https://doi.org/10.53587/25792865-2025.13-62

ԿԻԲԵՌՀԱՆՑԱՎՈՐՈՒԹՅԱՆ ԴՐՍԵՎՈՐՈՒՄՆԵՐԸ ԵՎ ԴՐԱՆՑ ՀԱԿԱԶԴՄԱՆ ՄԻՋՈՑՆԵՐԸ ՀԱՅԱՍՏԱՆԻ ՀԱՆՐԱՊԵՏՈՒԹՅՈՒՆՈՒՄ

Իսրայելյան Գ.Վ., Ղուկասյան Ա.Պ.

Փորձաքննությունների ազգային բյուրո,
Երևան, Հայաստան

Հեռահաղորդակցության և տեղեկատվական տեխնոլոգիաների բուռն զարգացումը, բնակչությանը մատուցվող ծառայությունների թվայնացումը և արհեստական բանականության ներթափանցումը կենցաղ վերջին տարիներին Հայաստանում հանգեցրել է կիբեռհանցավորության շարունակական աճի: Դա խոսում է կանխարգելիչ ներգործության ակտիվացման անհրաժեշտության մասին:

Այդ ուղղությամբ առաջարկություններ ներկայացնելու նպատակով հեղինակների կողմից իրականացվել է կիբեռհանցավորության քրեաբանական բաղադրիչների հետազոտություն: Մասնավորապես, բացահայտվել է 2019-2024թթ. կիբեռհանցավորության վիճակը, շարժընթացը, լատենտայնությունը պայմանավորող գործոնները, նկարագրվել են կիբեռհանցավորության կազմում ընդգրկված հանցատեսակներից ամենատարածվածի՝ համակարգչային հափշտակության կատարման տիպային եղանակները:

Կատարված հետազոտության արդյունքների վերլուծության հիման վրա հեղինակներն առաջարկում են կիբեռհանցավորության հակազդման միջոցներ:

Բանալի բառեր. *կիբեռհանցավորություն, համակարգչային հափշտակություն, տիպային եղանակ, հակազդման միջոցներ:*

Վերջին տարիներին Հայաստանի Հանրապետությունում արձանագրվում է կիբեռհանցավորության շեշտակի աճ [1, էջեր 35-36, 2, էջեր 16-17]: Չնայած այդ հանգամանքին, Հայաստանի Հանրապետությունում տվյալ խնդիրը քրեաբանների կողմից գիտական հարթակներում բավարար չափով հետազոտված չէ: Նշվածը պայմանավորում է սույն հետազոտության անհրաժեշտությունն ու արդիականությունը:

Հետազոտության նպատակն է ուսումնասիրել կիբեռհանցավորության դրսևորումները և ներկայացնել դրա հակազդմանն ուղղված առաջարկություններ:

Կատարված ուսումնասիրությունները վկայում են, որ նախկինում կիբերհանցագործությունների վերաբերյալ վիճակագրության ձևավորման համար չկար

Թղթակցական հասցեն՝ Իսրայելյան Գևորգ Վովայի, ՀՀ ԳԱԱ փորձաքննությունների ազգային բյուրոյի քրեաբանության կիրառական հիմնախնդիրների գիտահետազոտական կենտրոնի պետ, Եվրասիա միջազգային համալսարանի դասախոս, իրավաբանական գիտությունների թեկնածու, դոցենտ, էլ. հասցե՝ g_i_1979@mail.ru

միասնական մեթոդաբանություն: Այսպես, ըստ ՀՀ ՆԳՆ քրեական ոստիկանության գլխավոր վարչության տեղեկատվության՝ 2023թ-.ին գրանցվել է 1237 կիբեռհանցագործության դեպք [3], մինչդեռ ՀՀ ՆԳՆ Ինֆորմացիոն կենտրոնում հաշվառվել է ընդամենը 671 դեպք [4]:

Նշված անհամապատասխանությունը պայմանավորված է այն հանգամանքով, որ ՀՀ ՆԳՆ քրեական ոստիկանության գլխավոր վարչությունն իր կողմից վարվող վիճակագրությունում ներառել է նաև այն խարդախությունները (ՀՀ քրեական օրենսգրքի 255-րդ հոդվածով սահմանված), որոնք կատարվել են համակարգչային ցանցն օգտագործելով և չեն որակվել ՀՀ քրեական օրենսգրքի (այսուհետ՝ Օրենսգիրք) 257-րդ հոդվածով, մինչդեռ ՀՀ ՆԳՆ ինֆորմացիոն կենտրոնը հետևողականորեն առաջնորդվել է Օրենսգրքի 2-րդ հավելվածով նախատեսված կիբեռհանցագործությունների ցանկով (ընդունված ՀՀ ԱԺ կողմից 24.10.2024թ. ՀՕ 392-Ն օրենքով), որում և նշված խարդախությունները չեն ընդգրկվել:

Ի դեպ, նշված ցանկում տեղ չեն գտել համակարգչային տեխնիկայի կամ համացանցի օգտագործմամբ կատարվող մի շարք այլ հանցագործություններ (օրինակ՝ Օրենսգրքի 162, 163, 204, 205, 239, 270, 279, 328, 330, 393, 422, 426, 427, 4 28, 483, 484, 485, 502 հոդվածներով սահմանված և այլն):

