափակումը՝ տնտեսական շահ ստանալու նպատակով:

3. Մանկական պոռնագրաֆիա

Հանցակազմը ներառում է այնպիսի գործողություններ, ինչպիսիք են մանկական պոռնոգրաֆիայի.

- արտադրությունը,
- առաջարկումը,
- մատչելի դարձնելը,
- տարածելը,
- փոխանցումը,
- հայթայթումը՝ իր կամ այլ անձի համար,
- տիրապետումը:

ՀՀ քրեական օրենսգրքով սույն հանցագործությունը սահմանված է 263-րդ հոդվածի 2-րդ մասով եւ ներառում է «Համակարգչային համակարգի միջոցով մանկական պոռնոգրաֆիայի ներկայացնելը կամ համակարգչային համակարգում կամ համակարգչային տվյալների պահպանման համակարգում մանկական պոռնոգրաֆիայի պահպանելը»:

4. Հեղինակային եւ հարակից իրավունքներ

Ներառում է գործողություններ, որոնք ուղղված են հեղինակային կամ հարակից իրավունքների խախտումներին, որոնք արվում են դիտավորությամբ, խոշոր առեւտրային մասշտաբներով եւ

համակարգչային համակարգի միջոցով:

Ազգային օրենսդրությամբ հեղինակային իրավունքի խախտումների համար իրավական պաշտպանության միջոցները սահմանված են ե՛ւ Քաղաքացիական օրենսգրքով, ե՛ւ Քրեական օրենսգրքով՝ կապված խախտումների ծավալի հետ: Բաժանարար գիծը որոշվում է արարքի խախտման չափերով: Եթե հեղինակային իրավունքի խախտումը կատարվել է «զգալի» եւ «խոշոր» չափերով, նման խախտումը համարվում է հանցագործություն, եւ խնդիրը կարգավորվում է Քրեական օրենսգրքի 158-րդ հոդվածով: «Զգալի» չափ է համարվում, եթե հեղինակային իրավունքի օբյեկտ հանդիսացող թույլտվության գինը 50-100 հազար դրամ է, իսկ «խոշոր» չափը՝ 200 հազարից բարձր:

Մնացած բոլոր դեպքերում խնդիրը գտնվում է քաղաքացիաիրավական տիրույթում եւ կարգավորվում Քաղաքացիական օրենսգրքի 63-րդ գլխով սահմանված դրույթներով: Այդուհանդերձ, «զգալի» չափերով խախտման դեպքում անհրաժեշտ կլինի տուժողի դիմումը, քանի որ նման հիմքով քրեական հետապնդումն իրականացվում է մասնավոր մեղադրանքի կարգով, իսկ «խոշոր» չափերով կատարված հեղինակային իրավունքի խախտման դեպքը՝ հանրային մեղադրանքի կարգով, որը նշանակում է, որ իրավասու մարմինները կարող են քրեական հետապնդում իրականացնել անկախ տուժողի՝ դիմողի առկայությունից, օրինակ՝ ՋԼՄ-ներից ստացված տեղեկատվության հիման վրա:

ՄԱՍ 4

«ԿԻԲԵՐՀԱՆՑԱԳՈՐԾՈՒԹՅՈՒՆԸ ԵՎ ՑԱՆՑԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԱՆՈՆՆԵՐԻ ՊԱՀՊԱՆՈՒՄԸ ՀԱՅԱՍՏԱՆՈՒՄ» ԹԵՄԱՅՈՎ ՀԱՐՑՄԱՆ ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ

«ԿԻԲԵՐՀԱՆՑԱԳՈՐԾՈՒԹՅՈՒՆԸ ԵՎ ՑԱՆՑԱՅԻՆ ԱՆՎՏԱՆԳՈՒԹՅԱՆ ԿԱՆՈՆՆԵՐԻ ՊԱՀՊԱՆՈՒՄԸ ՀԱՅԱՍՏԱՆՈՒՄ» ԹԵՄԱՅՈՎ ՀԱՐՑՄԱՆ ՎԵՐԼՈՒԾՈՒԹՅՈՒՆ

Հարցումը կատարվել է Հայաստանի լրատվամիջոցների եւ քաղաքացիական հասարակության ներկայացուցիչների շրջանում

Հետազոտության գաղափարն ու մեթոդաբանությունը՝
Սուրեն Դեհերյանի

Արդյունքների տեխնիկական մշակումը եւ վերլուծությունը՝
Կարինե Դարբինյանի

Հարցումների պատասխանատու եւ տվյալների մուտքագրող՝
Հասմիկ Փայտյան

Ներածություն

Մենք ապրում ենք մի դարաշրջանում, երբ համակարգիչներն ու հեռահաղորդակցության տեխնոլոգիաները տարեցտարի լայն տարածում են գտնում բոլոր այն ոլորտներում, որոնք անհրաժեշտ են մարդու եւ պետության բավարար կենսունակությունն ապահովելու համար: Մարդու կյանքի անվտանգության ապահովումն ամենաբարդ խնդիրներից է: Այն կրկնակի բարդացավ, երբ պարզ դարձավ, որ անհրաժեշտություն կա յուրաքանչյուրի անվտանգության կրկնակի ապահովում, քանի որ այսօր, բացի իրական աշխարհից, գոյություն ունի նաեւ մեկ այլ՝ համակարգիչների, կիբերտարածության կամ, այլ կերպ ասած, վիրտուալ աշխարհ: Հասարակությունն ակտիվ կիրառության մեջ դրեց հեռահաղորդակցության տեխնոլոգիաներն ու գլոբալ ցանցերը՝ չկանխատեսելով, թե այդ նույն տեխնոլոգիաները ինչպիսի հնարավորություններ են ստեղծում չարագործների համար:

Հայաստանում քչերին է հայտնի, թե ինչ է նշանակում

«կիբերանվտանգություն»: Այն՝ որպես եզրույթ, ավելի շատ կիրառվում է տեղեկատվության կամ տեղեկատվական անվտանգություն նշանակությամբ: Սակայն հանրության շրջանում վերջինիս կարեւորությունը դեռեւս չի գիտակցվում այն աստիճան, որքան Արեւմուտքում: Նույնը կարելի է ասել «կիբերհանցագործություն» եզրույթի մասին:

Մինչդեռ կիբերտիրույթում հանցագործությունների քանակն աճում է համացանցից օգտվողների թվի աճին համընթաց: Կիբերհանցագործության զոհ կարող են դառնալ ինչպես շարքային օգտատերերը, այնպես էլ պետությունները՝ իրենց ողջ համակարգով: Ինտերպոլի տվյալների համաձայն՝ կիբերհանցագործության աճի տեմպերն աշխարհում ամենամեծն են:

Կիբերհանցագործի հիմնական թիրախը համակարգիչն է, որը կառավարում է տարաբնույթ տեղեկատվական գործողություններ եւ այն տեղեկատվությունը, որն առկա է այդ համակարգում: Ի տարբերություն այլ հանցագործների, ովքեր գործում են իրական աշխարհում, կիբերհանցագործները համակարգում առկա տեղեկատվությանը տիրանալու համար չեն օգտագործում «ավանդական» զենք՝ դանակ կամ հրազեն:

Համաձայն Norton Cybercrime Report-ի ամենամյա հարցումների, որոնք իրականացվել են 24 երկրներում (Հայաստանը ներառված չէ)՝ յուրաքանչյուր վայրկյան համացանցի 18 չափահաս օգտատերեր դառնում են կիբերհանցագործության զոհ: Օրինակ՝ 2012 թ. տվյալների համաձայն՝ աշխարհում կատարված կիբերհանցագործություններից ֆիզիկական անձինք, ընդհանուր առմամբ, կրել են 113 միլիարդ դոլարի վնաս, իսկ 2011 թ.՝ 110 միլիարդ դոլարի:

Հայաստանի պարագայում նման ուսումնասիրություն չի կատարվել, սակայն, համաձայն պաշտոնական վիճակագրության, կիբերհանցագործությունը մեծ տարածում չունի, թեպետ նշվում է, որ այստեղ էլ թվերը տարեցտարի աճում են:

Եվ քանի որ թե՛ ներքին, թե՛ արտաքին հաքերական հարձակումների առաջնային թիրախներից են զանգվածային լրատվամիջոցներին եւ հասարակական կազմակերպություններին պատկանող կայքերն ու էլեկտրոնային փոստերը, ուստի ուսումնա-

սիրությունն իրականացվեց հենց այս ոլորտների ներկայացուցիչների շրջանում:

Կարիք չկա հատուկ ուսումնասիրության՝ պարզելու, որ Հայաստանում նրանք տեղեկատվության տարածման, պահպանման եւ ստացման նպատակով համացանցի ամենաակտիվ սպառողներից են: Սակայն հետաքրքիր է պարզել, թե տվյալ ոլորտի ներկայացուցիչները՝ որպես ցանցի ակտիվ սպառողներ, որքանո՞վ են կարեւորում համացանցում իրենց գործունեության տեղեկատվական անվտանգությունը, հատկապես որ նրանց գործունեությունն անմիջականորեն կապված է երրորդ անձանց մասին տեղեկատվության սպառման, մշակման եւ հաղորդման հետ: Ուստի տվյալ անձինք պետք է ունենան անհրաժեշտ հմտություններ եւ բավարար հնարավորություններ նման տեղեկատվության անվտանգ պահպանման կամ ապահով տեղափոխման համար:

«Լրագրողներ հանուն ապագայի» կազմակերպությունը, ԵԱՀԿ երեւանյան գրասենյակի աջակցությամբ, 2014 թ. մայիս-սեպտեմբեր ամիսներին հարցում իրականացրեց Հայաստանի լրատվամիջոցների եւ քաղաքացիական հասարակության ներկայացուցիչների շրջանում՝ նրանցից հետաքրքրվելով համակարգչային սարքերից եւ համացանցից օգտվելու հաճախականության, սեփական տեղեկատվական անվտանգությունը պահպանելու կանոնների եւ կիբերհանցագործության թիրախում հայտնվելու սեփական փորձի մասին:

Հարցմանը մասնակցել են Հայաստանի յոթ մարզերի (ներառյալ՝ Երեւանը) լրատվամիջոցների եւ հասարակական կազմակերպությունների 50 ներկայացուցիչներ՝ յուրաքանչյուրը պատասխանելով ընդհանուր առմամբ 50 հարցի:

Սույն հարցման միջոցով փորձել ենք պարզել, թե որքանով են հարցման մասնակիցները կարեւորում տեղեկատվական անվտանգության կանոնների պահպանումը, եւ, արդյոք նրանց կողմից կուտակվող տեղեկատվությունն ունի բավարար պաշտպանվածություն՝ երրորդ կողմին հասանելի չդառնալու համար:

Հարցման մասնակիցները

Սույն հարցումն իրականացվել է «Լրագրողներ հանուն ապագայի» ՀԿ կողմից՝ 2014 թ. ընթացքում «Ազատ, վստահելի եւ անվտանգ առցանց տեղեկատվություն բոլորի համար» ծրագրի շրջանակներում կազմակերպված «Տեղեկատվական անվտանգությունն ու իրավունքը համացանցում» թեմայով դասընթացների մասնակիցների շրջանում:

Դասընթացի 50 մասնակիցներից 33-ը՝ ԶԼՄ, իսկ 17-ը՝ քաղաքացիական հասարակության ոլորտի ներկայացուցիչներ են: Մասնակիցների 56%-ը Երեւանից է, 44%-ը՝ Հայաստանի 6 մարզերից (Շիրակ՝ 14%, Լոռի՝ 10%, Արարատ՝ 6%, Սյունիք՝ 6%, Գեղարքունիք՝ 4% եւ Արմավիր՝ 4%):

Լինելով հիմնականում երկու ոլորտի ներկայացուցիչներ՝ նրանք զբաղեցնում են հետեւյալ պաշտոնները՝ լրագրող (66%), հասարակայնության հետ կապերի պատասխանատու (24%), SS մասնագետ (2%), հետազոտող-դիտորդ (2%), փաստաբան (2%), խմբագիր (2%) եւ ծրագրերի համակարգող (2%):

Մասնակիցների 74%-ը կամ 37-ը՝ իգական սեռի, իսկ 26%-ը կամ 13 մարդ արական սեռի ներկայացուցիչներ են:

50 մասնակիցներից 41-ը պատկանում են 18-30, 8-ը՝ 31-45, իսկ մեկը՝ 46-65 տարիքային խմբերին:

Բոլոր 50 մասնակիցները պատասխանել են հարցաթերթիկում ընդգրկված բոլոր 50 հարցերին:

Հարցումը կատարվել է անանուն:

Հարցվածների՝ համակարգիչներից եւ ցանցից օգտվելու ակտիվություն

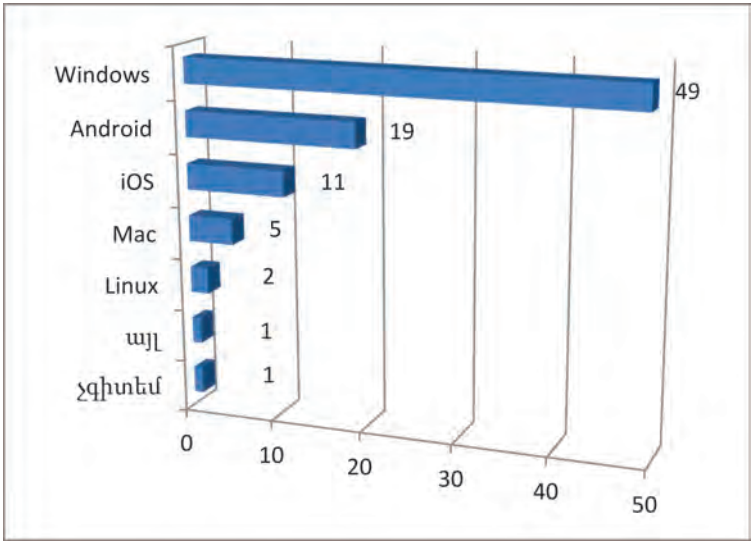
Մինչեւ տեղեկատվական անվտանգության խնդիրներին վերաբերող հարցերին անցնելը, պարզենք, թե հարցվածներն ինչ ակտիվությամբ են օգտվում համակարգչային սարքերից ու համացանցից:

Պետք է նշել, որ, ըստ հարցման արդյունքների, բոլոր մասնակիցներն օգտվում են մեկից ավելի համակարգչային սարքերից, ոմանք նույնիսկ՝ երկու եւ ավելի սարքերից, այդ թվում՝ սեղանադիր համակարգիչ (PC), նոութբուք, պլանշետ, սմարթֆոն եւ այլն:

Ամենաշատ կիրառվող սարքը հարցվածների շրջանում նոութբուքն է: Նման սարք օգտագործում են նրանցից 42-ը: Սեղանադիր համակարգչից օգտվում են հարցվածներից 32-ը, իսկ պլանշետից՝ 13-ը: Բոլոր հարցվածները օգտագործում են բջջային հեռախոս, որոնցից 26-ը՝ սմարթֆոն:

Հաջորդ հարցը վերաբերում է վերը նշված համակարգչային սարքերի օպերացիոն համակարգերի կիրառությանը (տե՛ս գծապատկեր 1), համաձայն որի՝ հարցվածներից 49-ն օգտվում է Windows օպերացիոն համակարգից (ՕՀ), նրանցից 19-ը՝ նաև Android ՕՀ-ից, 11-ը՝ iOS ՕՀ-ից, իսկ Mac ՕՀ-ից օգտվում է հարցվածներից 5-ը: Միայն երկուսն են նշել, որ օգտվում են Linux բաց կոդով գրված ՕՀ-ից: Մասնակիցներից միայն մեկը չի մանրամասնել, թե ինչ օպերացիոն համակարգից է օգտվում, իսկ մեկն էլ տեղեկացրել է, որ պարզապես չգիտի՝ ինչ օպերացիոն համակարգ է տեղադրված իր համակարգչային սարքում: Սակայն հարցվածների 74%-ն ասել է, որ իրենց համակարգչային սարքերում օգտագործում են լիցենզավորված օպերացիոն համակարգեր եւ հակավիրուսային ծրագրեր: 26%-ը համոզված չէ, որ ծրագրերը լիցենզավորված են:

Գծապատկեր 1. Օպերացիոն համակարգերի կիրառությունը (ըստ անձերի)

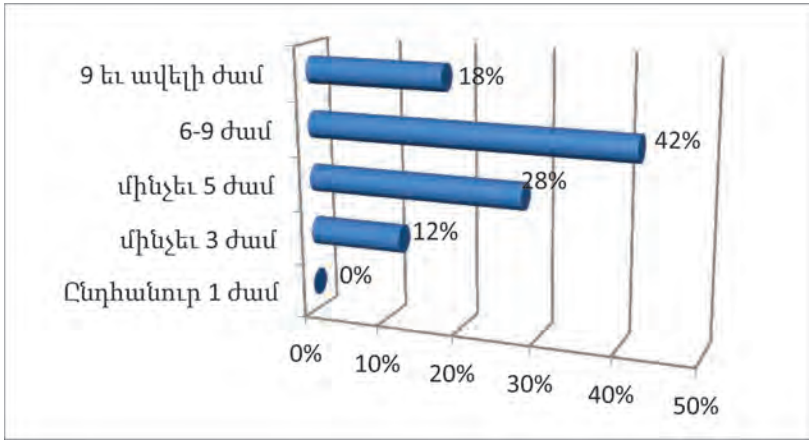


Հ.Գ. Յուրաքանչյուր մասնակից կարող էր ընտրել մեկից ավելի տարբերակ

Հետաքրքիր է դիտարկել նաեւ, թե օրական որքան ժամանակ են անցկացնում մասնակիցները համացանցում: Հարցի համար նախատեսված պատասխանների տարբերակները հինգն են. դրանցից մեկը՝ «ընդհանուր մեկ ժամ» տարբերակը, չի արժանացել մասնակիցներից եւ ոչ մեկի ուշադրությանը: Ըստ 2-րդ գծապատկերի՝ մասնակիցների 12%-ը կամ 6-ը, համոզված են, որ օրական համացանցից օգտվում են մինչեւ 3 ժամ: 28%-ը կարծում է, որ համացանցում անցկացնում է օրվա 5 ժամը:

Հարցվածների 42%-ը կարծում է, որ ներկայումս օրվա 6-9 ժամը ծախսում է միայն համացանցում: 18%-ը համոզված է, որ համացանցին տրամադրած օրական չափաբաժինն արդեն հասնում է 9 եւ ավելի ժամի: Հետեւաբար, հարցվածների 60%-ն օրական համացանցում անցկացնում է գրեթե այնքան, որքան աշխատանքային օրն է՝ շուրջ 8 ժամ: Հարցվածների մյուս 40%-ը, թեեւ համացանցից օգտվում է օրական մինչեւ 5 ժամ, խոստովանում է, որ այդ ժամաքանակի աճման միտումն ակնհայտ է:

Գծապատկեր 2. Համացանցում անցկացրած ժամերի քանակը (%)



Հարցին, թե ծախսած ժամաքանակի ո՞ր մասն են օգտագործում գործնական նպատակով, հարցվածների միայն 38%-ն է պատասխանել՝ «ամբողջությամբ», իսկ 62%-ը՝ «մասամբ»:

Արդյոք սնվելիս, քնելուց առաջ կամ արթնանալիս համակարգչային սարքերը կրկին հարցվածների կողքի՞ն են: Հարցվածների 64%-ը խոստովանել է, որ քնելիս իրենց մոտ են պահում համակարգչային սարքերը, մյուսները (36%)՝ ոչ:

44%-ը կամ հարցվածներից 22-ը նշել են, որ անգամ ընկերների հետ ճաշելիս հեռախոսի միջոցով օգտվում են համացանցից: Սակայն տվյալ 22-ից 10-ը խոստովանել են, որ ընկերներին ամենեւին էլ դուր չի գալիս դա, մյուս 10 հարցվածներն ասել են, որ ճաշելիս ընկերները եւս օգտվում են համացանցից:

Հաջորդ երեք հարցերի նպատակն է՝ պարզել այն հիմնական էլեկտրոնային հարթակները, որոնցից օգտվում են մասնակիցները: Համաձայն արդյունքների՝ հարցման մասնակիցներն ակտիվ են սոցիալական ցանցերում, օգտվում են տարբեր էլեկտրոնային փոստերից, մասամբ նաեւ՝ բլոգային հարթակներից:

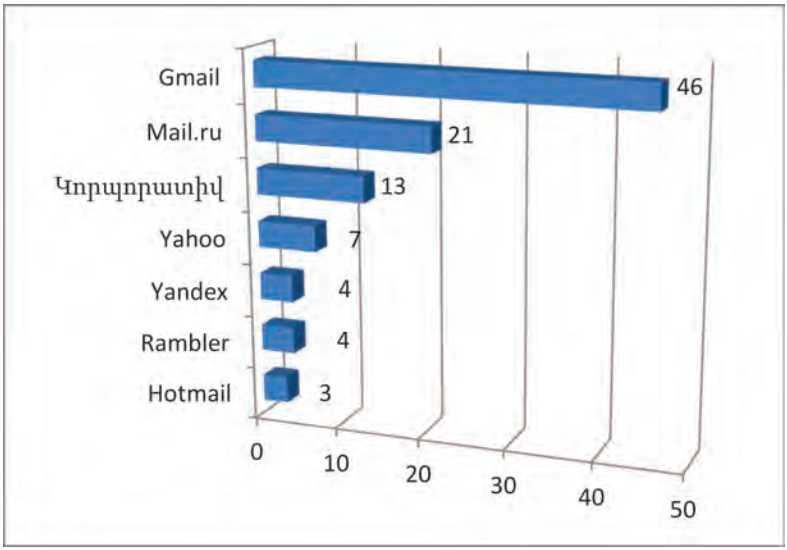
Հարցման բոլոր մասնակիցներն էջեր ունեն երկու եւ ավելի սոցիալական հարթակներում: Ընդ որում՝ բոլոր 50 մասնակիցներն էլ

օգտվում են «Ֆեյսբուք» սոցցանցից: Երկրորդ ամենատարածված հարթակը «Google+»-ն է: Ռուսական «Վկոնտակտե» սոցցանցը, ըստ կիրառության, հայտնվել է 3-րդ հորիզոնականում, որից օգտվում են հարցվածներից 18-ը: Իսկ ժամանակին Հայաստանում ամենաշատ ժողովրդականություն վայելող «Օդնոկլասնիկի» սոցցանցն այս հարցման աղյուսակում հայտնվել է նախավերջին հորիզոնականում՝ ընդամենը 16 օգտատերերի դրական պատասխանի շնորհիվ: Հարցվածներից 13-ը նշել են, որ էջեր ունեն նաեւ այլ սոցիալական ցանցերում:

Ի դեպ, մասնակիցների 22%-ը նշել է, որ արթնանալուց անմիջապես հետո ստուգում է սոցցանցերի իրենց էջերը, 26%-ը դա անում է արթնանալուց 15 րոպե անց: Հարցվածների մյուս կեսը առավոտյան չի շտապում ստուգել դրանք:

Գրեթե բոլոր հարցվածները նշել են, որ ունեն մեկից ավելի էլեկտրոնային հասցե: Ընդ որում՝ ամենակիրառելին այս խմբի շրջանում Gmail էլեկտրոնային փոստն է՝ 46 մարդ, այնուհետեւ Mail.ru-ն՝ 21: Հարկ է նշել, որ հարցվածների միայն 1/4-ն ունի կորպորատիվ աշխատանքային էլհասցե, ինչը հիմք է տալիս ենթադրելու, որ թե՛ աշխատանքային, թե՛ անձնական նամակագրությունը հիմնականում կատարվում է օտար՝ արեւմտյան կամ ռուսական կորպորացիաներին պատկանող էլփոստային ծառայությունների միջոցով (տե՛ս գծապատկեր 3):

Գծապատկեր 3. Ամենաշատ կիրառվող էլփոստի ծառայություններ



Հ.Գ. Յուրաքանչյուր մասնակից կարող էր ընտրել մեկից ավելի տարբերակ

Ինչ վերաբերում է բլոգային հարթակներին, այստեղ մասնակիցները փոքր-ինչ պասիվ են: Նրանց 20%-ը նշել է, որ ընդհանրապես չի օգտվում բլոգներից: 32%-ը նշել է, որ հիմնականում օգտվում է Wordpress եւ Blogspot բլոգային տիրույթներից, իսկ 4%-ը՝ նաեւ LifeJournal-ից: Սակայն այս շարքում առաջատար է համարվում «Թվիթեր» միկրոբլոգը, որից օգտվում է մասնակիցների 42%-ը՝ ակտիվության չափը չմանրամասնելով:

Կիբերհանցագործության սահմանումն ըստ հարցվածների

Հարցերի հաջորդ խումբը նպատակ ունի պարզելու, թե հարցման մասնակիցները երբեւէ եղե՞լ են կիբերհանցագործության թիրախ եւ արդյոք փորձո՞ւմ են պահպանել տեղեկատվական անվտանգության կանոնները:

Հարցին՝ «Ի՞նչ եք հասկանում «կիբերհանցագործություն» ասելով», հարցվածները տվել են հետեւյալ պատասխանները.

ԶԼՄ ոլորտի ներկայացուցիչների պատասխանները

1. Երբ համակարգչային ծրագրով քարտից ու համակարգչից նյութեր ու գումար են գողանում,
2. Համակարգչային անվտանգության դեմ ուղղված հանցատեսակ է: Այն ՀՀ քրեական օրենսգրքով նախատեսված հանցատեսակ է,
3. «Հարձակում» համակարգչի վրա եւ այնտեղից ինֆորմացիայի գողացում,
4. Վնասակար ծրագրերի մուտք, ընկերներից եկող վնասակար ինֆորմացիա,
5. Հաքերների հարձակում,
6. Ինտերնետի միջոցով կատարվող հանցագործություններ, հաքերային գործունեություն,
7. Վիրուսների տարածում, այլոց կայքեր մուտք գործել,
8. Պատասխան չկա,
9. Երբ կոտրում են անձնական հաշիվներ, էլփոստ, կայքեր եւ գողացված ինֆորմացիան օգտագործում հանցավոր նպատակներով,
10. Անձնական տվյալների օգտագործում անհայտ մարդկանց կողմից,
11. Անձնական տվյալների՝ երրորդ անձի կողմից հասանելիություն,
12. Առցանց հարթակում անձնական կյանքի գաղտնիության բացահայտում մեկ այլ անձի կողմից,
13. Անձնական հարթակում անօրինական գործունեություն,
14. Ես անհասկացող եմ,
15. Ինտերնետ տիրույթի օգտագործմամբ անձի/կազմակեր - պության տվյալների անօրինական օգտագործում, նրա տիրույթի ապօրինի ներթափանցում, կոտրում
16. Մուտք գործել ուրիշի տվյալների բազա, օգտվել փակ ինֆորմացիայից,

17. Հաքերների կողմից կայքերի, անձնական հաշիվների կոտրում եւ տվյալների գողացում,
18. Անձնական տվյալների, հեղինակային իրավունքի խախտում, սխալ տեղեկատվության մատուցում,
19. Կիբերանվտանգության դեմ ուղղված ցանկացած գործողություն,
20. Վիրտուալ տիրույթում կատարված հանցագործություն,
21. Անձնական տվյալների հափշտակություն եւ այլն,
22. Հանցագործություն, որը խախտում է մարդու իրավունքներն ու ազատություններն օնլայն հարթակում,
23. Օրինազանցություն համացանցում,
24. Հանցագործություններ, ուրիշի կյանքի ներխուժում վիրտուալ տիրույթում,
25. Անձի անձնական հաշիվների գաղտնազերծում, էլկայքերի տվյալների, նյութերի արգելափակում,
26. Առցանց տիրույթում հատուկ վիրուսային ծրագրերի միջոցով կատարվող բոլոր այն հանցագործությունները, որոնք հանցագործություն են նաեւ ոչ առցանց տիրույթում,
27. Արգելված արարք համացանցում
28. Վիրտուալ հանցագործություն իրական վտանգներով,
29. Որեւէ մարդու անհատական կամ բանկային տվյալների ձեռքբերում համակարգչի օգնությամբ շահադիտական նպատակներով,
30. Պատասխան չկա,
31. Պատասխան չկա,
32. Երբ հաքերային հարձակումների են ենթարկվում մարդիկ համացանցում գործողություններ կատարելիս,
33. Անօրինական գործողություն կոնկրետ կայքից ինֆորմացիա վերցնելու կամ այլ ինֆորմացիա տեղադրելու համար:

Հասարակական կազմակերպությունների ներկայացուցիչների պատասխանները

1. Կիբերտիրույթում իրականացվող հարձակումները տարաբնույթ նպատակներով,
2. Համացանցի ռեսուրսների օգտագործմամբ անձնական տվյալների ապօրինի զավթում,
3. Խաբեության միջոցով ինֆորմացիայի կորզում եւ դրա հետագա կիրառում այլ նպատակներով,
4. Էլեկտրոնային միջոցներից օգտվելով՝ մարդու/կազմակերպության անձնական տարածք ներխուժում,
5. Տեղեկատվության արտահոսք, անձնական կյանքի իրավունքի խախտում,
6. Ինֆորմացիոն տարածությունում կատարվող հանցագործություն, որի արդյունքում խախտվում են անձնական եւ հեղինակային իրավունքները,
7. Առանց իմ իմացության անձնական վիրտուալ տիրույթ ներխուժել եւ անձնական ինֆորմացիային ծանոթանալ/գողանալ,
8. Սոցցանցերի ջարդում եւ ինֆորմացիայի արտահոսք,
9. Վիրտուալ աշխարհում կատարված անօրեն գործունեություն,
10. Ոչ ֆիզիկական տիրույթում կատարված հանցագործություն,
11. Հանցագործություն, որը վնասում է հասարակությանը, սակայն զենքը շոշափելի չէ,
12. Անձի սոցցանցի կոտրում, տեղեկատվության ուսումնասիրում, տարածում կամ ձեռքբերում,
13. Համացանցում կատարված հանցագործություն,
14. Օնլայն տիրույթում հանցագործություն,
15. Համացանցի միջոցով կատարվող հանցագործություններ. այլ անձանց տվյալների օգտագործում, բանկային հաշվի կոտրում,
16. Ապօրինի ճանապարհով ինֆորմացիային տիրանալը տեխնիկական սարքերից,
17. Վիրտուալ հանցագործություն, հաքերային հարձակումներ, անձնական տվյալների հափշտակում:

Ինչպես երեւում է, մասնակիցներից միայն չորսն են հրաժարվել որեւէ սահմանում տալ այս հասկացությանը: Մյուսների սահմանումներում այն բնութագրվում է հիմնականում իբրեւ ապօրինի գործողություն կամ հանցագործություն:

Ինչեւէ, այս հարցին յուրաքանչյուր մասնակից սեփական տեսանկյունից է պատասխանել: Եթե մեկ սահմանման մեջ ամփոփվեն մասնակիցների պատասխանները, ապա կստացվի, որ «Կիբերհանցագործությունը որեւէ անձի կամ ընկերության վիրտուալ տիրույթ մուտք գործելն է՝ առանց տվյալ անձի կամ ընկերության համաձայնության կամ նախնական իրազեկման, որն ուղեկցվում է տվյալ տիրույթում առկա տվյալների անօրինական ուսումնասիրմամբ, տեղափոխմամբ կամ դրանց վնասմամբ, ինչն անօրինական գործողություն է եւ մարդու իրավունքների խախտում վիրտուալ տիրույթում»:

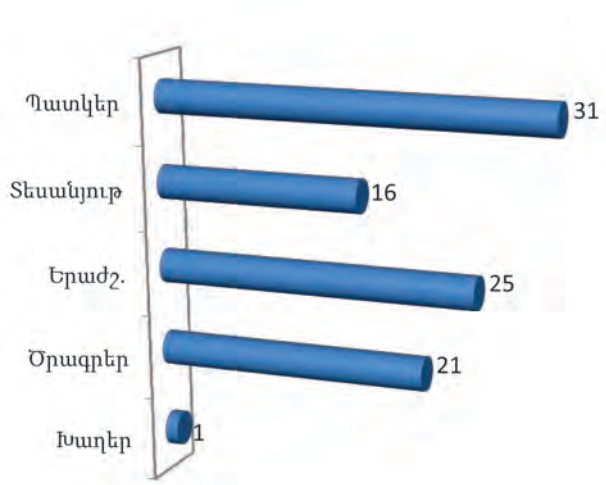
Համացանցից անվտանգ օգտվելու մշակույթը

Այժմ պարզենք, թե ինչ կանխարգելիչ կամ պաշտպանիչ միջոցներից են օգտվում հարցվածները կիբերհանցագործների թիրախում չհայտնվելու համար:

Հարցվածների 92%-ը պատասխանել է, որ իրենց համակարգչային սարքերը պաշտպանված են հակավիրուսային ծրագրերով: Մինչդեռ ընդամենը 68%-ի անձնական համակարգչային սարքերի մուտքն է արգելափակված գաղտնաբառով: Հարցվածների ուղիղ կեսը թույլ է տալիս, որ անձնական օգտագործման սարքից օգտվեն նաեւ իրենց հարազատները, ներառյալ երեխաները՝ խաղեր խաղալու կամ տարբեր ծրագրեր ներբեռնելու համար:

Մասնակիցների մեծ մասը՝ 80%-ը կամ 40 մարդ, ասում է, որ անձնական համակարգչային սարքերը միաժամանակ օգտագործում են ե՛ւ անձնական, ե՛ւ գործնական նպատակներով: Հարցվածների 86%-ը աշխատավայրի համակարգիչները կիրառում է նաեւ անձնական նպատակներով, օրինակ՝ սոցցանցեր կամ անձնական էլփոստեր մուտք գործելու համար: 56%-ն ասում է, որ աշխատանքային համակարգիչներում չի խուսափում պահել նաեւ անձնական տեղեկատվություն:

Գծապատկեր 4. Առավել հաճախ ներբեռնվող քոնթենթ (ըստ անձերի)



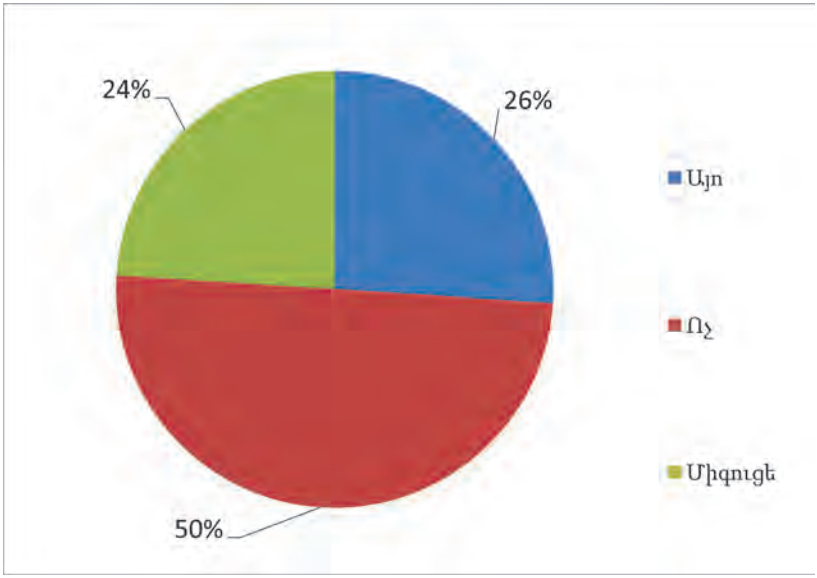
Ուշագրավ է նաեւ, որ հարցվածների կեսից ավելին՝ 54%-ը, իր անձնական եւ/կամ աշխատանքային փաստաթղթերը պահում է նաեւ այնպիսի առցանց պահուստներում, ինչպիսիք են Dropbox պահուստային հարթակը, Gmail էլփոստը եւ այլն: Նման դեպքերում օգտատիրոջ համար կարեւոր է, որ տեղեկությունն ապահով եւ անկորուստ պահվի համացանցում: Դա նախեւառաջ հնարավոր է անվտանգության նվազագույն կանոնները պահպանելու դեպքում:

Մինչդեռ հարցվածների 30%-ը խոստովանել է, որ սոցցանցերում եւ այլ տիպի էլեկտրոնային հաշիվներում աշխատանքն ավարտելուց հետո ոչ միշտ է սեղմում «Դուրս գալ» (Log out) հրահանգը: 22%-ը կամ 11 մարդ ասել են, որ իրենց էջերի գաղտնաբառը գիտեն նաեւ իրենց բարեկամները (ընկերները/գործընկերները):

Մասնակիցների 82%-ը նշել է, որ օգտվում է հանրային ազատ Wi-Fi կապից, սակայն նույն հարցվածների 62%-ը տեղյակ չէ, թե անվտանգության ինչ կանոնների պետք է հետեւել նման կապից օգտվելիս:

Ինչեւէ, հարցվածների 50%-ը համոզված է, որ իրենց համակարգչային սարքավորումներից տեղեկատվության կորուստ երբեւէ չի եղել: Մյուս 50%-ը ճիշտ հակառակ կարծիքն ունի. 26%-ը նշում է, որ համակարգչային սարքերից տեղեկատվության կորուստ է ունեցել, իսկ 24%-ը թեեւ համոզված չէ, սակայն չի բացառում նման կորուստը:

Գծապատկեր 5. Սարքերից տեղեկատվության կորուստ (%)



Թեեւ հարցվածների սարքերի մեծ մասն ապահովված է հակավիրուսային ծրագրերով, սակայն նրանց 78%-ը նշել է, որ իրենց համակարգիչներում եղել են վիրուսներ եւ վնասակար ծրագրեր: Հարցվածների 12%-ը համոզված չէ, որ եղել են վիրուսներ, եւ միայն 10%-ը կամ 5 մարդն է վստահ, որ իրենց համակարգչային սարքերում երբեք վնասակար ծրագրեր մուտք չեն գործել:

Վստահության աստիճանը սոցցանցերում շփումներում

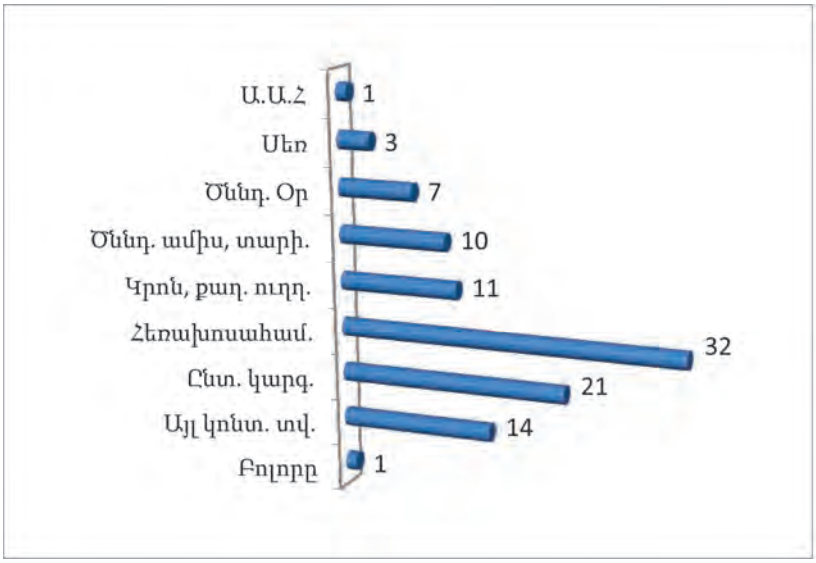
Հարցման արդյունքները ցույց են տալիս, որ անկախ սոցցանցերում ազատ շփումներից, յուրաքանչյուր օգտատեր ունի անձնական տվյալների հանրայնացման որոշակի սահման, որից այն կողմ տեղեկությունները համարում է խիստ մասնավոր:

Հարցվածների 84%-ն ասել է, որ սոցցանցերում միայն մասամբ է ներկայացնում իր անձին վերաբերող տվյալներ՝ որոշ տեղեկություններ համարելով խիստ մասնավոր: Դրանցից են՝ հեռախոսահամարը (նշել է 32 մարդ), ընտանեկան կարգավիճակի մասին տեղեկությունը (21 մարդ), այլ տիպի կոնտակտային տվյալները (14 մարդ), կրոնական, քաղաքական հայացքները (11 մարդ) եւ այլն:

«Արդյոք սոցիալական ցանցերում կապ հաստատո՞ւմ եք անծանոթ մարդկանց հետ» հարցին մասնակիցների 42%-ը տվել է դրական պատասխան, իսկ 58%-ը՝ բացասական:

Այն հարցին, թե «Երբեւէ ինչ-որ մեկը ջարդե՞լ է ձեր սոցիալական ցանցի պրոֆիլը եւ հանդես եկել ձեր անունից», հարցվածների 70%-ը պատասխանել է՝ «ոչ», 26%-ը կամ 13-ը՝ «այո» եւ միայն 2-ը՝ «չգիտեմ»:

Գծապատկեր 6. Անձնական տվյալներից ո՞րն եք համարում խիստ մասնավոր (ըստ անձանց թվի)



Հ.Գ. Յուրաքանչյուր մասնակից կարող էր ընտրել մեկից ավելի տարբերակ

Կեղծ էլեկտրոնային նամակներ

Հայտնի են դեպքեր, երբ ծանոթ ընկերությունների կամ ընկերների կեղծ էլեկտրոնային հասցեներից նամակներ են տարածվում՝ անհապաղ ֆինանսական օգնություն ցույց տալու կամ որոշ անձնական տվյալներ տրամադրելու խնդրանքով: Սույն հարցման մասնակիցներից նման իրավիճակում հայտնվել է միայն 3 մարդ, ովքեր դրական են պատասխանել հարցին՝ «Արդյոք տրամադրե՞լ եք տեղեկություն կեղծ էլեկտրոնային հասցեի՝ կարծելով, թե այն իրական հասցեատիրոջից է»: Մյուսները նշել են, որ նման իրավիճակում երբեւէ չեն հայտնվել:

Հետաքրքիր է նաեւ, որ հարցվածների 30%-ը նշել է, որ

էլեկտրոնային փոստի հասցեով ստացված անծանոթ նամակներն անմիջապես չի ջնջում: 6 մարդ կամ հարցվածների 12%-ն ասել է, որ իրենց էլեկտրոնային փոստի հասցեն կոտրել են եւ հանդես են եկել իրենց անունից: 40 մարդ կարծում է, որ իրենց հաշիվները երբեւէ չեն կոտրվել: Եվ միայն 4-ը ստույգ պատասխան չունեն:

Կիբերհանցագործության օրինակներ բջջային հեռախոսների միջոցով

Հեռախոսային վիրուսների պատճառով ֆինանսական կորուստ ունեցել են հարցվածներից ընդամենը երկուսը: Մյուս 48 մասնակիցները կարծում են, որ եթե երբեւէ իրենց բջջայիններում վիրուս է հայտնվել, ապա դա բջջայինի համարի հաշվին առկա գումարի նվազման կամ կորստի պատճառ չի հանդիսացել:

Մեկ հարցվածի հեռախոսի էկրանի արգելափակման արդյունքում հայտնվել է ազդանշան, որը զգուշացրել է, որ պետք է «տուգանք» վճարել այն ապաարգելափակելու համար: Սակայն մյուս 49 հարցվածները նման դեպք չեն մտապահել:

Մեր օրերում բջջային սարքի կորուստը հաճախադեպ երեւույթ է: Քիչ չեն դեպքերը, երբ մարդիկ մոռանում են իրենց բջջայինները տարբեր վայրերում՝ գրասենյակներում, ընկերների տանը, սրճարաններում, տաքսի ծառայության մեքենաներում եւ այլ վայրերում:

50 հարցվածներից 7-ը եւս հայտնվել են նման իրավիճակում: Նրանցից մեկի հեռախոսն այդպես էլ չի գտնվել: Մյուսներինը գտնվել են, սակայն նրանցից երկուսը չեն բացառում, որ նախքան իրենց վերադարձնելն այդ հեռախոսներն օգտագործվել են երրորդ անձանց կողմից:

Հարցին՝ «Երբեւէ բջջային հեռախոսում հայտնվե՞լ է այնպիսի ծրագիր, որը դուք չեք ներբեռնել», հարցվածների 76%-ը բացասական պատասխան է տվել, 10%-ը՝ դրական, իսկ 4%-ը՝ ո՛չ ժխտել, ո՛չ հաստատել է:

Մասնակիցներից 3-ը նշել են նաեւ, որ իրենց բջջային հեռախոսները կամ պլանշետը ենթարկվել են այլ տիպի կիբերհանցա-

գործության: Նրանցից միայն մեկն է մանրամասնել, ասելով, որ վարկաբեկման նպատակով նկարներ են ներբեռնել իր սարքում: Նմանատիպ կիբերհարձակման դեպքեր եղել են նաեւ հարցվածներից երեքի նոութբուքերի վրա:

Հարցվածներից մեկն էլ նշել է, որ համացանցի միջոցով ունեցել է նույնականացման քարտի տվյալների կորուստ:

«Ի՞նչ կանեք, եթե ձեր համակարգչային սարքը ենթարկվի կիբերհարձակման» հարցին, մասնակիցների կեսից ավելին՝ 51%-ը, պատասխանել է, որ կդիմի մասնագետի օգնությանը, 22%-ն ընտրել է ընկերոջ օգնության տարբերակը, իսկ 28%-ը կշտապի դիմել իրավապահ մարմիններին:

ԸՆԴՀԱՆՈՒՐ ԵԶՐԱԿԱՑՈՒԹՅՈՒՆՆԵՐ

• Ե՛վ լրատվամիջոցների, ե՛ւ քաղաքացիական հասարակության ներկայացուցիչներն ակտիվորեն օգտվում են ինչպես համակարգչային սարքերից, այնպես էլ համացանցից: Մշտապես առցանց հասանելիություն ապահովելու համար լրագրողներն ու քաղաքացիական հասարակության ներկայացուցիչները ձգտում են ունենալ շարժական այնպիսի համակարգչային սարքեր, ինչպիսիք են նոութբուքը, պլանշետը եւ սմարթֆոնը: Անձնական սարքերին զուգընթաց, օգտագործում են նաեւ աշխատանքային համակարգիչները:

• Հարցման թիրախային խմբի կեսից ավելին աշխատում է Windows օպերացիոն համակարգով (ՕՀ): Մեծ տոկոս են կազմում նաեւ Android ՕՀ-ով աշխատող սարքերը: Քիչ չեն նաեւ iOS եւ Mac օպերացիոն համակարգերից օգտվողների թիվը: Չնչին է բաց կոդով գրված ՕՀ-ից օգտվողների թիվը: Իսկ նման ծրագրերը լիցենզիա չեն պահանջում, հետեւաբար անվճար են: Լրատվամիջոցների եւ հասարակական կազմակերպությունների համար լիցենզիոն համակարգչային ծրագրեր ձեռք բերելը հավելյալ ֆինանսական ռեսուրս է պահանջում: Մինչդեռ անցնելով բաց կոդով գրված ՕՀ-երի՝ ֆինանսական համեստ եկամուտներ ունեցող կազմակերպությունները կարող են հավելյալ տնտեսում ունենալ, ինչպես նաեւ խուսափել ոչ լիցենզիոն՝ անօրինական ճանապարհով ձեռք բերված ծրագրերի կիրառումից, ինչը բարձրացնում է անվտանգության խոցելիությունը:

• Համացանցից օգտվելու ժամաքանակի աճման միտումն ակնհայտ է: Լրագրողների ու քաղաքացիական հասարակության ներկայացուցիչների մեծ մասը համացանցն օգտագործում է ավելի շատ, քան աշխատանքային օրվա համար նախատեսված 8 ժամն է: Այլ խոսքով, օրվա առնվազն 1/3 մասն անցնում է էկրանի առջեւ: Օգտատերերն օնլայն են սնվելիս,

երթեւեկելիս, աշխատանքային քննարկումների ժամանակ, իսկ քնելուց առաջ սիրելի սմարթֆոնները պարտադիր «տեղավորում են բարձի տակ»: Արդյոք սա չի՞ նշանակում, որ կյանքն այլեւս սիմբիոզ է՝ բաղկացած իրական եւ վիրտուալ պահերից, եւ լինում են պահեր, երբ դժվար է տարանջատել իրականը վիրտուալից:

• Լրագրողների եւ քաղհասարակության ներկայացուցիչների համար վիրտուալ աշխարհում հաղորդակցվելու եւ/կամ տեղեկատվություն հաղորդելու, սպառելու եւ պահպանելու հիմնական միջոցները համարվում են սոցիալական ցանցերը, լրատվական կայքերն ու էլփոստերը: Ի տարբերություն իրական աշխարհի, որտեղ տարածք հնարավոր է ձեռք բերել հիմնականում գնելու կամ վարձակալելու միջոցով, վիրտուալ աշխարհում յուրաքանչյուր օգտատեր հնարավորություն ունի անվճար հիմունքներով անսահմանափակ տիրույթ ձեռք բերելու այնպիսի միջավայրում, որտեղ ունի իրեն հետաքրքրող տեղեկատվական համայնք: Արդյունքում՝ յուրաքանչյուրն այսօր ունի մի քանի էջ սոցիալական տարբեր կայքերում, մի քանի էլհասցե՝ էլեկտրոնային փոստային ծառայություններում եւ դրանք օգտագործում է տարբեր նպատակներով:

• Թվային դարաշրջանում շատ կարեւոր են նոր մեդիա տեխնոլոգիաներից օգտվելու հմտությունները, սակայն կրկնակի կարեւոր՝ անվտանգ օգտվելու կարողությունը՝ հաշվի առնելով օրեցօր ավելացող կիբերհանցագործության ցուցանիշները: Հարցվածների մեծ մասը, կարծես, ճիշտ սահմանում է տալիս, թե ինչ է կիբերհանցագործությունը, սակայն անվտանգության հարցերին վերաբերող պատասխաններից երեւում է, որ առայժմ բավարար չի գիտակցում սեփական անձի համար կիբերհանցագործությունից բխող վտանգներն ու վնասները: Համակարգչային սարքերում հակավիրուսային ծրագրերի առկայությունը դեռ բավարար չէ համոզված լինելու համար, որ համակարգչային սարքը եւ

դրանում առկա տեղեկատվությունը պաշտպանված են:

• Համակարգչային սարքի անվտանգությունն ապահովելու համար անհրաժեշտ է հետեւել մի շարք կանոնների: Իսկ հարցման արդյունքները ցույց են տալիս, որ բոլորը չէ, որ հետեւում են դրանց: Օրինակ՝

- o համակարգչային սարքեր մուտք գործելը պաշտպանված չէ գաղտնաբառով,
- o համակարգչային սարքերից ազատ օգտվում են հարազատները, այդ թվում՝ երեխաները, ովքեր կարող են համացանցից ներբեռնել ցանկացած ծրագիր՝ զուգահեռաբար տարատեսակ վիրուսներ,
- o ոչ միշտ են կայքերում աշխատանքն ավարտելիս՝ վերջում սեղմում «Դուրս գալ» (Log out) հրահանգը:

Քանի որ նշվել էր, որ ՋԼՄ կամ ՀԿ ոլորտների ներկայացուցիչների անձնական համակարգչային սարքերն օգտագործվում են նաեւ գործնական նպատակներով, դա նշանակում է, որ տվյալ սարքում պահվող այլ անձանց կամ կազմակերպություններին վերաբերող տվյալների գաղտնիությունը վտանգված է, եթե անվտանգության տեսանկյունից անփույթ են օգտվում:

• Հարցվածների շրջանում չկար մեկը, ով բացառեր երբեւէ իր սարքերում օտար, անցանկալի ծրագրի կամ վիրուսի հայտնաբերումը: Սա նշանակում է, որ բոլոր մասնակիցները առնվազն մեկ անգամ եղել են կիբերհանցագործության զոհ: Այսպիսով կիբերհարձակումներն իրականացվում են յուրաքանչյուրի նկատմամբ՝ անկախ պաշտոնեական դիրքից, զբաղվածությունից եւ սոցիալական կարգավիճակից: Հարցվածներից մի քանիսի ներկայացրած օրինակները հուշում են, որ կատարվում են նաեւ թիրախավորված հարձակումներ: Հաշվի առնելով կիբերհանցագործությունների ավելացումն ու

կատարելագործումը՝ թիրախավորված հարձակումներն ավելի հաճախակի կդառնան: Ուստի պահանջվում է ավելի մեծ զգոնություն տվյալ ոլորտների ներկայացուցիչների կողմից՝ իրենց համակարգչային սարքերի տեղեկատվական անվտանգության համակարգերը ուժեղացնելու միջոցով:

• Ցանկացած տեղեկություն, որը կարող է հավելյալ միջոց դառնալ կիբերհանցագործների համար անձի եւ նրան շրջապատող հարազատների անվտանգությունը խարխլելու նպատակով՝ գտնվելու վայրը, ընտանեկան կարգավիճակը, երեխաների անունները, ուսման եւ հանգստի վայրերը, կոնտակտային տվյալները եւ այլն, պետք է զերծ պահել համացանցից: Մասնակիցների մի մասը պնդում էր, որ սոցիալական ցանցերում չի հաղորդում իր անձին վերաբերող խիստ մասնավոր տեղեկատվություն:

• Հարցվածների նշած կիբերհանցագործության օրինակները, որոնք տեղի են ունեցել բջջային հեռախոսների միջոցով, թեեւ զանգվածային բնույթ չեն կրում, սակայն մտահոգության տեղիք են տալիս: Անկախ այն բանից՝ նման գործողությունների հետեւում կանգնած են ներքին թե արտաքին ուժեր, մեկ մարդ թե կազմակերպված խումբ՝ մի բան հստակ է. Հայաստանի քաղաքացին եւս այս մեծ սարդոստայնում գտնվում է կիբերհանցագործների թիրախում, որին զոհ չդառնալու համար անհրաժեշտ են բարձր զգոնություն եւ մշտապես լրացվող գիտելիքներ տեղեկատվական անվտանգության ոլորտի վերաբերյալ:

ՄԱՍ 5

ՀԵՏՍՆՈՈՒԴԵՆՅԱՆ ԱՇԽԱՐՀԸ. ԻՆՉՊԵ՞Ս ՀԱՅՏՆՎԵՑԻՆՔ ՀԱԿԱՈՒՏՈՊԻԱՅՈՒՄ

ՀԵՏՍՆՈՈՒԴԵՆՅԱՆ ԱՇԽԱՐՀԸ. ԻՆՉՊԵ՞Ս ՀԱՅՏՆՎԵՑԻՆՔ ՀԱԿԱՈՒՏՈՊԻԱՅՈՒՄ

Սամվել Մարտիրոսյան

Վերջին երկու տասնամյակների ընթացքում, երբ հեռահաղորդակցման ոլորտը յուրահատուկ տեխնոլոգիական վերելք ապրեց, հասարակության շրջանում ծնվեցին բազմաթիվ լեգենդներ պետությունների կողմից գաղտնալսումների վերաբերյալ: Սակայն այդ սահմռկեցուցիչ լեգենդներն ակնթարթորեն մանկական հեքիաթի վերածվեցին, երբ մամուլում լույս տեսավ ԱՄՆ հատուկ ծառայությունների նախկին աշխատակից Էդվարդ Սնոուդենի տրամադրած փաստաթղթերը:

Դեռեւս հակաուտոպիական գրականությունից հայտնի է, որ մարդիկ ապրել են սպասելիքներով, որ պետությունը տոտալ վերահսկողություն է իրականացնելու հասարակությունում: Չնայած շատ հակաուտոպիստական գաղափարներ, որոնք թվում էին խիստ անիրատեսական, իրականացվում էին սպասվածից շատ ավելի աննկատ: Օրինակ՝ Ջորջ Օրուելի «1984» հակաուտոպիական վեպում նկարագրված թվացյալ ծայրահեղ բռնապետությունն իրականում գոյություն ուներ Խորհրդային Միությունում: Պարզապես, գրքերում այդ ամենն ավելի խտացված եւ ընդլայնված է ներկայացված: Սակայն առանձնապես տարբերություն չկար. ավելի շատ ռեսուրսների խնդիր էր: Խորհրդային Միության համար Օրուելի «1984»-ում ներկայացված հասարակությունը երազանք էր, որն իրականություն դարձնելու համար պահանջվում էին ֆինանսական մեծ ներդրումներ:

Գաղտնի թե բացահայտ բոլորին հետեւելու ցանկությունը մշտապես հանդիսացել է բռնապետությունների ամենամեծ երազանքը: Այդ նպատակով էլ ստեղծված հատուկ գաղտնի ծառայությունները լրտեսել են սեփական ժողովրդին, սակայն լիակատար հաջողության հասնելու հնարավորություն չեն ունեցել: Արդյունավետությունն ավելի բարձրացնելու համար այդ «արդար» գործին փորձել են ներգրավել սեփական ժողովրդին, որը եւս ոչ միշտ է լիարժեք արդյունք տվել:

Անցան տարիներ, ստեղծվեց համացանցը, արբանյակային լրտեսության մասին լեգենդները սկսեցին տարածվել: Առաջինն այն մասին էր, որ ԱՄՆ-ն իր դաշնակիցների հետ գործարկել է մի գլոբալ լրտեսական համակարգ, որի միջոցով, օգտագործելով արբանյակային եւ այլ ռադիոէլեկտրոնային տեխնոլոգիա, գաղտնալսումներ է իրականացնում աշխարհով մեկ: Այդ լրտեսական համակարգը, ըստ ասեկոսեների, կոչվում էր «էշելոն»: 2001 թ. Եվրոպան մտահոգվեց ամերիկյան լրտեսական համակարգով: Եվրախորհրդարանն այդ առնչությամբ խոր վերլուծություն հրապարակեց[11]: Հարկ է նշել, որ խոսքը ոչ միայն ԱՄՆ-ի, այլեւ ԱՄՆ, Մեծ Բրիտանիա, Կանադա, Ավստրալիա եւ Նոր Զելանդիա համատեղ գործողությունների մասին է, որոնց լրտեսական համագործակցությունն ընդհանուր Five Eyes անվանումն է ստացել:

Արդեն այն ժամանակ պարզ էր, որ նշված հինգ երկրները մեծ ջանքեր են գործադրում համաշխարհային տեղեկատվական հոսքերին տիրանալու համար: Բացի տնտեսական լրտեսությունից եւ անվտանգության հարցերից, կասկածներ կային, որ գաղտնալսման են ենթարկվում նաեւ տվյալ երկրների համար հետաքրքրություն ներկայացնող որոշ խմբերի ներկայացուցիչներ: Ավելին՝ հարց էր առաջանում, թե ինչպե՞ս են ընտրվում գաղտնալսման թիրախները: Շրջանառվում էին լեգենդներ, որ համակարգը գաղտնալսումներն սկսում է այն ժամանակ, երբ ցանկացած անհատ զանազան բանալի բառեր է կիրառում: Օրինակ՝ եթե նամակում օգտագործում եք «ռումբ» կամ «ահաբեկչություն» բառերը, համակարգը սկսում է հետեւել ձեզ: Շատ գեղեցիկ, սակայն անհիմնաստ լեգենդ: Քանի որ հասկանալի է, որ նման բանալի բառեր օգտագործում են ամենաանվնաս անձինք, մինչդեռ ահաբեկիչներն ունեն իրենց կոդային համակարգը, որն անընդհատ փոփոխվում է:

Երբ Էդվարդ Սնոուդենը իր փաստաթղթերը փոխանցեց լրագրող Գլեն Գրինվալդին, եւ սկսվեցին հրապարակումները, մարդկությունը

11. European Parliament, REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)) , 11 July 2001, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//EN

հասկացավ, որ բոլոր հակաուտոպիական վեպերի հեղինակները շատ համեստ եւ զուսպ պատկերացումներ ունեին բռնապետությունների կողմից մարդկանց հետեւելու ներուժի մասին: Քանի որ պարզ դարձավ, որ ամերիկյան եւ բրիտանական գաղտնի ծառայությունները փաստացի ստեղծել են մի համակարգ, որը մեզ տեղափոխել է ինչ-որ կիբերպանկային իրականություն: Ապագան արդեն այստեղ է, պարզապես, մենք տեղյակ չենք դրա մասին:

Այն, ինչ աստիճանաբար բացահայտվում է Սնոուդենից հետո, թույլ է տալիս հասկանալ, որ ԱՄՆ ազգային անվտանգության ծառայությունը (National Security Agency (NSA) եւ Բրիտանիայի կառավարական հաղորդակցության կենտրոնն (Government Communications Headquarters (GCHQ) իրականացնում էին գլոբալ հետախուզում, որի թիրախում են Երկիր մոլորակի բոլոր բնակիչները: Օգտվելով աշխարհում համացանցի եւ բջջային տեխնոլոգիաների ներթափանցումից՝ գաղտնի ծառայությունները տարիներ շարունակ փաստացի հետեւել են աշխարհի գրեթե յուրաքանչյուր բնակչի: Իհարկե, ինչ-որ անձանց ավելի հանգամանորեն են հետեւել, սակայն տեղեկատվություն հավաքվել է գրեթե բոլորի մասին. դրա համար օգտագործվել են էլեկտրոնային փոստի ծառայությունները, սոցիալական ցանցերը, հեռախոսները, դրանցում տեղադրված հավելվածները: Նույնիսկ Angry Birds համակարգչային խաղը հանդիսացել է գործիք, որի միջոցով վերլուծվել է հեռախոսի տիրոջ բնավորությունը: Հավաքել են մարդկանց գրառումները, հեռախոսազանգերը, միմյանց հետ տարբեր հարթակներում կապերը, աշխարհագրական վայրի փոփոխությունները եւ այլ տեղեկություններ: Եվ այդ ամենը համադրելով՝ ստեղծել են յուրաքանչյուրի սոցիալական պատկերը: Փաստացի, ԱՄՆ-ի ազգային անվտանգության ծառայությունը եւ Բրիտանիայի կառավարական հաղորդակցության կենտրոնը կարող են ավելի շատ բան իմանալ մեր մասին, քան մենք ինքներս:

Այս ամենն անցյալում չէ. շատ հավանական է, որ ներկան շատ ավելի տպավորիչ է, քանի որ Սնոուդենը չի տիրապետել բոլոր տվյալներին: Բացի այդ, նրա տեղեկությունները սահմանափակվում են 2012 թվականով: Շատ հավանական է, որ այսօր լրտեսական

համակարգը շատ ավելի կատարելագործված է:

Սնոուդենի բացահայտումներն էլեկտրաշոկի ազդեցություն ունեցան հանրության վրա: Մինչեւ Սնոուդենի ի հայտ գալը, հայտնի էին կրիպտոանարխիստների շատ նեղ խմբեր, որոնք կոչ էին անում հնարավորինս թաքնվել կառավարություններից, օգտագործել գաղտնագրման համակարգեր: Այդ ժամանակ մեծամասնությունը կրիպտոանարխիստներին համարում էր կիսացնդած, բայց զվարճալի դեմքեր: Մինչդեռ այսօր կրիպտոանարխիստներն ունեն բոլոր իրավունքները բացականչելու՝ «Մենք ձեզ զգուշացնո՛ւմ էինք»: Այսօր նրանց ձայնն ավելի լսելի է դառնում:

Շարքային քաղաքացիներն արդեն մտահոգվում եւ փորձում են միջոցներ ձեռնարկել անձնական կյանքն ավելի պաշտպանված դարձնելու համար: Հետզհետե ավելի շատ են տարածվում գաղտնագրման համակարգերը, որոնք այս պահին դեռ անխոցելի են համարվում ԱՄՆ ազգային անվտանգության ծառայության եւ Բրիտանիայի կառավարական հաղորդակցության կենտրոնի մասնագետների համար: Օրինակ՝ TextSecure պաշտպանված կարճ հաղորդագրությունների համակարգն արդեն մոտ մեկ միլիոն ներբեռնում ունի «Android» համակարգով աշխատող հեռախոսների վրա: Իսկ մասնավոր ցանցային ծառայություններ տրամադրողներն անցնում են ավելի պաշտպանված համակարգերի, որպեսզի չկորցնեն իրենց բաժանորդներին: Օրինակ՝ երբ պարզ դարձավ, որ «Ֆեյսբուքը» մեծաքանակ տվյալներ է տրամադրել ամերիկյան գաղտնի ծառայությանը, իսկ «Թվիթերը»՝ ոչ, սկսվեց օգտատերերի մեծ թվով արտահոսք մի ցանցից մյուսը:

Այսօր օգտատերերի տվյալների պաշտպանությունը լուրջ մտահոգության առիթ է տեխնիկական համայնքի համար, քանի որ օգտատերերի անձնական կյանքի պաշտպանությունը, իրականում, բավականին բարդ գործընթաց է եւ պահանջում է գիտելիք ու հմտություն:

Սնոուդենի բացահայտումները բերեցին նրան, որ տեխնիկական համայնքը մտահոգվեց կապի ընդհանուր գաղտնագրման հարցերով: Օրինակ՝ այսօր, եթե այցելում եք որեւէ լրատվական կամ ժամանցային կայք, ձեր կապն իրականացվում է բաց http հոսքերով,

ինչը թույլ է տալիս տեսանելի լինել երրորդ կողմի՝ ձեր մատակարարի (պրովայդերի) կամ գաղտնի ծառայության ներկայացուցչի համար: Երբ օգտվում եք, օրինակ՝ բանկային համակարգից կամ գնումներ եք կատարում ցանցում, ապա սկսում եք օգտվել պաշտպանված https արձանագրությունից: Այս դեպքում երրորդ կողմը չի կարող տեսնել, թե ինչ տվյալներ եք փոխանցում ցանցով, չի կարող գողանալ ձեր գաղտնաբառը եւ այլն:

Մինչեւ վերջերս https արձանագրությունը կիրառվում էր հիմնականում բանկային եւ առեւտրային համակարգերում: Նույնիսկ էլեկտրոնային փոստերը եւ շատ սոցիալական ցանցեր սա չէին կիրառում: Օրինակ՝ «Ֆեյսբուքը» մինչեւ վերջերս հնարավորություն էր տալիս ակտիվացնելու այդ արձանագրությունը, սակայն առանց հատուկ միջամտության կապը տրամադրում էր բաց միջոցով: Yahoo փոստը նման հնարավորություն ընձեռեց 2012 թ.-ից հետո: Սնոուդենը «դրդեց» այդ ծառայություններին անցնել պաշտպանված կապի:

Բայց սա բավարար չէ: Նախկինում կարծում էինք, որ անձի վերաբերյալ խոցելի տեղեկատվությունը նրա անձնական նամակագրություններն են: Սակայն վերջին բացահայտումները ցույց տվեցին, որ գաղտնի ծառայությունները հնարավորություն ունեն, մեծաքանակ տեղեկատվություն մշակելով, անձի մասին կարծիք կազմելու՝ հիմնվելով նրա՝ սոցիալական կայքերում առկա կապերի, հետաքրքրությունների, կարդացած հոդվածների, դիտած տեսանյութերի վրա:

Վերջերս Google ընկերությունը հայտարարեց, որ այսուհետ կայքերը որոնողական համակարգում կդասակարգվեն նաև ըստ նրանց պաշտպանված մուտքի: Այսինքն՝ այն կայքը, որն այցելուին տեղեկությունը տրամադրում է https արձանագրության միջոցով, որոնողական համակարգում ավելի առաջնային հորիզոնականում կլինի, քան այն կայքը, որը չի կիրառում այդ համակարգը: Https-ի կիրառության շնորհիվ գաղտնալսող կառույցները կամ անհատներն ի վիճակի են լինում տեղեկություն ստանալ միայն այն մասին, թե օգտատերն ինչ կայք է այցելել, սակայն թե որ հոդվածներն է ընթերցել եւ որ տեսանյութն է դիտել, երրորդ կողմին հասանելի չի լինում:

Google-ի անվտանգության համակարգը թույլ չի տալիս երրորդ

կողմին տեղեկանալ օգտատերերի կողմից որոնվող բառերի, հետաքրքրությունների շրջանակի, ինչպես նաեւ այն մասին, թե ինչպես են դրանք փոփոխվում ամիսների ընթացքում: Ի տարբերություն Google համակարգի՝ Bing եւ Yandex համակարգերը նման պաշտպանություն չունեն, քանի որ դեռ չեն կիրառում https արձանագրությունը, այլ կերպ ասած՝ ապրում են նախասնոուդենյան դարաշրջանում:

Գուցե ոմանց համար նման գործողությունները կարեւոր չեն, ոմանք էլ կարծում են, թե իրենք այդքան էլ կարեւոր չեն գաղտնի ծառայությունների համար: Սակայն պետք չէ թերագնահատել սեփական անձի նկատմամբ նման ծառայությունների հետաքրքրությունը: Անկախ անձի սոցիալական կամ այլ կարգավիճակից՝ նրան հետեւելու համար այսօր արդեն ծախսվում են միլիարդավոր դոլարներ: Իսկ ժամանակները շատ արագ են փոխվում: Այսօր նման մասշտաբի գաղտնալսում իրականացնելու հնարավորություն ունեն աշխարհի մի քանի երկրներ, որն էլ անում են առանց հատուկ ճնշում գործադրելու:

Սակայն չի բացառվում, որ մոտ ապագայում գաղտնալսողների թիվը մեծանա, եւ դրանց շարքերում լինեն ոչ միայն երկրներ, այլեւ մասնավոր կորպորացիաներ, որոնք նույնպես նման գործընթաց սկսելու հնարավորություն ունեն:

Սնոուդենի ի հայտ գալը շատ բան բացահայտեց, որը, ցավոք, հասարակությունը շատ դանդաղ է գիտակցում:

ՄԱՍ 6

ՀԱՅԱՍՏԱՆԻ ԿԻԲԵՐԱՊԱԳԱՆ

ՀԱՅԱՍՏԱՆԻ ԿԻԲԵՐԱՊԱԳԱՆ

Սամվել Մարտիրոսյան

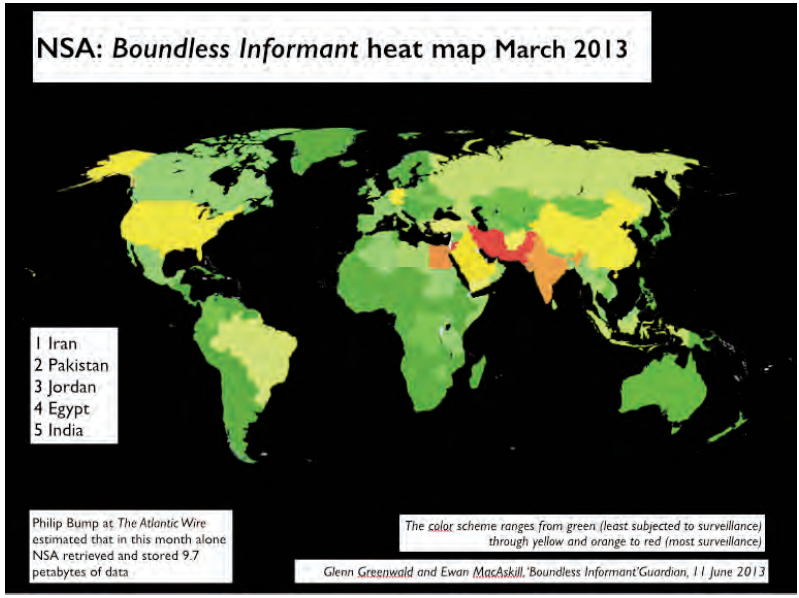
Հետսնոուդենյան դարաշրջանում է հայտնվել նաեւ Հայաստանը եւ, միգուցե, առանց գիտակցելու կամ ձգտելու դեպի նման աշխարհ: Աշխարհ, որտեղ մի կողմից զանազան գաղտնի ծառայություններ փորձում են տիրանալ մարդկանց եւ պետությունների տեղեկատվությանը, մյուս կողմից՝ գլուխ են բարձրացնում մինչ այդ ընդհատակում գործող զանազան կրիպտոպանկեր, հաքերներ եւ այլ ձախ ծայրահեղական խմբեր, որոնք փորձում են պայքարել նման ճնշող պետական համակարգերի դեմ:

Հաճախ կարելի է լսել, թե Հայաստանը ոչ մեկին հետաքրքիր չէ՝ չհաշված մեր հարեւաններին, որոնք, հակառակը, մեծ հետաքրքրությամբ փորձում են այստեղից տեղեկատվություն կորզել: Սակայն հենց Սնոուդենի բացահայտումները ցույց տվեցին, որ մենք այդքան էլ անհետաքրքիր երկիր չենք: Այսպես, Սնոուդենը հայտնեց, որ ամերիկյան Ազգային անվտանգության ծառայության (National Secutity Agency (NSA) համակարգերից մեկը, որը կոչվում է Boundless Informant, թույլ է տալիս տեսնել, թե որ երկրից ինչ քանակությամբ տվյալներ են գողացվել վերջին 30 օրվա ընթացքում: Ըստ Սնոուդենի տրամադրած քարտեզի՝ Հայաստանը բավականին մեծ հետաքրքրություն է ներկայացրել այդ պահին ամերիկյան գործակալության համար, ավելի մեծ հետաքրքրություն, քան հարեւան Վրաստանը կամ Ադրբեջանը:

Այնպես որ, եթե նույնիսկ մենք մեզ համարում ենք ոչ կարեւոր երկիր, ուրիշներն արդեն վաղուց այդպես չեն համարում: Բացի դրանից, ակնհայտ է, որ մենք՝ որպես երկիր, հետաքրքրություն ենք ներկայացնում նաեւ այլ երկրների գաղտնի ծառայությունների համար, եւ, ամենայն հավանականությամբ, Հայաստանի դեմ իրականացվում են մի շարք տեղեկատվական հատուկ գործողություններ: Ինչպես նշվեց, անմիջականորեն հայտնի է, որ նման գործողություններ այստեղ կատարվում են Ադրբեջանի եւ Թուրքիայի հատուկ ծառայությունների կողմից: Չի բացառվում, որ դրանք կատարվում են

նաեւ Իրանի եւ Ռուսաստանի Դաշնության ծառայությունների կողմից՝ չնայած այդ մասին հստակ եւ ստուգված տվյալներ բաց աղբյուրներում չեն հայտնաբերվել:

Boundless Informant քարտեզի պատկերը



Արդեն արձանագրվել է առնվազն երկու դեպք, երբ անհայտ երկրների կողմից կիրառվել են հատուկ վիրուսային համակարգեր, որոնք հնարավորություն են տվել լրտեսելու բազմաթիվ երկրների պետական կառույցներին: Այսպես, Red October կոչվող վիրուսային համակարգը, որը, ամենայն հավանականությամբ, կապ ուներ Չինաստանի հետ, լրտեսում էր բազմաթիվ երկրների պետական կառույցներին: Հայաստանն ամենավարակված երկրներից մեկն է եղել՝ ըստ Կասպերսկի լաբորատորիայի տվյալների[12]: Իսկ 2014 թ. հայտնաբերված Turla կամ Snake կոչվող վիրուսային համակարգը,

12. The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies, http://securelist.com/blog/incidents/57647/the-red-october-campaign/

որը, ենթադրաբար, կապ ուներ Ռուսաստանի գաղտնի ծառայությունների հետ, Հայաստանի տարածքն օգտագործել է այլ երկրների դեսպանատների ներքին համակարգերը վարակելու համար[13]: Դա նշանակում է, որ Հայաստանը ոչ միայն ինքն է թիրախ համարվում, այլեւ, ընդհանուր առմամբ, ակտիվորեն ներգրավված է հատուկ ծառայությունների տեղեկատվական «խաղերի» մեջ, ընդ որում՝ որպես պասիվ սուբյեկտ:

Տեղեկատվության անվերահսկելիության հետ կապված իրավիճակն աստիճանաբար ավելի է բարդանում: Դեռ մի քանի տարի առաջ ենթադրում էինք, որ զանազան հատուկ ծառայություններ ցանցի միջոցով կարող են հետեւել մարդկանց: Սակայն այսօր մի կողմից տեխնիկական միջոցներն են զարգացել, մյուս կողմից՝ մարդիկ ավելի ու ավելի շատ են օգտվում ցանցից, հոժարակամ ավելի շատ անձնական տեղեկատվություն են այնտեղ տեղադրում, ավելի շատ սարքեր են գործածում եւ ավելի շատ գործողություններ իրականացնում ցանցի միջոցով: Եթե շուրջ տասը տարի առաջ Հայաստանում միջին ընտանիքում նույնիսկ մեկ համակարգիչ էլ չկար, իսկ եթե կար, ապա մեկը մյուսին փոխարինելով օգտվում էին ընտանիքի բոլոր անդամները եւ նույնիսկ հարեւանները, ապա վերջին մի քանի տարիների ընթացքում Հայաստանի բնակչության կեսից ավելին հայտնվել է համացանցում: Ընդ որում, մեկ անձին արդեն հասնում է մի քանի համակարգչային սարք: Միայն բջջային հեռախոսահամարների քանակով Հայաստանում բաժանորդներն անցել են ներթափանցման 100%-ը (մեկ շնչին հասնում է միջինը 1,3 հեռախոսահամար): Համակարգիչներն էլ ներթափանցել են մեր առօրյան ինչպես քաղաքներում, այնպես էլ՝ գյուղական շրջաններում:

Եվ եթե օգտատերերի համար յուրաքանչյուր համակարգչային սարք պատուհան է դեպի լույս աշխարհ, ապա այն նաեւ դուռ է կիբերհանցագործների համար: Կիբերհանցագործներն այլեւս միայն սեփական նախաձեռնությամբ չէ, որ հանդես են գալիս կամ

13. Turla: Spying tool targets governments and diplomats, http://www.symantec.com/connect/blogs/turla-spying-tool-targets-governments-and-diplomats

կատարում պետությունների պատվերները: Այսօր ձեւավորվում են կիբերվարձկանների սեւ շուկաներ, որտեղ համապատասխան վճարի դիմաց կարելի է տարբեր պատվերներ կատարել: Հայաստանում եւս նկատելի է նման կիբերվարձկանների օգտագործումը՝ առայժմ քաղաքական դաշտում: Մոտ ապագայում չի բացառվում, որ ակտիվանան նաեւ կիբերհարձակումները որոշ անհատների եւ կազմակերպությունների վրա, որոնք կիրականացվեն ոչ միայն պետության, այլեւ մասնավոր հատվածի կողմից: Իսկ առցանց հարձակումները կազմակերպությունների կամ լրատվամիջոցների վրա եւ համացանցի միջոցով տարբեր ոլորտների իրավապաշտպանների հետապնդումներն աստիճանաբար կդառնան սովորական երեւույթ:

Այսպիսի զարգացումները, ամենայն հավանականությամբ, կստիպեն հայաստանյան հասարակությանն ավելի լուրջ վերաբերվել անձնական տվյալներին, անձնական կյանքի պաշտպանությանը: Նման միտումներ արդեն նկատվում են շատ երկրներում: Ամենուրեք այս թեմաները սկսում են հետաքրքրել հասարակության լայն զանգվածներին: Մինչ այժմ սրանք միայն փոքրաթիվ կիբերանարխիստների կողմից ստեղծվող խնդիրներ էին, որոնց շատերը լուրջ չէին վերաբերվում:

Հայաստանի համար եւս մոտ ապագայում նշմարվում է մի մեծ սկզբունքային խնդիր, որը կապ ունի երկրի ընդհանուր աշխարհաքաղաքական դիրքորոշման փոփոխման հետ: Վերջին զարգացումները հանգեցրին Հայաստանի անդամակցությանը Եվրասիական միությանը: Այս միությունը, չնայած հայտարարվում է որպես զուտ տնտեսական կառույց, կարող է իր հետ բերել նաեւ շատ ավելի լուրջ քաղաքական եւ հասարակական ինտեգրացիոն գործընթացներ անդամ երկրների միջեւ: Հայաստանն այս շարքում աշխարհագրորեն եւ տնտեսապես ամենափոքր, սակայն խոսքի ազատության, ցանցային ազատությունների եւ, ընդհանրապես, ժողովրդավարական գործընթացների տեսանկյունից՝ ամենազարգացած երկիրն է: Գաղտնիք չէ, որ Ռուսաստանում, Ղազախստանում եւ Բելառուսում այս ոլորտներում բազմաթիվ խնդիրներ կան: Եթե դիտարկենք զուտ համացանցի տեսանկյունից, ապա

Ղազախստանում պարբերաբար արգելափակման են ենթարկվում բազմաթիվ խոշոր սոցիալական մեդիաների հարթակներ[14]: Բելառուսը հայտնի է որպես մի երկիր, որը բազմիցս մեղադրվել է ընդդիմադիր գործիչներին եւ կազմակերպություններին ցանցի միջոցով լրտեսելու մեջ[15]: Ռուսաստանի Դաշնությունը կիրառում է կայքերի՝ առանց դատարանի որոշման արգելափակում[16], ներմուծում է քաղաքացիներին համացանցում հետեւելու նորացված հատուկ համակարգ[17] (տե՛ս նաեւ 7-րդ մաս):

Այս ամենը հաշվի առնելով, նաեւ տեսնելով ընդհանուր միտումները, որոնք տանում են դեպի համացանցում ավելի ուժեղ սահմանափակումների Եվրասիական միության նշված երկրներում՝ հարց է առաջանում՝ որքանո՞վ Հայաստանի իշխանությունները եւ հասարակությունը մոտ ապագայում կկարողանան դիմակայել նման մոտեցումների ներմուծմանը մեր երկրում: Այս հարցի պատասխանը կարող է տալ միայն Հայաստանի հասարակությունը՝ հստակ գործողությունների միջոցով: Այսօր ՀՀ իշխանությունները ցանցային ազատությունները սահմանափակելու որեւէ բացասական ձգտում չեն ցուցաբերում: Ավելին, այսօր Հայաստանը համարվում է համացանցային ազատ երկիր[18]: Հայաստանի կառավարությունը պատրաստակամություն է հայտնել ձեւավորելու մշտական գործող համացանցի կառավարման ֆորում, որը ենթադրում է, որ համացանցի վերաբերյալ կարեւորագույն հարցերը կառավարվելու են ոչ միայն իշխանությունների, այլեւ բոլոր շահագրգիռ մարմինների կողմից, որոնք ներառում են քաղաքացիական հասարակությունը, բիզնեսը, ակադեմիական եւ տեխնիկական համայնքները[19]:

Այսպիսով, այսօր կարեւոր է, որ հասարակության այն

14. WP Blocked in Kazakhstan and Kyrgyzstan, http://ma.tt/2011/06/wp-blocked-in-kazakhstan-and-kyrgyzstan/
15. COUNTRIES UNDER SURVEILLANCE, Belarus, REPORTERS WITHOUT BORDERS, http://en.rsf.org/surveillance-belarus,39746.html
16. РосКомСвобода, http://rublacklist.net/
17. СОРМ-3, http://www.mfisoft.ru/products/sorm/sorm3/yanvar
18. FREEDOM ON THE NET, Armenia, Freedom House report, 2013 , https://freedomhouse.org/report/freedom-net/2013/armenia#.VG5Fj1V7h5Q
19.Հայաստանում կստեղծվի ինտերնետի կառավարման համաժողով http://168.am/2013/03/08/192823.html

հատվածները, որոնք գիտակցում են հնարավոր բացասական եւ դրական զարգացումները, ցանցում հնարավորինս ակտիվորեն ներգրավվեն համացանցի կառավարման հարցերում, որպեսզի երկիրը կարողանա զարգանալ ճիշտ ուղղությամբ եւ չհայտնվի զանազան հոսանքների ազդեցության տակ:

Часть 7

РУССКАЯ РУ-летка

РУССКАЯ РУ-летка. РУНЕТ ПОД УГРОЗОЙ ГЛОБАЛЬНОЙ ПРЕДФИЛЬТРАЦИЕЙ ВСЕГО ИНТЕРНЕТ-ТРАФИКА

Саркис Дарбинян
Россия

В соответствии с данными отчета OpenNetInitiative, опубликованного в декабре 2010г. виртуальная сеть России представляла из себя достаточно открытое пространство, в котором отсутствовала политическая и нравственная цензура. Такая оценка была поставлена в результате международного мониторинга даже несмотря на то, что в тоже время Россия находилась на почетном 147 месте по свободе печати по результатам исследования Worlidewide Press Freedom Index.

Одна из наиболее авторитетных мировых организаций, исследующих свободу слова и осуществление цензуры в разных странах, Freedom House в 2011 году выставила Российской Федерации 52 бала из 100, называя российскую зону Интернета «почти свободным» пространством.

Препятствия в доступе: наличие инфраструктурных и экономических препятствий для доступа в Интернет, практика ограничения или блокирования определенных приложений или технологий, правовые, нормативные и другие административные формы технического контроля над Интернетом.

При выставлении рейтинга Freedom House учитывает такие факторы как препятствие в доступе к Интернету, наличие практики ограничения или блокирования определенных приложений или технологий, практики фильтрации и блокирования веб-сайтов, осуществление цензуры, самоцензуры и манипуляции информацией. Вместе с тем ключевым элементом исследования является нарушение прав пользователей Интернета в стране: степень защиты прав пользователей на неприкосновенность частной жизни, административные и иные ограничения интернет-активности пользователей,

уровень правительственного контроля над пользователями, наличие юридических и внесудебных последствий, вытекающих из деятельности пользователей в Интернете, таких как судебное преследование, тюремное заключение, случаи применения насилия или другие формы преследования.

