ԿԻԲԵՌՀԱՆՑԱՎՈՐՈՒԹՅԱՆ ՎԻԿՏԻՄՈԼՈԳԻԱԿԱՆ ԿԱՆԽՄԱՆ ՄԻՋՈՑՆԵՐԸ

Մնացականյան Արտակ

ՀՀ ՆԳՆ կրթահամալիրի

ուսումնամեթոդական և զարգացման վարչության պետ,

ոստիկանության փոխգնդապետ, ի. գ. թ., դոցենտ

Համառոտագիր: Կիբեռհանցավորության հակազդման խնդիրը անկյունաքարային է դարձել բոլոր երկրների համար, և այս մասշտաբային պայքարը հաջողելու համար անհրաժեշտ է ներդնել կիբեռհանցավորության կանխարգելման ամբողջ գործիքակազմը: Ավանդական մի շարք հանցագործություններ կատարվում են տեղեկատվական տեխնոլոգիաների և համացանցի միջոցով և այս ժամանակահատվածում պայքարել կիբեռհանցավորության դեմ ավանդական կանխարգելման միջոցներով այլևս նպատակահարմար և արդյունավետ չեն: Ներկայումս հետզհետև ավելի է արդիական դառնում կիբեռհանցավորության դեմ պայքարի վիկտիմոլոգիական գործիքակազմը, այս առումով այլևս նորություն չէ կիբեռվիկտիմոլոգիան:

Հոդվածում քննարկվում են կիբեռհանցավորության ընդհանուր վիկտիմոլոգիական կականխարգելման իրավական, ակադեմիական, կազմակերպակառավարչական և գաղափարախոսական միջոցները:

Բանալի բառեր. համացանց, կիբեռզոհ, տեղեկատվական տեխնոլոգիաներ, կանխարգելում, համակարգիչ, սպառնալիք:

Նախաբան

Կիբեռհանցավորության դեմ պայքարի արդիականությունը կասկած չի հարուցում՝ հաշվի առնելով վիրտուալ իրականության և կիբեռտարածության օր օրի ընդլանումը: Այս մասին են վկայում նաև կիբեռհանցավորության ծավալի և աճի վերաբերյալ առկա վիճակագրական տվյալները[1]: Կիբեռհանցավորության հակազդման խնդիրն

[1] Կիբեռհանցավորության վիճակագրական տվյալների մասին առավել մանրամասն տե՛ս **Ա. Մնացականյան**, «Կիբեռհանցավորության վիկտիմոլոգիական կանխարգելման առանձնահատկությունները», Օրենքի պատվար ամսագիր 17-րդ համար, Երևան, 2024թ. մարտ, էջեր՝ 171-181:

անկյունաքարային է դարձել բոլոր երկրների համար, և այս մասշտաբային պայքարը հաջողելու համար անհրաժեշտ է ներդնել կիբեռհանցավորության կանխարգելման ամբողջ գործիքակազմը: Հաշվի առնելով կիբեռհանցավորության բազմակողմանիությունը՝ վերջինիս դեմ պայքարում անհրաժեշտ է ներգրավել պետական գործունեության բոլոր հնարավորությունները, այդ թվում՝ իրավական, տեխնիկական, հոգեբանական, սոցիալական և այլն: Հասարակությունը թևակոխել է մի ժամանակահատված, որտեղ հնարավորինս ընդլայնվել են տեղեկատվական տեխնոլոգիաները, վիրտուալ իրականությունը, և դրանք ներթափանցել են կյանքի գրեթե բոլոր բնագավառներ: Ավանդական մի շարք հանցագործություններ կատարվում են տեղեկատվական տեխնոլոգիաների և համացանցի միջոցով, և այս ժամանակահատվածում կիբեռհանցավորության դեմ ավանդական կանխարգելման միջոցներով պայքարելն այլևս նպատակահարմար և արդյունավետ չէ: Այս իրականության մեջ անհրաժեշտ է վերանայել կիբեռհանցավորության դեմ պայքարի մեթոդաբանությունը, կանխարգելման միջոցները, դրանք առավելագույնս համապատասխանեցնել ժամանակակից տեղեկատվական հասարակության առանձնահատկություններին, մշակել համապատասխան միջոցներ և գործիքակազմ՝ կանխարգելման միջոցառումների արդյունավետությունը բարձրացնելու նպատակով:

Ընդհանուր վիկտիմոլոգիական կականխարգելումը բխում է սոցիալական նորմերից և պետական իշխանության գործադիր, տարածքային կառավարման և տեղական ինքնակառավարման մարմինների՝ օրենքով սահմանված համապատասխան գործունեությունից, որի բովանդակությունն է կազմում կանխարգելիչ միջոցառումների իրականացումը՝ նպատակ հետապնդելով հակազդել քրեածին գործընթացներին, հասարակության մեջ ամրապնդել ապահովության և կայունության մթնոլորտ, վերացնել անձի իրավունքների, ազատությունների և օրինական շահերի խախտման սպառնալիքները, որոնք ծագում են նրա նկատմամբ հանցագործության կատարման հնարավորությունից, հնարավոր վիկտիմիզացումից: Վիկտիմոլոգիական կանխարգելման ընդհանուր մակարդակում նշված նպատակների իրագործումը պահանջում է.

- բացահայտել, վերլուծել և ընդհանրացնել վիկտիմայնության պատճառները և պայմանները,

- մշակել և իրականացնել վիկտիմածին գործոնների և իրավիճակների վերացմանը կամ չեզոքացմանն ուղղված միջոցներ,

- փոփոխել օրենսդրական դրույթներն այն ակնկալիքով, որ ապահովվի հանցագործություններից տուժողներին անհրաժեշտ աջակցություն, ստեղծվեն նոր

պետական և ոչ պետական կառույցներ, որոնց աշխատանքը կուղղվի նրանց պաշտպանությանը,

- ներգործել բնակչության առանձին շերտերի վրա՝ նպատակ ունենալով նվազեցնել կամ թույլ չտալ նրանց վիկտիմիզացումը,

- դաստիարակել քաղաքացիներին և բարձրացնել նրանց իրավագիտակցությունը,

- ուսուցանել համապատասխան կադրերին՝ տուժողների հետ աշխատելու համար:[2]

Ներկայումս հետզհետև ավելի է արդիական դառնում կիբեռհանցավորության դեմ պայքարի վիկտիմոլոգիական գործիքակազմը: Այս առումով այլևս նորություն չէ կիբեռվիկտիմոլոգիան: Կիբեռհանցավորության դեմ պայքարում ընդհանուր վիկտիմոլոգիական կանխարգելման միջոցներից սույն հոդվածում կքննարկվեն հետևյալները.

- **Իրավական,**

- Ակադեմիական,

- Կազմակերպակառավարչական,

-Գաղափարախոսական:

<u>Ընդհանուր վիկտիմոլոգիական կանխարգելման իրավական միջոցներ:</u>

Իրավական միջոցները մասնագիտական գրականության մեջ բնութագրվում են տարբեր ձևերով, սակայն կարելի է ընդհանրացնել. այս միջոցները ենթադրում են ոլորտը կարգավորող օրենսդրության կատարելագործում, մեկ միասնական իրավական ակտի մշակում և ընդունում (դա կլինի, օրինակ, կիբեռհանցավորության կանխարգելման մասին օրենք, հանցագործությունների կանխարգելման մասին, կրիմինոլոգիական կանխման մասին և այլն), որի շրջանակներում կկարգավորվեն կոնկրետ կիբեռհանցավորության դեմ պայքարի մեթոդաբանությունը, գործիքակազմը, կանխման միջոցները, սուբյեկտները, միջոցառումները և այլն:

Համացանցի ներդրման և տեղեկատվական տեխնոլոգիաների զարգացմանը զուգընթաց ամբողջ աշխարհում անհրաժեշտություն առաջացավ իրավական կարգավորում տալ վիրտուալ իրականություն «տեղափոխված» արժեքների պաշտպանությանը:

Տեղեկատվական տեխնոլոգիաների իրավական կարգավորման գործընթացը կապված էր համակարգիչների և համացանցի ստեղծման, զարգացման հետ: Համացանցի հայտնաբերման վերաբերյալ կան տարբեր կարծիքներ. մասնավորապես՝ նշվում են 1958,