Հաշվի առնելով վերը նշվածը՝ գտնում ենք, որ այս առումով հարկ կլինի լրամշակել արդեն իսկ օրենսդրական ամրագրում ստացած կիբեռհանցագործությունների ցանկը՝ այն համապատասխանեցնելով առկա իրողություններին:

Մեր կարծիքով, կիբեռհանցավորությունն իր մեջ ներառում է՝

- ✓ համակարգչային համակարգի և համակարգչային տվյալների անվտանգության դեմ ուղղված հանցագործությունները (Օրենսգրքի 359-365 հոդվածներով սահմանված),
- ✓ կիբեռհափշտակությունները, այդ թվում համացանցային խարդախությունը (Օրենսգրքի 255 հոդված), համակարգչային հափշտակությունը (Օրենսգրքի 257 հոդվածով սահմանված),
- ✓ պոռնկագրական նյութեր կամ առարկաներ պատրաստելը, տարածելը կամ պահպանելը (Օրենսգրքի 300 հոդվածով սահմանված),
- ✓ համակարգչային տեխնիկայի կամ համացանցի օգտագործմամբ կատարվող այլ հանցագործությունները (Օրենսգրքի 162, 163, 204, 205, 239, 270, 279, 328, 329, 330, 393, 422, 426, 427, 428, 483, 484, 485, 502 և այլ հոդվածներով սահմանված):

Համաձայն ՀՀ ՆԳՆ ինֆորմացիոն կենտրոնի տվյալների՝ եթե 2019թ. Հայաստանում գրանցվել է կիբեռհանցագործությունների 126 դեպք, ապա 2020թ.՝ 209, 2021թ.՝ 279, 2022թ.՝ 521, 2023թ.՝ 671, 2024թ.՝ 812: ***Փաստորեն, վերջին հինգ տարիների ընթացքում կիբեռհանցագործությունների թիվն աճել է ավելի քան վեց անգամ:***

Հաշվի առնելով այն հանգամանքը, որ 2024թ.-ի ընթացքում արձանագրված կիբեռհանցագործությունների 97,0%-ը բաժին է հասել համակարգչային հափշտակություններին [3], հարկ է առավել հանգամանալից անդրադառնալ վերջիններիս:

Համակարգչային հափշտակության դեպքերի վերջին տարիների շարժընթացը նույնպես դրսևորել է աճի կայուն միտում. եթե 2019թ. արձանագրվել է 80 դեպք, ապա 2020-ին՝ 157, 2021-ին՝ 178, 2022-ին՝ 456, 2023-ին՝ 618, 2024-ին՝ 788: ***Փաստորեն, վերջին հինգ տարիների ընթացքում համակարգչային հափշտակության դեպքերի թիվն աճել է մոտ 10 անգամ:***

Այսուհանդերձ, ինչպես նշում են փորձագետները, վերը նշված վիճակագրական ցուցանիշները բնավ չեն արտացոլում կիբեռհանցավորության իրական վիճակը. այն ունի բարձր լատենտայնություն: Միջազգային փորձագետների գնահատմամբ՝ Հայաստանում կարող է տարեկան կատարվել մոտ 100,000 կիբեռհանցագործություն [5]:

Լատենտայնությունը կարող է պայմանավորվել մի շարք գործոններով, ինչպես օրինակ.

- անձը չի կարողանում մուտք գործել սոցցանցերի իր օգտահաշիվ, մտածելով, թե տեխնիկական խնդիր է,
- անձը գտնում է, որ կիբեռհանցագործությունները գրեթե չեն բացահայտվում, դիմելու դեպքում էլ անիմաստ ժամանակի կորուստ է լինելու ,
- ռեպուտացիոն ռիսկերը, երբ հանցագործներն ապօրինի հասանելիություն են ստացել որևէ բանկի հաճախորդների տվյալներին, ու բանկը գերադասում է ինքը խնդիրը լուծել՝ առանց իրավապահներին դիմելու ,
- քննության ընթացքում հնարավոր է բացահայտվեն տուժողի համար ոչ ցանկալի տեղեկություններ:

Մեր կողմից կատարված ուսումնասիրության արդյունքները ցույց են տալիս, որ հանցավոր տրանզակցիա կատարելու համար խարդախներն անհրաժեշտ վավերապայմանները ձեռք են բերում հետևյալ հնարքներով.