В 2011г. действительно были зафиксированы немногочисленные случаи преследования гражданских активистов и блогеров, а в СМИ стали наблюдаться первые крупные проблемы со свободой прессы. В то же время российский Интернет представлял из себя достаточно свободную зону, в которой отсутствовало хоть какое-то специальное регулирование.

№139-ФЗ. Открытие ящика пандоры

Первой ласточкой наступающих серьезных изменений в государственной информационной политике стало появление 07 июня 2012г. законопроекта № 89417-6 о "чёрных списках сайтов" (О внесении изменений в Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" и отдельные законодательные акты Российской Федерации).

Анализ введения он-лайн цензуры по всему миру показывает, что детская порнография и наркотики, которые можно найти в сети Интернет, — являются лучшими аргументами для манипулирования сознанием граждан, для внедрения механизмов фильтрации в глобальной сети, так как, очевидно, большинство граждан согласятся с тем, что такая информация вредна, а потому не должна существовать. Однако, детская порнография и другая негативная информация, которая в результате применения механизмов фильтрации, на самом деле, никуда не исчезает, становится отличным поводом для многих политических деятелей, чтобы оправдать введение внесудебных механизмов цензурирования Интернета.

Такие основания становятся объяснением вмешательства государства в Интернет, что приводит к неминуемому расширению существующего законодательства и принятию специальных законодательных актов, регулирующих общественные отношения и при-

ватность в сети.

Впервые о борьбе с педофилией в Интернете заговорила Еврокомиссар Сесилия Мальмстром в своей главной речи на конференции 6 мая 2010г. Буквально через пару лет на трибуне Государственной думы Российской Федерации депутат Елена Мизулина повторяет все слово в слово, и в отличие от Европейской комиссии, в очень ускоренном темпе законопроект становится законом, обязательным всеми гражданами и организациями к исполнению.

Так, 28 июня 2012г. депутатами Государственной думы большинством голосов был принят Федеральный закон №139-ФЗ, который сразу же назвали в Рунете «законом о черных списках». Это стало началом российской практики по внесудебному закрытию доступа к сайтам на уровне Интернет провайдеров.

Российская ассоциация электронных коммуникаций (РАЭК), представляющая самых влиятельных представителей IT бизнеса в Рунете, выступила с резкой критикой закона. К протесту присоединились и многие Интернет-гиганты. Ряд крупных ресурсов ушли в блэкаут за день до итогового голосования по законопроекту и участвовали в самой крупномасштабной Интернет забастовке в истории страны.

Однако, несмотря на резкую критику, как со стороны бизнеса, так и со стороны общества, закон, вводящий внесудебную блокировку ресурсов через реестр запрещенных сайтов, был принят и вступил в силу с 01 ноября 2012г. Закон впервые определил:

- основания для блокировки сайтов - это педофилия, наркотики и суициды;
- порядок взаимоотношений между пользователями, провайдерами и государственными органами;
- уполномоченные органы, на которых возлагались полномочия по принятию решений о блокировке контента. За наркотики отвечает Федеральная служба Российской Федерации (ФСКН); за суициды – Роспотребнадзор; за педофилию – Роскомнадзор.

С первых же дней работы закона 139-ФЗ, практика правоприменения наглядно показала, что все опасения интернет-отрасли и общества сбываются. Интернет-ресурсы стали заносится в Реестр по самым нелепым основаниям. Например, одно из крупнейших вики-сообществ Луркоморье обвинили в пропаганде наркомании, а энциклопедия Абсурдопедия была обвинена в пропаганде суицида. В другом случае, ФСКН нашел на форуме онлайн-игры EVE-online термин "наркотик" (используемый в игре как жаргонизм) и запретил сайт и т.д. В первые же недели работы Реестра под блокировку попадали сайты Google и YouTube. Вскоре в Сети появились и первые выгрузки информации из Реестра.

01 ноября 2012г., в день вступления в силу №139-ФЗ, силами гражданских активистов Пиратской партии России был сформирован и запущен специальный проект — РосКомСвобода, целью которого являлось наблюдение за правоприменением и публикация материалов о заблокированных сайтах по новому законодательству.

17 декабря этого же года РосКомСвобода опубликовала первый результат мониторинга правоприменения принятого закона. Так, согласно проведенной аналитике, более 2000 сайтов или 96% находящихся в реестре ресурсов, стали подвергаться незаконной блокировке. Зачастую, только из за того, что находились в силу архитектуры Интернета, на тех же IP адресах, что и сайты с сомнительным содержанием.

Но самыми серьезными и позднее подтвердившимися опасениями всех экспертов Интернет отрасли было то, что введенный механизм для фильтрации информации в сети Интернет, рано или поздно, будет использован для политической и копирайт цензуре.

Кроме новых ограничений для российских пользователей, закон привел еще и к нарушениям прав пользователей из других стран, национальное законодательство которых не содержит правовых оснований для Интернет-цензуры. В декабре 2012г. поступило первое сообщение, что российские магистральные операторы осуществляют блокировку интернет-трафика для пользователей

Армении по закону 139-ФЗ.

В январе появилась и первая реакция вице-президента общественной организации “Интернет сообщество Армении” Григория Сагияна о недопустимости блокировки интернет-сайтов по законам России вне её пределов. Все чаще становились известны случаи, когда пользователям таких стран, как Армения, Азербайджан, Молдавия, Узбекистан, Казахстан и др. магистральные провайдеры, такие как "Билайн" и "Ростелеком" ограничивали доступ к ресурсам.

22 марта Госдума расширила перечень категорий информации, которые могут быть заблокированы, обозначив это п. "г" в Реестре: "о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия)".

№187-ФЗ. Антипиратская цензура

25 января 2013г. на сайте Минкультуры был опубликован законопроект "О внесении изменений в отдельные законодательные акты Российской Федерации в целях прекращения нарушений интеллектуальных прав в информационно-телекоммуникационных сетях, в том числе в сети "Интернет", после чего стало очевидно, что механизм блокировки сайтов будет также использован лоббистами от медиа-индустрии для закрытия множества сайтов, которые могут быть использованы для неавторизованного копирования материалов, защищенных авторским правом.

С развитием высокоскоростного Интернета и удобных он-лайн сервисов у пользователей появилась возможность меняться любым информационно-развлекательным контентом и программным обеспечением без какого-либо участия посредников. Таким образом, многие бизнес-схемы, используемые ранее издателями и распространителями для длительного извлечения прибыли из авторского контента, перестали работать в цифровом мире. Такое положение дел, несомненно, вызывало обеспокоенность у издательско-дистрибьютерской индустрии, которая стала существенно отставать от технологического прогресса, однако имела острое желание вмешиваться в регулирование процесса обмена информацией в

Интернете.

Даже если цели политических лидеров и правоохранителей разнятся с целями индустрии копирайта, тем не менее все заинтересованные группы продвигают одни и те же новые инструменты в общество, которые, по их словам, могут облегчить взаимоотношения между участниками в сети, а на самом деле, направлены на то чтобы получить контроль над коммуникациями.

6 июня 2013г., ровно год спустя после внесения в Госдуму законопроекта о "чёрных списках сайтов", был внесен очередной проект законодательного акта, который в последствии будет назван "антипиратский" или "закон против интернета".

Законопроект предусматривал блокировку сайта в качестве обеспечительных мер по иску о нарушении исключительных авторских прав на фильмы, в т.ч. телефильмы, кинофильмы. Кроме того, такие меры предлагалось применять и в случае нахождения на сайте ссылки или информации, при помощи которой можно получить доступ к нелицензионному произведению, защищенному авторским правом.

IT отрасль и Яндекс снова публично раскритиковали закон, пояснив, что закон технически не реализуем и потенциально вреден. 4 июля Пиратская партия России, Ассоциация пользователей Интернета и РосКомСвобода совместно подготовили и запустили общественную петицию об отмене "закона против интернета" 187-ФЗ. За месяц данная общественная инициатива с беспрецедентной скоростью собрала на страничке Российская общественная инициатива (РОИ) 100 тысяч подписей верифицированных граждан. Против "антипиратского" закона и в поддержку петиции об отмене 187-ФЗ прошли митинги и другие оффлайн-акции в ряде городов России: Москве, Санкт-Петербурге, Казани, Калининграде, Томске, Бийске, Хабаровске, Ханты-Мансийске, Иваново, Новосибирске, Пензе, Кемерово.

Однако, также как это случилось с №139-ФЗ, мнение общественности и профессиональных игроков IT рынка услышано не было, закон был достаточно быстро принят обеими палатами и под-

писан президентом, а с 01 августа 2013 он уже вступил в силу. В этот же день состоялась Всероссийская интернет-забастовка, в которой приняли участие тысячи интернет-ресурсов самой разной тематике и посещаемости, а петиция об отмене №187-ФЗ была просмотрена более 1 млн раз.

Уровень свободы Интернета в России

В соответствие с докладом Freedom House «О свободе сети» на 2013г. Интернет в России стал менее свободным. Уровень свободы Интернета в России в 2013 году эксперты Freedom House оценили в 54 балла против 52 баллов в 2012 году. В целом в рейтинге свободы Интернета Россия опустилась по сравнению с показателем 2013 года на 10 пунктов, заняв 41-е место из 100.

Довольно очевидно, что причиной снижения рейтинга свободы Интернета за два года и опускание России на один уровень с Венесуэлой и Зимбабве произошло из-за принятия законов о блокировке сайтов №139-ФЗ и №187-ФЗ, закона, возвращающего клевету в Уголовный кодекс, ужесточения госрегулирования в Рунете, давления на онлайн-активистов и наращивания списка экстремистских материалов, запрещенных к распространению.

Согласно докладу в период с января 2012 года по февраль 2013 года количество сайтов, которые российские власти по требованию региональных прокуратур заблокировали как экстремистские, возросло на 60 процентов. Кроме того, значительно увеличилось количество уголовных дел в отношении интернет-активистов – с 38 в 2011 году до 103 в 2013 году.

В ноябре 2013 г., спустя год после вступления в силу первого закона, РосКомСвобода опубликовала доклад о правоприменении первого закона «о черных списках сайтов». В соответствии с докладом, за год существования реестра в него было внесено 741 IP-адресов и 1392 интернет-ресурсов. Для достижения этой цели всего было подвергнуто неправомерной блокировке 83215 добропорядочных интернет-сайтов. Сайты блокировались лишь по причине того, что они находились на тех же сетевых адресах, что и тот или иной

запрещенный контент. Таким образом, 98% от общего кол-ва блокируемых ресурсов составляли сайты, не содержащие какой-либо незаконный контент.

№398-ФЗ. Возвращение политической цензуры.

В конце 2013г. произошло то, что многие правозащитники и эксперты в области IT, предсказывали. 8 декабря 2013г. депутат Луговой внес в Госдуму законопроект, расширяющий основания для блокировки сайтов в сети Интернет. Законопроект предусматривал возможность моментального ограничения доступа к интернет-ресурсам по политическим причинам. Так, на Роскомнадзор по требованию Генерального прокурора либо его заместителей, возлагались обязательства вносить идентификаторы сайтов, распространяющих «информацию, содержащую призывы к массовым беспорядкам, осуществлению экстремистской деятельности, разжиганию межнациональной и (или) межконфессиональной розни, участию в террористической деятельности, участию в публичных массовых мероприятиях, проводимых с нарушением установленного порядка» в специальный реестр. А всем российским Интернет провайдерам доступа подлежало осуществлять блокировку внесенных в специальный реестр сайтов всеми доступными способами. При этом, в отличие от №139-ФЗ и №187-ФЗ, законопроект не предусматривал даже предварительное предупреждение хостинг-провайдера или владельца сайта напрямую для добровольного своевременного удаления материалов, признанных уполномоченными органами незаконными.

РАЭК и общественность вновь выступили с резкой критикой закона, но уже по привычному сценарию, минуя какие-либо общественные и экспертные обсуждения, закон в рекордно короткие сроки, 28 декабря 2013г., принимается большинством голосов депутатов Государственной думы и уже с 01 февраля 2014г. вступает в законную силу.

13 марта 2014 года состоялось первое и наиболее одиозное решение по блокировке трех крупных сетевых новостных ресурсов

и блога известного оппозиционного политика Алексея Навального. Роскомнадзор по требованию Генеральной прокуратуры РФ внес в единый реестр запрещенной информации следующие интернет-ресурсы: kasarov.ru, grani.ru, ej.ru и navalny.livejournal.com.

В день принятия решения о прекращении доступа граждан к указанным сайтам в реестр были внесены доменные имена и IP-адреса самих Интернет-изданий, а также самых больших по численности блог-платформ «Эха Москвы» и «Живого Журнала». Для того, чтобы сохранить доступ граждан к другим блогам, администрацией «Эхо Москвы» было принято решение полностью удалить блог Навального с сайта, а ЖЖ ограничило доступ к блогу с территории Российской Федерации.

Все ресурсы, подвергшиеся внесудебной блокировке, обжаловали решение Генеральной прокуратуры и действия Роскомнадзора в различных судах общей юрисдикции, однако все прошедшие суды постановили, что блокировка сайтов была правомерной, и не нарушает права и интересы третьих лиц. Несмотря на отсутствие какой-либо независимой судебной позиции по указанным делам, в результате судебных разбирательств было выяснено, что, во-первых, при принятии решения о блокировке, прокуратура не имела каких-либо конкретных претензий к определенным материалам, однако имела претензии к общему характеру публикуемых новостей, а, во-вторых, стало понятно, что блокировка сайтов носит постоянный характер, т. к. законом не предусмотрен алгоритм исключения сайта из реестра.

Таким образом, указанные сайты до сих пор находятся в реестре запрещенных сайтов и подвергаются блокировке со стороны всех операторов связи по указанию Роскомнадзора.

Вместе с тем, в 2013 году было трудно остановить порыв всех желающих дополнить список оснований новыми запретами. В течение года был внесен ряд законопроектов, направленных на расширение оснований для блокировки сайтов. Среди них были такие предложения как ограничение доступа к сайтам в связи с публикацией тел погибших, распространением материалов о жестоком обращении с животными, недостоверной информации о банках и

публичных организаций, информации и объявлений о деятельности мистиков (в т.ч. гадалок, астрологов, магов, экстрасенсов) и многое другое.