---

[2] Տե՛ս «Դասախոսություններ վիկտիմոլոգիական դասընթացի», ՀՀ ոստիկանության ակադեմիա, Երևան, 2015թ., էջ-42:

1962, 1969 թվականները, իսկ ոհմանք կարծում են, որ համացանցն ի հայտ է եկել 1983 թվականին[3]: Դեռևս 1958 թվականին ԱՄՆ նախագահ Էյզենհաուերի հանձնարարությամբ պաշտպանության նախարարության կազմում ստեղծվում է առաջադեմ հետազոտությունների կազմակերպությունը:

Առաջին համակարգչային հանցագործությունը, ըստ հրապարակումների, կատարվել է 1969 թվականին ԱՄՆ-ում՝ ոմն Ալֆոնսե Կոնֆեսսորեի կողմից: Վերջինս անօրինական ճանապարհով ներգործել էր համացանց և կատարել հափշտակություն, որի վնասը կազմել էր 620 հազար ԱՄՆ դոլար[4]:

Այս իրադարձությունը կենտրոնացրեց իրավապահ մարմինների և գիտնականների ուշադրությունը, ինչի արդյունքում սկսվեց պայքարը կիբեռհանցավորության դեմ: Սկզբնական փուլում իրավապահ մարմինները կիբեռհանցավորության դեմ պայքարում օգտագործում էին ավանդական հանցագործությունների իրավական կարգավորումները, սակայն համացանցի զարգացման հետ զուգընթաց պարզ դարձավ, որ ոչ բոլոր հանցագործությունների դեպքում կարելի է առաջնորդվել ավանդական նորմատիվ կարգավորումներով, քանի որ փոխվում էին հանցագործությունների ձևաչափը, կատարման միջոցները, առարկան, գործիքակազմը և այլն:

1973 թվականին Շվեդիան պատասխանատվություն սահմանեց համակարգչային հանցագործությունների համար՝ դրանով իսկ դառնալով կիբեռհանցավորության դեմ պայքարն օրենքով ամրագրած առաջին պետությունը: Սակայն այս ոլորտում առավել մեծ հաջողություններ գրանցվեցին ԱՄՆ-ում՝ 1979 թվականին Դալլասում ամերիկյան փաստաբանների ասոցիացիայի համաժողովում սահմանվեցին համակարգչային հանցագործությունների տեսակները և ընդգրկվեցին ԱՄՆ-ի քրեական օրենսգրքում, իսկ արդեն 1986 թվականին ընդունվեց «Համակարգիչների օգտագործմամբ խարդախությունների և չարաշահումների վերաբերյալ» օրենքը:

Մեծ Բրիտանիայում նմանատիպ առաջին օրենքն ընդունվեց 1991 թվականին՝ «Համակարգչային տեխնոլոգիաների ոչ իրավաչափ օգտագործումը»:

80-ական թվականներին շատ երկրներ եկան այն եզրահանգման, որ համակարգչային տեղեկատվության պաշտպանությունն ազգային քրեաիրավական կարգավորմամբ բավարար չէ, և այս խնդրով պետք է զբաղվել անդրազգային մասշտաբով: 1985-1989

---

[3] Տե՛ս **Ястребов Д.А.**, Институт уголовной ответственности в сфере компьютерной информации (опыт международно-правового сравнительного анализа) // Государство и право, 2005. №1, էջ 53-63:

[4] Տե՛ս **Медведев С.С.**, Мошенничество в сфере высоких технологий: дис. …канд. юрид. Наук, Краснодар, 2008. էջ 31:

թվականներին այս խնդրով սկսեց զբաղվել եվրոխորհրդի կազմում գործող համակարգչային հանցագործությունների փորձագետների կոմիտեն: 1989-2004 թվականների ընթացքում Եվրոպայի խորհրդի կողմից ընդունվել են մի շարք իրավական ակտեր, իսկ 2004 թվականի հուլիսի 1-ին ուժի մեջ մտավ «Կիբեռհանցագործությունների մասին» կոնվենցիան[5], որը Հայաստանի Հանրապետությունում ուժի մեջ է մտել 2007 թվականի փետրվարի 1-ին:

ՀՀ-ում կիբեռհանցավորության դեմ պայքարի իրավական միջոցների գործիքակազմը լիարժեք չի օգտագործվում, առանձին իրավապահ մարմինների գործունեությունը կարգավորող իրավական ակտերով ընդհանրական ձևաչափով սահմանվում է հանցագործությունների պրոֆիլակտիկա իրականացնելու պարտավորություն, սակայն սա ամենևին էլ բավարար չէ այս հանցավորության դեմ պայքարում: ՀՀ քրեական օրենսգրքի 38-րդ գլխում զետեղված է համակարգչային համակարգի և համակարգչային տվյալների անվտանգության դեմ ուղղված 7 հանցակազմ: Հաշվի առնելով կիբեռհանցավորության տեմպերի աճը՝ կառավարությունը հանդես էր եկել քրեական օրենսգրքում կիբեռհանցագործությունների ցանկ սահմանելու առաջարկությամբ[6]:

Որպեսզի ավելի պարզ լինի կիբեռհանցավորության ընդհանուր կանխարգելման իրավական միջոցների արդյունավետությունը, դիտարկենք հետևյալ օրինակը. Մինչև 2015 թվականը ՀՀ-ում մեծ պահանջարկ ունեցող համարանիշների տրամադրման ընթացակարգում սահմանվում էր, որ կորած զույգ համարանիշների փոխարեն հատկացվում են թվերի ու տառերի այլ հավաքածու պարունակող համարանիշներ[7]: Ինչպես գիտենք, մեծ պահանջարկ ունեցող համարանիշների արժեքները կարող են հասնել մինչև ութ միլիոն դրամի, իսկ որոշ դեպքերում (աճուրդի պարագայում)՝ ավելի շատ: Այս կարգավորումը բերում էր նրան, որ զույգ համարանիշների կորստյան դեպքում անձն այլևս հնարավորություն չէր

---

[5] Տե՛ս https://cyberleninka.ru/article/n/evolyutsiya-zakonodatelstva-ob-ugolovnoy-otvetstvennosti-za-sovershenie-prestupleniy-v-sfere-vysokih-tehnologiy/viewer /վերջին մուտք՝ 02.09.2024թ/

[6] Տե՛ս https://www.shantnews.am/news/view/1478754.html /վերջին մուտք՝ 03.09.2024թ/

[7] Տե՛ս «Պետական գրանցման ենթակա տրանսպորտային միջոցների տեսակների ցանկը, տրանսպորտային միջոցների պետական հաշվառման կարգը, պետական գրանցման եվ պետական հաշվառման համար պարտադիր ներկայացվող փաստաթղթերի ցանկերը, տրանսպորտային միջոցի սեփականության իրավունքի պետական գրանցման վկայականի, պետական հաշվառման ազգային ու միջազգային վկայագրերի և «ժամանակավոր ներմուծում» մաքսային ընթացակարգով Հայաստանի Հանրապետություն ներմուծված տրանսպորտային միջոցների հաշվառման վկայագրի ձևերը, «ժամանակավոր ներմուծում» մաքսային ընթացակարգով հայաստանի հանրապետություն ներմուծված տրանսպորտային միջոցների հաշվառման կարգը, հաշվառման համարանիշներին ներկայացվող պահանջները, ինչպես նաեվ տրանսպորտային միջոցների համարանիշների հաշվառման ու հատկացման կարգը սահմանելու, Հայաստանի Հանրապետության կառավարության 2006 թվականի նոյեմբերի 30-ի N 1853-ն որոշման մեջ փոփոխություններ կատարելու և Հայաստանի Հանրապետության կառավարության 2007 թվականի օգոստոսի 30-ի n 1041-ն որոշումն ուժը կորցրած ճանաչելու մասին» ՀՀ կառավարության 09.09.2010 թվականի թիվ 1251-Ն որոշման 12-րդ հավելվածի 21-րդ կետը:

ունենում վերականգնել կամ վերադարձնել իր կատարած ծախսը: Այս հանգամանքից սկսեցին օգտվել հանցագործները, ՀՀ-ում աննախադեպ տարածում ստացավ մեծ պահանջարկ ունեցող համարանիշների գողությունը: Այս հանցագործությունը պարունակում էր կիբեռհանցավորության տարրեր, քանի որ հանցագործները համարանիշների գողությունից հետո տարբեր սոցիալական կայքերով (հիմնականում՝ Telegram) կապ էին հաստատում տուժողի հետ, պահանջում էին համարանիշի համար որոշակի գումար, գումարը նույնպես փոխանցվում էր հիմնականում կրիպտոարժույթով, իսկ համարանիշի գտնվելու վայրի մասին տեղեկատվությունն ուղարկվում էր տուժողին: Հանցագործությունը լատենտային բնույթ էր կրում. տուժողներն ստիպված գնում էին գործարքի և հիմնականում չէին հայտնում իրավապահ մարմիններին: Այս հանցագործությունների բացահայտումը գործնականում անհնար էր, քանի որ ո՛չ սոցիալական կայքն էր հնարավոր լինում բացահայտել, ո՛չ կրիպտոարժույթների փոխանցումները: Արդյունքում խնդիրը լուծվեց հենց իրավական միջոցով, մասնավորապես՝ վերոնշյալ կառավարության որոշման մեջ կատարվեց փոփոխություն, որով սահմանվեց, որ կորած զույգ համարանիշների փոխարեն կարող են հատկացվել կա՛մ կրկնօրինակը՝ հերթական վերաթողարկմանը համապատասխանող արաբական թվանշանով գրառմամբ (օրինակ՝ առաջին անգամ վերաթողարկվելու դեպքում գրառվում է 1), կա՛մ թվերի ու տառերի այլ հավաքածու պարունակող համարանիշներ:

Իրավական կարգավորումներից դուրս է մնացել սոցիալական կայքերի գործունեությունը, ներկայումս մեծ տարածում է գտել տարբեր դրամահավաքները, կարելի է տարբեր սոցիալական կայքերում նկատել, օրինակ, զոհված զինծառայողների ընտանիքների կարիքների, հաշմանդամ երեխաների վիրահատությունների, ընտանի կենդանիների փրկության կամ ստերջացման համար դրամահավաքների հայտարարությունները, որոնք, սակայն, բացարձակապես չեն վերահսկվում. պարզ չի՝ ովքեր են կազմակերպիչները, ինչքան գումարներ են հավաքում, արդյո՞ք այդ միջոցները ծառայում են նպատակին, ա՞րդյոք վերադարձվում են ավելացած գումարները և այլն: Այս պարագայում իրավական միջոցներով կարելի էր սահմանել վերահսկողություն, արգելել դրամահավաքները կամ նախատեսել կոնկրետ խողովակների միջոցով, որպեսզի ստուգվեն իրական նպատակները, կազմակերպիչները, գումարների և միջոցների բաշխումը և այլն: Սրանք, իհարկե, առանձին դեպքեր են, սակայն կիբեռհանցավորությունն ավելի լայնամասշտաբ է և բազմաբնույթ, ուստի անհրաժեշտ է ամբողջ ծավալով օգտագործել կիբեռհանցավորության դեմ պայքարի իրավական միջոցների գործիքակազմը:

<u>Ընդհանուր վիկտիմոլոգիական կանխարգելման ակադեմիական միջոցներ:</u>

Ակադեմիական միջոցները ենթադրում են գիտական հանրույթի գործունեության ակտիվացում կիբեռհանցավորության վիկտիմոլոգիական կանխարգելման ոլորտում: Դա կարող է իրականացվել գիտական միջոցառումների (համաժողովներ, սեմինարներ, քննարկումներ և այլն), հոդվածների և զեկույցների հրապարակման միջոցով: Այս միջոցառումները կարող են իրականացվել ինչպես գերատեսչությունների, ուսումնական հաստատությունների, այնպես էլ մասնավոր գիտական կազմակերպությունների և անհատ գիտնականների մասնակցությամբ: Հաշվի առնելով կիբեռհանցավորության վտանգավորությունը և մասշտաբները՝ կիբեռվիկտիմոլոգիական կանխարգելման խնդիրները պետք է լինեն գիտական հանրույթի ուշադրության կենտրոնում, օրինակ՝ 2023 թվականի հունիսի 15-ին ՀՀ ՆԳՆ կրթահամալիրում տեղի ունեցավ «Կիբեռհանցավորության դեմ պայքարի քրեաիրավական, քրեադատավարական և կրիմինալոգիական հիմնախնդիրները» թեմայով միջազգային գիտագործնական համաժողով, որտեղ ներկայացված զեկույցներն ընդգրկվեցին «Օրենքի պատվար» գիտամեթոդական ամսագրի 16-րդ համարում:

Ակադեմիական միջոցները պայմանականորեն կարելի է բաժանել 2 մասի՝ գիտական և կրթական:

Գիտական միջոցների շրջանակներում նեղ մասնագիտական հանրույթի առաջ ծագում են հետևյալ մարտահրավերները՝

1. Սահմանել կիբեռվիկտիմոլոգիան և թվային կիբեռվիկտիմիազիան որպես ինքնուրույն հետազոտության ոլորտ,
2. Հստակեցնել տեղեկատվական տարածքում առկա սպառնալիքների նկարագրությունը և դասակարգումը,
3. Մշակել առկա սպառնալիքների հայտնաբերման, նույնականացման և կանխարգելման մեթոդներ,
4. Բացահայտել կիբեռվիկտիմիզացիայի պատճառները և պայմանները,
5. Ուսումնասիրել կիբեռզոհի անձի առանձնահատկությունները և ներազդելու հնարավորությունները,
6. Վերլուծել թվային ծառայությունների անվտանգության ներկա և ապագա խնդիրները (վիկտիմոլոգիական տեսանկյունից),
7. Հետազոտել կիբեռզոհի վարքագծի և պատճառված վնասի միջև կապի առանձնահատկությունները:

Այս հետազոտությունները հնարավորություն կտան թարմացնելու կիբերանվտանգության ապահովման միջոցներն ու մեթոդները հայեցակարգային (տեսական) մակարդակում[8]:

Կրթական մակարդակում նույնպես առկա են որոշակի խնդիրներ, մասնավորապես՝ ինչպես գիտենք, իրավապահ մարմինների աշխատակիցների համար որպես կրթական ցենզ հիմնականում սահմանվում է բարձրագույն իրավաբանական կրթություն: Ուսումնական պլանների և առարկայացանկերի ուսումնասիրությունները ցույց են տալիս, որ ներկայումս իրավաբանական բուհերում նախատեսվող գիտելիքները չեն ապահովում կիբեռհանցավորության դեմ պայքարելու հենքը: ՌԴ-ի մի շարք ուսումնական հաստատություններում արդեն իսկ ներդրվել է կիբեռվիկտիմոլոգիան որպես առանձին դասընթաց: Այս հանցավորության դեմ պայքարում անհրաժեշտ են նեղ մասնագիտական գիտելիքներ՝ տեղեկատվական տեխնոլոգիաների, համացանցի, կիբեռտարածության, ինչպես նաև այս հանցագործությունների պատճառների և պայմանների վերհանման, կանխարգելման և նոր մեթոդների մասին:

<u>Ընդհանուր վիկտիմոլոգիական կանխարգելման կազմակերպակառավարչական միջոցներ:</u>

Այս միջոցները ենթադրում են կիբեռհանցավորության դեմ պայքարի համապատասխան համակարգի ձևավորում, որը կներառի կազմակերպություններ, տեխնոլոգիաներ, գործիքակազմ, նեղ մասնագիտական գիտելիքներով օժտված մասնագետներ:

ՀՀ-ում կիբեռհանցավորության դեմ պայքարի ամբողջ բեռը դրված է ՆԳՆ ոստիկանության և ԱԱԾ-ի համապատասխան մասնագիտական ստորաբաժանումների վրա, սակայն այս մասշտաբի հանցավորության դեմ պայքարը հաջողելու համար սա բավարար չէ:

Մասնագիտական գրականության մեջ բազմիցս նշվում է, որ որքան բարձր է պետության նորարարական զարգացման մակարդակը, այնքան ավելի արդյունավետ է կիբերհանցագործությունների դեմ պայքարը: Մի շարք զարգացած երկրներում կիբեռհանցավորության դեմ պայքարի հարցով զբաղվում են ինչպես պետական հիմնարկների և կազմակերպությունների ներգրավմամբ, այնպես էլ դրամաշնորհներով գործող մասնավոր կազմակերպությունների օգնությամբ: Այս առումով առավել հաջողված են կիբեռհանցավորության դեմ պայքարում ԱՄՆ-ի ձեռքբերումները:

---

[8] Տե՛ս **Жмуров Д. В.**, Общая виктимологическая профилактика киберпреступности. Юридическая наука и практика: Вестник Нижегородской академии МВД России, 2022. № 4 (60) էջ՝137-138:

ԱՄՆ-ում կիբեռհանցավորության կանխարգելմանն ուղղված միջոցառումների կազմակերպման համակարգը բազմակողմանի է և բարդ: Կարևոր դեր է հատկացված ԱՄՆ արդարադատության նախարարությանը (համապետական մակարդակով), որի ենթակառույցները տեղական մակարդակով կատարում են համապատասխան գործառույթներ յուրաքանչյուր նահանգում:

Հետաքննությունների դաշնային բյուրոն ունի հատուկ բաժին՝ կիբեռանվտանգության և ենթակառուցվածքների անվտանգության գործակալությունը, որը հաշվետու է ԱՄՆ ներքին անվտանգության նախարարությանը: Վերջինս ուսումնասիրում ու վերլուծում է համացանցում առկա սպառնալիքները և համապատասխան տեղեկատվություն և ծառայություններ է մատուցում ձեռնարկատիրական կազմակերպություններին՝ հաքերային հարձակումներից և չարտոնված ներխուժումներից պաշտպանելու նպատակով:

ԱՄՆ-ն ունի նաև այլ դաշնային գործակալություններ և ծառայություններ, այդ թվում՝ Միացյալ Նահանգների Գաղտնի ծառայությունը, որի հիմնական գործառույթներն են՝ պաշտպանել երկրի նախագահին, նրա ընտանիքի անդամներին, սեփականությունն ու գաղտնիությունը համացանցում: Բացի այդ, Գաղտնի ծառայությունը տեղական պաշտոնյաներին վերապատրաստում և փոխանցում է նախնական փուլում կիբեռհանցագործության դեմ պայքարի հմտությունները, ինչպես նաև կանխարգելիչ աշխատանքներ է իրականացնում բնակչության շրջանում: ԱՄՆ ներգաղթի և մաքսային մարմինը նույնպես իրականացնում է համացանցում մարդկանց թրաֆիքինգի և սեռական ստրկության սպառնալիքների վերլուծություն և կանխարգելում:

Տեղական մակարդակում գործում է կիբեռհանցագործությունների դեմ պայքարի կենտրոնների ցանցը, որը բաղկացած է ծրագրավորողներից և հաքերային խմբերից: Նման կենտրոնների գործունեությունը շատ արդյունավետ է, քանի որ աշխատակիցների մի մասը նախկին կիբերհանցագործներ են, որոնք աշխատում են իրավապահ մարմինների վերահսկողության ներքո: Վերջիններս տեղեկատվություն են տրամադրում համացանցում անօրինական գործունեության նրբությունների և դրանց դեմ պայքարի մեթոդների մասին: Բացի այդ, պետությունը խրախուսում է կիբեռանվտանգության հատուկ ստորաբաժանումների ստեղծումն ու զարգացումը յուրաքանչյուր հաստատությունում (կազմակերպություններ, ընկերություններ, ինչպես նաև դպրոցներ, համալսարաններ, մանկապարտեզներ): Այսպիսով՝ գրեթե յուրաքանչյուր ոլորտում աշխատում են

մասնագետներ, որոնք վերլուծում են կիբեռտարածության սպառնալիքները և իրազեկում այդ մասին աշխատակիցներին[9]:

Ընդհանուր վիկտիմոլոգիական կանխարգելման գաղափարախոսական միջոցներ:

Այս միջոցները ենթադրում են հասարակության մեջ կիբեռհանցավորության դեմ պայքարի մշակույթի ձևավորում՝ կիբեռհանցավորության կանխման և կիբեռհանցագործների դեմ պայքարին մասնակցելու կարևորության մասին իրազեկության բարձրացման միջոցով. Անհրաժեշտ է հստակեցնել զոհի վարքագծի կարևորությունը, տուժողի տեղն ու դերը վիկտիմոլոգիական կանխարգելման գործընթացներում:

Այս մշակույթի ստեղծման հիմք կարող են լինել հասարակության տարբեր շրջանակների լայնամասշտաբ իրազեկման աշխատանքները: Վիճակագրությունը ցույց է տալիս, որ 3-10 տարեկան երեխաների 71 տոկոսը տարբեր սարքերի միջոցով (սմարթֆոն, համակարգիչ և այլն) մուտք են գործում համացանց, իսկ արդեն 10 տարեկանում երեխաների 91 տոկոսն ունի անձնական օգտագործման սմարթֆոններ[10]: Անհրաժեշտ է կիբեռհանցավորության սպառնալիքների և կանխարգելման մասին դասընթացներ նախատեսել՝ ընհուպ մանկապարտեզներից: Ի վերջո, կիբեռհանցավորության կանխարգելման ամենաարդյունավետ միջոցառումներից մեկը համարվում է հասարակությանն այս վտանգների մասին հնարավորինս իրազեկելը[11]:

---

[9] Տե՛ս https://www.researchgate.net/publication/380226620_Victimological_aspects_of_countering_internet_crime_and_local_government_practices /վերջին մուտք՝ 05.09.2024թ./

[10] Տե՛ս **Рыжова Н.И.**, **Громова О.Н.**, Киберугрозы цифрового социума и их профилактика в рамках виктимологической деятельности // Вестник Российского университета дружбы народов. Серия: Информатизация образования, 2020, Т. 17, № 3, էջ՝ 256:

[11] Տե՛ս, օրինակ, **Իսրայելյան Գ.**, «Հայաստանի Հանրապետությունում համակարգչային հափշտակության ընդհանուր զոհաբանական կանխարգելման արդի խնդիրները», Դատական իշխանություն, ապրիլ-սեպտեմբեր, 4-9 (298-303) 2024թ. էջ՝41-49:

ВИКТИМОЛОГИЧЕСКИЕ МЕРЫ ПРЕДУПРЕЖДЕНИЯ КИБЕРПРЕСТУПНОСТИ

Мнацаканян Артак Самвелович

Начальник управления по учебно-методической работе

и развитию Образовательного комплекса полиции МВД Республики Армения,

подполковник полиции, кандидат юридических наук, доцент

Проблема противодействия киберпреступности стала краеугольным камнем для всех стран, и чтобы добиться успеха в этой масштабной борьбе, необходимо внедрить весь инструментарий предотвращения киберпреступности. Ряд традиционных преступлений совершается с использованием информационных технологий и Интернета, и в этот период борьба с киберпреступностью традиционными мерами профилактики уже не является целесообразной и эффективной. В настоящее время виктимологический инструментарий борьбы с киберпреступностью постепенно становится все более актуальным, в этом смысле кибервиктимология уже не нова.

В статье рассматриваются правовые, научные, организационно-управленческие и идеологические средства общей виктимологической самопрофилактики киберпреступности.

Ключевые слова: Интернет, кибержертва, информационные технологии, профилактика, компьютер, угроза.

VICTIMOLOGICAL MEASURES OF PREVENTION OF CYBERCRIME

Mnatsakanyan Artak

Head of Educational-Methodical and Development Department

Police Educational Complex of the Ministry of Internal Affairs of the Republic of Armenia

Police Lieutenant Colonel, PhD in Law, Associate Professor

The problem of countering cybercrime has become a cornerstone for all countries, and in order to succeed in this large-scale fight, it is necessary to implement the entire toolkit of cybercrime prevention. A number of traditional crimes are committed through information technology and the Internet, and nowadays, fighting cybercrime with traditional prevention measures is no longer appropriate and effective. Currently, the victimological toolkit for combating cybercrime is gradually becoming more relevant, in this respect cybervictimology is no longer a novelty.

The article touches upon the legal, academic, organizational-managerial and ideological means of general victimological prevention of cybercrime.

Key words: Internet, cybervictim, information technology, prevention, computer, threat.

Հոդվածը գրախոսվել է՝ 01.11.2024թ.
Ներկայացվել է տպագրության՝ 13.09.2024թ.