1. Ֆիշինգ (անգլերեն fishing՝ ձկնորսություն): Որպես «կարթ»՝ հանցագործներն օգտագործում են հատուկ ստեղծված ինտերնետային կայք՝ բանկային հաշիվ մուտք գործելու վավերապայմաններ նախատեսող դաշտերով, իսկ որպես «խայծ»՝ որոշակի պատրվակ, որը հայտնվում է տուժողին՝ նշված կայք մտնելու և վճարման վավերապայմանները լրացնելու համար :

Օրինակ, հանցագործը հետևում է «List.am» կայքում որևէ ապրանքի վաճառքի թարմ հայտարարություններին, ընտրում է դրանցից մեկը, որևէ մեսենջերներով (Viber, Telegram, WhatsApp) մտնում վաճառողի հետ նամակագրության մեջ և հայտնում ապրանքը գնելու իր մտադրության մասին: Այնուհետև տվյալ մեսենջերով վաճառողին է ուղարկում կեղծ հղում, որտեղ առաջարկում է լրացնել վերջինիս քարտային վավերապայմանները՝ ապրանքի գումարը «ուղարկելու» համար: Հիպերհղումով անցնելով, համացանցի անուշադիր օգտատերը կարող է և չնկատել զեղծարարությունը, քանի որ նման էջերն արտաքնապես նման են հայտնի ծառայությունների կայքերի ձևավորմանը («Հայ Փոստի» կամ տարբեր բանկերի): Իրականին նման կարող է լինել նաև կեղծ վեբ-էջի հասցեն (haypost-online.com, ameriabank_24.am և այլն): Եթե գնորդը «կուլ է տալիս խայծը» և լրացնում է կեղծ ձևանմուշը , ապա հանցագործին են անցնում համապատասխան բանկային հաշիվ

մուտք գործելու գնորդի վավերապայմանները: Հաշված րոպեների ընթացքում հանցագործը մուտք է գործում տվյալ անձի բանկային հաշիվ և առկա դրամական միջոցները փոխանցում իր կողմից վերահսկվող այլ բանկային հաշվին, էլեկտրոնային դրամապանակներին կամ կրիպտոհաշիվներին:

Հարկ է նշել, որ վերջին ժամանակաշրջանում հաճախակի են դարձել նաև որոնողական համակարգերում օգտատերերի հարցումները հասցեագրող ֆիշինգ կայքերի ստեղծման դեպքերը: Քաղաքացիները դրանց վրա անմիջականորեն դուրս են գալիս բրաուզերների (Google, Yandex և այլն) փնտրողական հարցումների միջոցով: Տեսնելով որոնման արդյունքում արտացոլված կայքի «ծանոթ վերնագիրը և տարբերանշանը» և չստուգելով կայքի հասցեի և բանկային հաստատության դոմենային հասցեի համապատասխանությունը՝ տուժողը կեղծ ձևանմուշում լրացնում է քարտի անհրաժեշտ վավերապայմանները, որոնք անմիջականորեն հայտնվում են հանցագործի ձեռքում:

Օրինակ, հանցավորը «Facebook» կամ «Instagram» սոցիալական կայքով ներկայանում է որևէ կազմակերպության (օրինակ՝ «Գազպրոմ» ընկերության) մենեջեր կամ նմանատիպ ծրագրերով զբաղվող այլ կազմակերպության աշխատակից կամ ֆինանսական խորհրդատու, ներդրումային կեղծ կայքերում ներդրում կատարելու և եկամուտի հետ միասին հետ փոխանցելու պատրվակով տուժողից պահանջում և փոխանցման միջոցով ստանում է գումար, սակայն փոխանցելուց հետո խաբեությամբ հափշտակում է այն:

2. «Օգնություն ընկերոջը»: Հանցագործները գաղտնաբառի գուշակման կամ ֆիշինգի միջոցով ձեռք են բերում չարտոնված մուտք (հակում) դեպի սոցցանցի էջեր, որից հետո հաղորդագրություններ են ուղարկվում կոտրված էջի «Ընկերներ» բաժնում առկա այլ օգտատերերին՝ տարբեր պատրվակներով լուսանկար կամ բանկային վճարային քարտի տեղեկատվություն տրամադրելու խնդրանքով (օրինակ՝ շտապ անկանխիկ վճարում կատարելու համար, քանի որ դիմումատուի քարտն իբրև թե արգելափակված է), կամ «ընկերոջ» անունից խարդախը կարող է խնդրել որոշակի գումար փոխանցել իր քարտին՝ կյանքի դժվարին իրավիճակում հայտնվելու կապակցությամբ: Դյուրահավատ օգտատերը, կարծելով, որ շփվում է էջի իրական տիրոջ հետ, փոխանցում է պահանջվող գումարը կամ հանցագործին հայտնում իր բանկային քարտի տվյալները (հաճախ նաև բանկի կողմից SMS հաղորդագրությամբ ուղարկված անվտանգության կոդը), որից հետո գումարը հափշտակվում է քարտային հաշվից:

Օրինակ, հանցագործը համացանցի «Facebook.com» սոցիալական ցանցում, տուժողի՝ հիմնականում արտերկրում՝ ԱՄՆ-ում կամ ՌԴ-ում գտնվող ընկերոջ անունով և նկարներով ֆեյսբուքյան էջ է բացում ու խաբեությամբ փրկանում որպես օգնություն տուժողի կողմից «Թել-Սել» հավելվածով կամ այլ էլեկտրոննային եղանակով փոխանցված գումարին:

Սոցիալական ցանցերում տարածված «ընկերոջն օգնելու» խարդախության մեկ այլ տեսակ է բուժման նպատակով կեղծ բարեգործական ֆոնդերի ստեղծումը: Նման

դեպքերում խաբեբաները խումբ են ստեղծում և տեղեկատվություն տարածում, թե իբր միջոցներ են անհրաժեշտ ծանր հիվանդ մարդու (հաճախ՝ երեխայի) բուժման համար:

3. Վիֆիշինգ (անգլերեն voice fishing կամ «ձայնային ձկնորսություն»): Հանցագործները զանգահարում են տուժողի բաժանորդային հեռախոսահամարին կամ նրա մեսենջերի հաշվին (հիմնականում WhatsApp, Viber կամ Telegram): Խոսակցության ընթացքում հանցագործը ներկայանում է որպես բանկի կամ իրավապահ մարմնի աշխատակից (ՆԳՆ, ԱԱԾ, Քննչական կոմիտե) և մտացածին պատրվակով (կասկածելի գործարքի կասեցում, քարտի օգտագործման անվտանգության մակարդակի բարձրացում, բանկային հաշվի սեփականատիրոջ անձնագրային տվյալների վերստուգում և այլն), դրամական միջոցներ հափշտակելու նպատակով տուժողից տեղեկություններ է կորզում բանկային վճարային քարտերի առկայության, դրանց գործածության ժամկետների, CVV կոդերի, անձնագրային տվյալների, SMS կոդերի մասին: Որոշ դեպքերում հանցագործները տիրապետում են բանկային վճարային քարտերի որոշ վավերապայմաններին, ինչպես նաև այն անձանց անձնական տվյալներին, որոնց անունով դրանք թողարկվել են: Շատ դեպքերում հանցագործները զանգեր կատարելիս օգտագործում են IP հեռախոսակապ (տուժողը իր հեռախոսի էկրանին տեսնում է փոփոխված համար:)

Օրինակ, որևէ բանկի տարբերանշանով «WhatsApp» մեսենջերով կամ բջջային հավելվածով կամ «բանկի հեռախոսահամարով» քաղաքացու հետ կապ հաստատած անձը ներկայանում է որպես փվյալ բանկի աշխատակից, հավելվածի անվտանգությունն ապահովելու պատրվակով խաբեությամբ տիրանում է տուժողի բանկային քարտի տվյալներին և հաշվեհամարից կանխիկացնում գումար կամ ձևակերպում առցանց վարկ:

4. Բանկային քարտին հասանելիություն: Բանկային հաշիվներից գողություն կատարելու համար միշտ չէ, որ հանցագործներն օգտագործում են խորամանկ սխեմաներ: Որոշ դեպքերում դրան կարող են նպաստել.

- ✓ բանկային քարտի կորուստը,
- ✓ դրանց մատչելի վայրերում թողնելը,
- ✓ մեկանգամյա վճարումներ կատարելու համար այլ անձանց փոխանցելը,
- ✓ PIN կոդը քարտին կից պահելը (օրինակ՝ թղթի վրա գրված PIN կոդը դրամապանակում պահելը կամ բանկային քարտի վրա նշելը),
- ✓ բանկային քարտի լուսանկարչական պատկերների կամ վճարման վավերապայմանների պահպանումը բջջային հեռախոսում, փոստային օգտահաշվում կամ հեռավար ամպային պահեստարանում:

5. Գնում կանխավճարով: Ինտերնետային խարդախության ամենապարզունակ, բայց ոչ պակաս արդյունավետ ձևերից է վիրտուալ ազդագրերում, թեմատիկ կայքերում, սոցիալական ցանցերում և ինտերնետ մեսենջերների խմբերում որոշակի ապրանքի «շահեկան» գներով վաճառքի գովազդ տեղադրելը: Ապրանքը փոստային կամ առաքման ծառայության միջոցով ստանալու համար ընդամենը անհրաժեշտ է կատարել որոշակի կանխավճար «վաճառողի» կողմից նշված բանկային քարտին կամ

էլեկտրոնային դրամապանակին: Փոխանցումը կատարելուց հետո, իհարկե, ապրանքն այդպես էլ չի առաքվում, իսկ «վաճառողն» անհետանում է:

6. Շանտաժ: Այս դեպքում հանցագործները գումար շորթելու նպատակով սպառնում են տուժողին, որ կտարածեն նրա վերաբերյալ վարկաբեկիչ տեղեկություններ: Օրինակ, ստանալով չարտոնված մուտք դեպի ինտերնետ ռեսուրսներ (սոցիալական ցանցերի էջեր, էլ. նամակագրություն և ամպային օգտահաշիվներ) և տիրանալով հանրայնացման համար անցանկալի նկարների, տեսագրությունների կամ գրագրության, հանցագործները նամակագրություն են սկսում տուժողի հետ՝ շորթելով տարբեր գումարներ, չվճարելու դեպքում՝ սպառնալով դրանք տարածել համացանցում:

7. Խարդախության այլ ձևեր.