№97-ФЗ. Круглосуточная поголовная слежка за пользователми.

По сравнению с 2013 год, который ознаменовался принятием целой плеяды законов, вводящих цензуру, и так или иначе регулирующих общественные отношения граждан в сети, 2014 год начался с еще более агрессивного законодательства.

28 февраля 2014г. в рамках так называемого антитеррористического пакета законопроектов, предложенного к принятию депутатом Яровой, были приняты следующие варварские законы: о расширении полномочий ФСБ по обыску граждан и их автомобилей при наличии достаточных оснований подозревать их в совершении преступления, о контроле над сетевыми коммуникациями граждан и о об ограничении анонимных электронных платеже.

После разоблачений Сноудена о тотальной слежке американских спецслужб за информационными коммуникациями между гражданами многих государств по всему миру при помощи существующих информационных сетей и сетей связи, законодатели в России пошли еще дальше. Отличительной чертой новой российской инфополитики стало то, что отличие от США, в которых после событий 11.09 был принят Патриотический акт, давший правительству и полиции широкие полномочия по надзору за гражданами и начало государственной программе слежки за гражданами PRISM, российские группы, заинтересованные в принятии «антитеррористического пакета законопроектов», не скрывали свое желание контролировать коммуникации граждан и предлагали делать это не скрытно, как в США, а открыто с помощью возложения новых обязательств на «информационных посредников» по собиранию информации о деятельности пользователей ресурсов (логов).

Указанным законом «организаторов распространения информации» (владельцев сайтов и различных десктопных/мобильных приложений, в т.ч. иностранных), перечень которых подлежал опре-

делению Роскомнадзором, обязали за свой счет на собственном оборудовании хранить данные о приеме, передаче, доставке, обработке различной электронной информации о пользователях в течение 6 месяцев, а также предоставлять эту информацию правоохранительным органам по первому требованию.

Закон установил новые обязательства для посредников по сбору следующих данных о пользователях: контактов адресной книги и электронной почты, количество и объем сообщений, все авторизации через сторонние сервисы, информации о том, как ведет личную переписку внутри интернет-ресурса, точное время посещений, список DNS-серверов, используемых пользователем, информацию о том, как ведет переписку с провайдерами хостинга и регистраторами доменных имен, вся информация, внесенная при регистрации пользователя на интернет-ресурсе, информация об используемом пользователем оборудовании и ПО, все факты авторизации с точным временем, все факты изменения пользователем своих данных, факты прекращения пользователем использования интернет-ресурса, факты о произведенных денежных операциях пользователем с указанием информации о корреспонденте — идентификаторе платежной системы, валюты и суммы, осуществленных транзакциях (с указанием идентификатора платежной системы («электронного кошелька»), сумм прихода либо расхода и ряд других не менее казалось бы конфиденциальных данных, о которых должен знать только инициатор и получатель.

Вместе с тем, закон предусматривал, что в случае если организатор распространения информации не может осуществлять возложенные на него законом обязанности, то по договоренности с уполномоченными госорганами, он может обеспечить доступ к такой информации о пользователях в полном объеме на постоянной основе и без каких-либо запросов. Тогда он освобождается от обязанности хранить такую информацию.

Закон также возложил новые обязанности и на блогеров, фактически приравняв их к СМИ и ограничив возможность анонимного использования блог-платформ. Отныне все блогеры, которые

имеют 3000 уникальных посещений в сутки, с 01 августа 2014г. обязаны регистрироваться в специальном реестре Роскомнадзора, указывать на сайте свое настоящее имя и координаты для связи, а также выполнять ряд обязанностей, свойственные профессиональным журналистам - например, проверять публикуемую информацию.

За несоблюдение новых требований российского законодательства, новые субъекты правового регулирования - организаторы распространения информации и блогеры, могут быть привлечены к административному наказанию, предусматривающему крупные административные штрафы (до 500 000 рублей).

Кроме того, в ФЗ «Об информации» было добавлено еще одно основание для блокировки сайтов в сети Интернет - неисполнения организатором распространения информации в сети «Интернет» обязанностей, предусмотренных №97-ФЗ.

И еще одним новшеством «антитеррористического пакета законопроектов» стал запрет на неперсонифицированные электронные платежи. Общая сумма перевода не может превышать 1000 рублей в день и 15000 рублей в течение месяца, а анонимные переводы любых денежных знаков из-за границы полностью запрещаются.

№433-ФЗ и №274-ФЗ. Запрет обсуждения сепаратизма.

2013 год был особо богат различного рода запретами тех или иных действий в глобальном Интернет-пространстве, а военные действия на Украине и фактическое отсоединение Крымской Республики с последующим присоединением ее к России, побудили российскую власть принять ряд законов, ужесточающих высказывания в сети. 20 декабря 2013г. был принят закон о добавлении в Уголовный кодекс России специального состава преступления за «публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации». Те же деяния осуществляемые с помощью СМИ или Интернета образуют квалифицирующий состав преступления.

До принятия указанного закона использование для пропаганды

или оправдания сепаратизма собственного блога отягчающим обстоятельством вообще не считалось.

Таким образом если призывы вернуть Крым Украине, будут озвучены с экрана телевизора, через газету или в Интернете, лицо может быть привлечено к уголовной ответственности в соответствии со ст. 280.1 УК РФ с назначением наказания в виде обязательных работ до 480 часов либо лишение свободы на срок до 5 лет.

Летом 2014 года, авторы закона посчитали, что новая уголовная ответственность за призывы к сепаратизму слишком мягкая. Таким образом №274-ФЗ, вступившим в силу с 02 августа 2014г., было установлено более строгое наказание - за обычные призывы до 4 лет лишения свободы, и в СМИ/Интернете — дополнительное наказание в виде лишения права занимать определенную должность либо заниматься определенной деятельностью на срок до 3 лет.

№101-ФЗ. Запрет мата.

Указанный закон явился следствием борьбы за нравственность в обществе и духовные скрепы россиян. Впервые введен законодательный запрет на использование матерных слов и их производных на уровне ФЗ «О государственном языке». Закон вводит ответственность в виде штрафов (ст.6.27 КоАП РФ) за распространение аудио и видео продукции на любых видах носителей, экземпляров печатной продукции (за исключением продукции средств массовой информации), содержащих нецензурную брань, без специальной упаковки и текстового предупреждения в виде словосочетания «содержит нецензурную брань»: для физ. лиц – от 2000 до 2500 р., для юр лиц – от 40000 до 50000 р.; повторное нарушение для физ. лиц – от 2500 до 5000 р., юр.лиц - от 50000 до 100000 р.

Кроме того, законом предусматривалась возможность административного приостановления деятельности юридического лица сроком до 90 суток.

№242-ФЗ. Запрет на хранение персональных данных россиян.

Принимая этот закон, депутаты, естественно, мотивировали его

принятие необходимостью защитить персональные данные россиян от компаний, которые согласно разоблачением Сноудена, тайно следят за российскими пользователями соц.сетей и различных Интернет-сервисов.

Однако, экспертам IT отрасли и правозащитникам было довольно очевидно с самого начала, что указанный крайне непродуманный закон принимается, прежде всего, для точечного применения против крупнейших американских компаний, таких как Google, Facebook, Twitter в свете обострившихся внешнеполитических отношений двух государств.

Так, Федеральным законом от 21 июля 2014г., который должен предположительно вступить в силу с 01 сентября 2016г. (предлагалось также вступление в силу закона с 01 января 2015г.), предусматривается, что «при сборе персональных данных, в том числе посредством сети Интернет, оператор обязан обеспечить запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации с использованием баз данных, находящихся на территории Российской Федерации». В противном случае, сайт, уличенный в сборе и хранении персональных данных российских граждан не на серверных мощностях, находящихся в пределах юрисдикции РФ, может быть заблокирован. Согласно новому основанию к ФЗ «Об информации» все уникальные идентификаторы такого сайта должны быть внесены Роскомнадзором в специальный реестр нарушителей персональных данных и далее блокироваться всеми Интернет провайдерами.

Принятие законопроекта угрожает закрытием для России почти всего мирового Интернета, от социальных сетей, таких, как Facebook, и до электронной почты, а также несет существенные риски для отечественного IT-бизнеса. Речь идет обо всех сервисах, которые требуют аутентификации пользователя (к примеру, ввода для регистрации имени и фамилии).

Резонансный закон вызвал резкую критику всего бизнес сообщества, так или иначе задействованного в коммуникациях с

конечными пользователями по средствам сети Интернет, а также самих пользователей. Введение императивных норм в законодательство означало фактическое лишение человека права самостоятельно распоряжаться своими персональными данными, особенно в силу устаревшей и расплывчатой формулировки «персональных данных», которая может включать в себя самый большой объем информации, «прямо или косвенно идентифицирующих человека». Кроме того, закон накладывал значительные финансовые обременения на бизнес, который в силу закона вынужден теперь вкладывать денежные средства в создание новых data-центров в России, т. к. технологические мощности существующих data-центров не позволят справиться со всем тем массивом информации, который отныне может храниться только на российских серверах.

Закон противоречит Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных». Принятие указанного закона еще более отдалило Россию от прогрессивного европейского законодательства в указанной сфере. И это несмотря на то, что еще до принятия закона, РФ не признавалась Европейским сообществом страной, обеспечивающей адекватную защиту прав субъектов персональных данных.

Постановление Правительства №758. WiFi по паспорту.

Во исполнение антитеррористического блока законопроектов №97-ФЗ, Правительством РФ был принят еще один резонансный документ - Постановление Правитльства №758 от 31 июля 2014г.

Подзаконным актом установлено, что до оказания услуг связи по передаче данных и предоставлению доступа к сети Интернет с использованием пунктов коллективного доступа оператор проводит идентификацию пользователей.

Сведения о пользователях (ФИО, реквизиты основного документа, удостоверяющего личность), а также об объеме и времени оказания им услуг связи должны храниться оператором универсального обслуживания не менее 6 месяцев. При этом, оператор связи должен также идентифицировать пользователей и используемое

ими оконечное оборудование.

Вместе с тем, на юридических лиц и индивидуальных предпринимателей (ИП) была возложена новая обязанность - представлять оператору связи список лиц, использующих его пользовательское (оконечное) оборудование для выхода в Интернет. Этот список должен быть заверен уполномоченным представителем и обновляться не реже 1 раза в квартал.

Итоги

Как видно, за последние несколько лет в России было принято большое количество специальных нормативно-правовых актов, вводящих цензуру контента, в связи с чем статья 15 Федерального закона «Об информации» была расширена до пяти различных оснований, по которым фактически любой Интернет-сайт может быть заблокирован (преимущественно, во внесудебном порядке).

За два года правоприменения более 174 582 ресурсов было подвергнуто блокировке. Доступ к 74 475 ресурсам, что составляет 92,8% блокируемых сайтов, ограничивается в настоящее время лишь только за то, что находятся на тех же IP адресах, что и страницы с противоправным контентом.

Однако, даже несмотря на то, что в результате всех наспех принятых законодательных актов, специальным законом №149-ФЗ «Об информации, информационных технологиях и о защите информации» за два года было введено 5 новых статей, предусматривающих порядок ограничения доступа к информационным ресурсам, органы прокуратуры демонстрируют, что не очень то сильно нуждаются в специальном законодательстве, блокируя через суд все то, что представляется им незаконным. Закрепление в законе закрытого списка оснований для ограничения доступа к Интернет ресурсам, к сожалению, оказалось не способно установить единые, понятные и прозрачные для всех новые правила игры в РУнете.

Так, за последний год участились случаи блокировки региональными судами по требованию районных прокуратур различных сайтов игровой тематики, сайтов с предложениями интим услуг, сай-

тов на которых была обнаружена информация о том, как давать взятки, сайтов с иконой «Pussy Riot» а также иных сайтов, не поименованных в законе. Кроме того, были зафиксированы случаи, когда выработанные правовые механизмы для блокировки сайтов в сети, использовались недобросовестными участниками предпринимательской деятельности в своих личных бизнес интересах.

На этом фоне с каждым годом растет количество уголовных и административных дел, возбужденных против обычных пользователей Интернета. Привлекая пользователей к административной и уголовной ответственности, правоохранительные органы демонстрируют активную борьбу с противоправным поведением в цифровом пространстве, о чем регулярно отчитываются в СМИ. Однако, все чаще эта деятельность больше напоминает охоту за виртуальными ведьмами, результатом которой является публикация статистики о выявленных правонарушениях и раскрытых преступлениях, чем реальную борьбу с киберпреступниками, которые остается вне досягаемости сотрудников правоохранительного блока.

Вводя все новые ограничения для гражданско-правового оборота информации в сети, депутаты и чиновники каждый раз прикрываются самыми гуманными основаниями — защита детей, охрана прав авторов, забота об общественных интересах. Но к сожалению, ни один из принятых за последнее время законов, регулирующих Интернет в России, не смог справиться с провозглашенными задачами, ради которых все и затевалось. Результатом таких непродуманных действий в сфере законотворчества становится уход успешных стартапов в иностранные юрисдикции с размещением выделенных серверов за пределами РФ, создание многочисленных зеркал в darknet (TOR, i2p), а также падение российского рынка IT и зависимой инфраструктуры.

По количеству пользователей интернета Россия ещё в 2012 году вышла на первое место в Европе. По опросу Всероссийского центра изучения общественного мнения (ВЦИОМ) более 66% россиян, что составляет около 76,3 млн. человек, являются пользователями Интернета.

Очевидно, что цензура и слежка всегда идут рука об руку. Принятие новых законов, ограничивающих права миллионов граждан, и одновременно расширяющих возможности чиновников и полицейских, непременно ведут к злоупотреблениям со стороны сотрудников государственного аппарата и нарушению фундаментальных прав человека, а именно права на свободу выражения мнения, права на свободу слова, получение/распространения информации, права на тайну частной жизни и тайну переписки. Именно по этой причине сегодня назрела необходимость регламентации новых цифровых прав граждан, в т. ч. права на шифрование и права на анонимность, без которых реализация и защита базовых прав, гарантированных Всеобщей декларацией прав человека, в эпоху развития информационного общества становится невозможной.

Կազմող եւ խմբագիր՝ Սուրեն Դեհերյան
«Լրագրողներ հանուն ապագայի» ՀԿ
Հեռ.՝ (+37410) 20-45-67
Բջջ.՝ (+37493) 53-93-34
էլ.փոստ՝ info@jnews.am
Կայք՝ JNews.am