– Խարդախը խնդրում է լիցքավորել որոշակի բջջային հեռախոսահամար կամ վճարային քարտ՝ «Մայրիկ, լիցքավորիր այս հաշիվը 500 դրամով: Ինձ հետ մի զանգիր, ես քեզ ավելի ուշ կզանգեմ: Շտապ է պետք:» գրառմամբ:

– Խարդախը զանգում է և անմիջապես անջատում է հեռախոսը, իսկ երբ տուժողը կատարում է հետադարձ զանգ՝ բաժանորդը միանում է ինքնապատասխանիչին: Արդյունքում՝ նրա բջջային հեռախոսի հաշվից գումար է գանձվում, քանի որ զանգը վերահասցեավորվում է վճարովի համարին:

– Տուժողը ստանում է SMS հաղորդագրություն ինչ-որ շահումի մասին, որից հետո բաժանորդին առաջարկում են «շահումը» ստանալու համար ուղարկել վճարովի հաղորդագրություն կամ փոխանցել ոչ մեծ գումար ինչ-որ բանկային քարտի:

– Տուժողը ստանում է SMS հաղորդագրություն՝ ինչ-որ հղումով, որը գործարկելու դեպքում սկսվում է վիրուսի նպատակային ներբեռնման գործընթաց:

– Տուժողը ստանում է SMS հաղորդագրություն կամ զանգ, որով հաղորդվում է, որ բաժանորդը չի վճարել տուգանքը, որից հետո անձին խնդրում են վճարել այն՝ գումար փոխանցելով «հատուկ» ընթացիկ հաշվին կամ համալրելով կոնկրետ բանկային հաշիվը:

– Տուժողը ստանում է SMS հաղորդագրություն այն մասին, որ վճարային քարտը արգելափակված է, և նշվում է հեռախոսահամար, որով կարող է ստանալ տեղեկատվություն և աջակցություն: Տուժողի կողմից տվյալ հեռախոսահամարով զանգ կատարելուց հետո նրանից պահանջվում է PIN կոդ, CVV կոդը (քարտի դարձերեսի եռանիշ կոդը), քարտի համարը և այլ տվյալներ, որոնք անհրաժեշտ են բանկային հաշվից գումար հանելու համար:

Թվարկված եղանակներով կատարվող հափշտակությունների պարագայում հանցագործները, որպես կանոն, ձեռք են բերում կրիպտոարժույթ, որի շարժը վերահսկելի չէ, կամ հափշտակված գումարները փոխանցվում են հանցագործների կողմից տնօրինվող, սակայն այլ անձանց պատկանող բանկային քարտերին, որոնցից այնուհետև կանխիկացվում կամ փոխանցվում են Հայաստանում գործունեություն ծավալող բուքմեյքերական ընկերությունների խաղային հաշիվներին:

Հաշվի առնելով խնդրո առարկա հանցագործությունների կատարման առանձնահատկությունները՝ **հատուկ կանխարգելման** կազմակերպման ուղղությամբ առաջարկում ենք.

1) լուծել իրավապահ մարմինների տեխնիկական վերազինման, համապատասխան հավելվածներ հասանելիության հարցը, մասնավորապես՝ պարբերաբար համագործակցել «Chainalysis» ընկերության տարածաշրջանային ներկայացուցչության հետ՝ հատկապես «Reactor» ծրագրային ապահովումից օգտվելու ժամանակավոր արտոնագրեր ստանալու նպատակով, որի միջոցով հնարավոր է տեղեկություններ ստանալ Հայաստանի Հանրապետությունում շրջանառվող կիրոպտոարժույթների վերաբերյալ,

2) իրականացնել Հայաստանի Հանրապետության տեղեկատվական տիրույթի, մասնավորապես՝ դոմենային տիրույթի և հայտնի սոցիալական ցանցերի հայկական սեգմենտի մշտադիտարկում, օպերատիվորեն հայտնաբերել համացանցում անօրինական բովանդակությամբ համապատասխան տեղեկատվություն և համարժեք արձագանքել դրան [6, էջ 88],

3) ապահովել մշտական համագործակցություն կիբեռհանցագործությունների դեմ պայքարի ոլորտում ներգրավված միջազգային կառույցների և կազմակերպությունների, օտարերկրյա պետությունների համապատասխան ստորաբաժանումների հետ,

4) մշակել կիբեռհանցավորության դեմ պայքարի պետական ռազմավարություն:

Համակարգչային հափշտակությունների կանխարգելման համար հատկապես արդյունավետ են **զոհաբանական բնույթի կանխարգելիչ միջոցառումները:** Այս ուղղությամբ, մեր կարծիքով, անհրաժեշտ է.

1. Բնակչության շրջանում անցկացնել համակարգչային հափշտակությունների և այլ կիբեռհանցագործությունների զոհաբանական հարցերով սեմինարներ, քննարկումներ և այլ միջոցառումներ, մասնավորապես՝ կազմակերպել զոհաբանական իրադրությունում համարժեք վարքի դրսևորման հոգեբանական թրեյնինգներ, անցկացնել զոհային վարքի նախականխումն ապահովող գործոնների վերաբերյալ դասախոսություններ, խմբային հոգեթերապիաներ:

2. Իրավապահ մարմինների միջոցով բնակչության շրջանում անցկացնել իրազեկման միջոցառումներ այն մասին, թե ինչպես խուսափել զոհածին իրավիճակից, ինչպիսի վարքագիծ դրսևորել համացանցային կասկածելի ծանոթությունների առաջարկ ստանալիս, ում դիմել համակարգչային հափշտակությունից տուժելու դեպքում, ինչպես նաև տեղեկատվություն տարածել համակարգչային հափշտակություններ կատարողի անձի առանձնահատկությունների և հանցանքի կատարման արդի ձևերի մասին [7, էջ 45]:

Նշված միջոցառումների շրջանակներում զոհածին վարքի դրսևորումից խուսափելու համար արդյունավետ կարող է համարվել հասարակությանը լրատվամիջոցներով պարբերաբար հորդորել պահպանելու հետևյալ սկզբունքները.

1. Երբեք և ոչ մի պարագայում որևէ մեկին չի կարելի հայտնել սեփական բանկային հաշիվների և բանկային քարտերի վավերապայմանները, ներառյալ այն

անձանց, ովքեր ներկայանում են որպես բանկի կամ իրավապահ մարմինների աշխատակիցներ (երբ հնարավոր չէ արժանահավատորեն պարզել նրանց ինքնությունը):

Եթե զանգ եք ստանում «բանկի աշխատակցից», ապա պետք է ճշտել վերջինիս անունն ու հեռախոսահամարը, ավարտել խոսակցությունը և զանգահարել բանկ՝ բանկի հեռախոսահամարով: Պետք է հաշվի առնել, որ բանկի իրական աշխատակիցը գիտի հետևյալ տվյալները՝ քարտատիրոջ ազգանունը, անձնագրի տվյալները, թե որ քարտերն են թողարկվել, հաշվի մնացորդը: Առավել ևս պետք է գիտենալ, որ բանկային հաստատությունների աշխատակիցները հաճախորդների հետ շփվելու համար երբեք չեն օգտագործում մեսենջերներ (Viber, Telegram, WhatsApp):

Հեռախոսային խոսակցության ընթացքում (նույնիսկ բանկի աշխատակցին), ինչպես նաև սոցիալական ցանցերում հաղորդակցվելու միջոցով չպետք է հայտնել քարտի ամբողջական համարը, դրա գործողության ժամկետը, CVC/CVV կոդը (գտնվում է քարտի դարձերեսին), ինտերնետ-բանկինգի մուտքանունն և գաղտնաբառը, անձնագրի տվյալները, կոդ բառը (թվային կոդը) SMS հաղորդագրություններից:

Եթե «բանկի աշխատակիցը» զրույցի ընթացքում տեղեկացնում է, որ հաճախորդի քարտով չարտոնված գործարքներ են կատարվում, պետք է պատասխանել, որ անձամբ եք գալու բանկ, քանի որ նման բոլոր հարցերը պետք է լուծվեն բանկի մասնաճյուղում, ոչ թե հեռախոսով:

2. Առցանց վճարումներ կատարելու համար պետք է օգտվել միայն վստահելի վճարային ծառայություններից, անպայման ստուգել ռեսուրսի դոմենի անունը բրաուզերի հասցեագոտում:

3. Չի կարելի պահել բանկային քարտերը, դրանց լուսանկարները և վավերապայմաններն այնպիսի վայրերում, որոնք կարող են հասանելի լինել կողմնակի անձանց: Նույնը վերաբերում է հանրայնացման ոչ ենթակա (կոնֆիդենցիալ բնույթի) լուսանկարներին, տեսաձայնագրություններին և գրագրությանը:

4. Եթե չկան հավաստի տեղեկություններ գումարի հասցեատեր սուբյեկտի իսկության վերաբերյալ, անհրաժեշտ է ձեռնպահ մնալ առցանց վճարումներ կատարելուց (կապված ապրանքների և ծառայությունների համար կանխավճարների, կազմակերպությունների և անհատների օգտին կատարվող բարեգործության, հովանավորչության և այլնի հետ):

5. Չի կարելի ինտերնետի օգտատերերի խնդրանքով գումար փոխանցել անծանոթ էլեկտրոնային դրամապանակի, բանկային վճարային քարտի, SIM քարտին կցված հաշիվներին:

6. Բանկային հեռավար սպասարկման համակարգեր (ինտերնետ բանկինգ, մոբայլ բանկինգ), էլեկտրոնային փոստարկղեր, սոցիալական ցանցերի

օգտահաշիվներ և այլ ռեսուրսներ մուտք գործելու համար անհրաժեշտ է օգտագործել բարդ գաղտնաբառեր, որոնք կբացառեն դրանց կռահումը: Պետք է ձեռնպահ մնալ այն գաղտնաբառերից, որոնք պարունակում են ծննդյան ամսաթվեր, անուններ, ազգանուններ և այլն (որոնք հեշտությամբ կարելի է գտնել տեղեկատվության հանրամատչելի աղբյուրներից, սոցիալական ցանցերից):

7. Երբ սոցիալական ցանցերում բանկային վճարային քարտի մանրամասների հարցումով հաղորդագրություն է ստացվում «Ընկերոջից», առանց դրան պատասխանելու, անհրաժեշտ է ուղղակիորեն կապվել այդ օգտատիրոջ հետ կապի այլ միջոցներով:

8. Սոցիալական ցանցի օգտահաշիվը կոտրելու դեպքում աջակցության ծառայության միջոցով անհրաժեշտ է անհապաղ վերականգնել մուտքն այնտեղ կամ այն արգելափակել՝ զուգահեռաբար այդ փաստի մասին զգուշացնելով սոցիալական ցանցի շփման շրջանակին:

9. Անհրաժեշտ է խուսափել անծանոթ էլփոստի հասցեից կամ մեսենջերի օգտահաշվից ստացված ֆայլը բացելուց կամ մրցանակի կամ շահումի մասին հաղորդագրության հղումով անցում կատարելուց:

Կիբեռհանցավորության **լատենտայնության կանխարգելման** ուղղությամբ, կարծում ենք, անհրաժեշտ է.

1. իրականացնել բնակչության իրավագիտակցության բարձրացման միջոցառումներ, մասնավորապես՝ ձևավորել իրավունքների պաշտպանության հարցով իրավասու մարմիններին դիմելու պահանջմունք (պահանջատիրությունը),

2. գաղափարախոսական աշխատանքներ տանել կիբեռհարձակումների թիրախում գտնվող կազմակերպությունների, օրինակ՝ բանկերի անձնակազմի հետ՝ ինքնուրույն պայքար իրականացնելուց հրաժարվելու մոտեցում ձևավորելու նպատակով,

3. իրականացնել իրավապահ մարմինների հեղինակության և նրանց հանդեպ վստահության բարձրացման միջոցառումներ, ինչը հենք կհանդիսանա կիբեռհանցագործությունների վերաբերյալ բնակչության կողմից տեղեկատվություն հայտնելու համար [8, էջեր 63-74]:

Ամփոփելով կատարված վերլուծությունները՝ անհրաժեշտ է փաստել հետևյալը.

Հեռահաղորդակցության բուռն զարգացումը, բնակչությանը մատուցվող ծառայությունների թվայնացումը և արհեստական բանականության ներթափանցումը կենցաղ վերջին տարիներին Հայաստանում հանգեցրել է կիբեռհանցավորության շարունակական աճի: 2019-2024թթ. վիճակագրական տվյալների վերլուծության արդյունքները ցույց են տալիս, որ կիբեռհանցավորության կազմում ընդգրկված հանցատեսակներից ամենատարածվածը կիբեռհափշտակություններն են: Դրանց կատարման տիպային եղանակներն են ֆիշինգը, «օգնությունն ընկերոջը», վիֆիշինգը,

բանկային քարտին, հասանելիությունը, կանխավճարով գնումը և խարդախության այլ ձևերը:

Նախկինում կիբերհանցագործությունների վերաբերյալ վիճակագրության ձևավորման համար չկար միասնական մեթոդաբանություն: Արդյունքում ի հայտ է եկել տվյալների անհամապատասխանություն: Բացի այդ, Օրենսգրքի՝ կիբեռհանցագործությունների ցանկում տեղ չեն գտել համակարգչային տեխնիկայի կամ համացանցի օգտագործմամբ կատարվող մի շարք այլ հանցագործություններ: Ուստի անհրաժեշտ է ապահովել վիճակագրության միասնական մեթոդաբանությունը և լրամշակել օրենսդրական ամրագրում ստացած կիբերհանցագործությունների ցանկը՝ այն համապատասխանեցնելով առկա իրողություններին:

Հաշվի առնելով խնդրո առարկա հանցագործությունների կատարման առանձնահատկությունները՝ հատուկ կանխարգելման կազմակերպման ուղղությամբ անհրաժեշտ է լուծել իրավապահ մարմինների տեխնիկական վերազինման, համապատասխան հավելվածներ հասանելիության հարցը, իրականացնել Հայաստանի Հանրապետության տեղեկատվական տիրույթի մշտադիտարկում, մշակել կիբեռհանցավորության դեմ պայքարի պետական ռազմավարություն և այլն:

Զոհաբանական կանխարգելման ուղղությամբ անհրաժեշտ է բնակչության շրջանում կազմակերպել կիբեռհանցագործությունների զոհաբանական հարցերով սեմինարներ, քննարկումներ և այլ միջոցառումներ, իրավապահ մարմինների միջոցով բնակչության շրջանում անցկացնել իրազեկման միջոցառումներ այն մասին, թե ինչպես խուսափել զոհածին իրավիճակից, ինչպիսի վարքագիծ դրսևորել համացանցային կասկածելի ծանոթությունների առաջարկ ստանալիս, ում դիմել համակարգչային հափշտակությունից տուժելու դեպքում և այլն:

Կիբեռհանցավորության լատենտայնության կանխարգելման ուղղությամբ անհրաժեշտ է իրականացնել բնակչության իրավագիտակցության բարձրացման, գաղափարախոսական, իրավապահ մարմինների հեղինակության և նրանց հանդեպ վստահության բարձրացման միջոցառումներ:

Գրականության ցանկ

1. Հայաստանի Հանրապետության դատախազության 2022 թվականի գործունեության մասին հաղորդում, էջեր 35-36 // https://www.prosecutor.am/storage/dynamic_web_pages/rep_50_8560351818.pdf (վերջին մուտք՝ 03.03.2025թ):.
2. Հայաստանի Հանրապետության դատախազության 2023 թվականի գործունեության մասին հաղորդում, էջեր 16-17 //https://www.prosecutor.am/storage/dynamic_web_pages/dyn_page_285_1465690793.pdf (վերջին մուտք՝ 03.03.2025թ):.
3. https//www.police.am/news/view/kan[argeich201021.html (վերջին մուտք՝ 03.03.2025թ):.

4. ՀՀ ՆԳՆ ինֆորմացիոն կենտրոնի պաշտոնական վիճակագրություն // https://www.police.am/search.html?search=%D5%BE%D5%AB%D5%B3%D5%A1%D5%AF%D5%A1%D5%A3%D6%80%D5%B8%D6%82%D5%A9%D5%B5%D5%B8%D6%82%D5%B6 (վերջին մուտք՝ 03.03.2025թ):.
5. ՀՀ-ում ամենատարածվածը ֆիշինգն է: ՔԿ-ն հուշում է ինչպես չդառնալ կիբեռհանցագործության զոհ // https://kizaket.am/news/805799 (վերջին մուտք՝ 03.03.2025թ):.
6. Իսրայելյան Գ., Տեղեկատվական և հաղորդակցական տեխնոլոգիաների օգտագործման միջոցով կատարվող հափշտակությունների տիպային մեխանիզմները և կանխարգելման միջոցները Հայաստանի Հանրապետությունում // Դատական իշխանություն, հուլիս-սեպտեմբեր 2024, 7-9 (301-303), էջեր 85-91:
7. Իսրայելյան Գ, . Համակարգչային հափշտակության ընդհանուր զոհաբանական կանխարգելման արդի խնդիրները Հայաստանի Հանրապետությունում // Դատական իշխանություն, ապրիլ-հունիս 2024, 4-6 (298-300), էջեր 41-48:
8. Իսրայելյան Գ. Վ., Հարությունյան Ա. Ս., Լատենտային հանցավորության կանխարգելման արդի խնդիրները Հայաստանի Հանրապետությունում: Մենագրություն / Գ.Վ. Իսրայելյան, Ա.Ս. Հարությունյան. – Եր.: Հեղ. հրատ., 2021. – 88 էջ:

ПРОЯВЛЕНИЯ КИБЕРПРЕСТУПНОСТИ И МЕРЫ ПРОТИВОДЕЙСТВИЯ ИМ В РЕСПУБЛИКЕ АРМЕНИЯ

Израелян Г.В., Гукасян А.П.

В статье речь идет о развитии в последние десятилетия телекоммуникационных и информационных технологий, а также цифровизации услуг предоставляемых населению. В сложившейся на текущий момент ситуации, в том числе проникновении искусственного интеллекта в повседневную жизнь, в Республике Армения наметилась устойчивая тенденция роста киберпреступности. Данное обстоятельство свидетельствует о необходимости активизации превентивных мер воздействия, с целью минимизации возможных рисков связанных с преступной активностью в виртуальном пространстве. Авторы приходят к выводу, что данная проблема мало изучена и требует дальнейших исследований. С целью представления предложений в данном направлении авторами было проведено исследование криминологических аспектов киберпреступности в Республике Армения. В частности, выявлены состояние, динамика и факторы латентности киберпреступности в период 2019–2024 гг., а

также описаны типичные способы совершения одного из наиболее распространённых видов киберпреступлений-компьютерных хищений. В данной статье предпринята попытка раскрыть основные причины развития киберпреступности в Республике Армения. На основе анализа результатов проведённого исследования авторы предлагают меры противодействия преступлениям в сфере информационных технологий.

Ключевые слова: *киберпреступность, компьютерное хищение, типичный способ, меры противодействия.*

MANIFESTATIONS OF CYBERCRIME AND MEANS OF COMBATING THEM IN THE REPUBLIC OF ARMENIA

Israelyan G., Ghukasyan A.

The rapid development of telecommunications and information technologies, the digitalization of services provided to the population, and the penetration of artificial intelligence into everyday life in Armenia in recent years have led to a continuous increase in cybercrime. This speaks of the need to activate preventive action.In order to present recommendations in this direction, the authors conducted a study of the criminological components of cybercrime. In particular, the following trends were identified for 2019-2024: The factors determining the state, trend, and latency of cybercrime are described, and typical methods of committing computer theft, the most common type of crime included in cybercrime, are described. Based on the analysis of the results of the conducted research, the authors propose countermeasures against cybercrime.

Keywords: *cybercrime, computer theft, typical method, countermeasures.*

Ներկայացվել է խմբագրության 14.01.2025
Ընդունվել է տպագրութան 15.04.2025