ԱՆԱՀԻՏ ԲԱԲԱԽԱՆՅԱՆ
ԵՊՀ իրավագիտության ֆակուլտետի «Քրեական
արդարադատություն և փաստաբանություն»
մագիստրոսական ծրագրի ուսանող,
ՀՀ գլխավոր դատախազի օգնական

ՔՐԵԱԿԱՆ ՊԱՏԱՍԽԱՆԱՏՎՈՒԹՅՈՒՆԸ ՀԱՄԱԿԱՐԳՉԱՅԻՆ ՍԱԲՈՏԱԺԻ (ՆԵՆԳԱԴՈՒԼԻ) ՀԱՄԱՐ

Համակարգչում, համակարգչային համակարգում, համակարգչային ցանցում կամ համակարգչային այլ սարքավորման վրա կատարվող հանցագործությունները դուրս են եկել յուրաքանչյուր երկրի սահմաններից ու վերածվել վերազգային հիմնախնդրի, որի հաղթահարման միակ եղանակը բոլոր պետությունների կողմից դրա արգելմանն ուղղված միջոցառումների և խիստ վերահսկողական մեխանիզմների իրագործումն է:

Սույն հոդվածում կատարվել է ՀՀ քրեական օրենսգրքի «Համակարգչային սաբոտաժը (նենգադուլը)» վերտառությամբ հոդվածով նախատեսված հանցակազմի հետազոտություն:

Հոդվածում ուսումնասիրվել և վերլուծվել են քննարկվող հանցակազմի քրեաիրավական բնութագիրը, հանցակազմի տարրերը, վեր են հանվել խնդրահարույց այնպիսի կարգավորումներ, որոնք գործնականում արարքի քրեաիրավական որակման կապակցությամբ կարող են առաջացնել որոշակի խոչընդոտներ: Կատարված վերլուծության արդյունքում սույն ոլորտում քրեական օրենսդրության կատարելագործման նպատակով ներկայացվել են օրենսդրական առաջարկներ:

Հիմնաբառեր *– «Կիբեռհանցագործությունների մասին» Բուդապեշտի կոնվենցիա, համակարգչային սաբոտաժ, համակարգիչ, համակարգչային համակարգ, համակարգչային ցանց:*

ՆԵՐԱԾՈՒԹՅՈՒՆ

Տեղեկատվական տեխնոլոգիաների դերը ժամանակակից հասարակական հարաբերությունների համակարգում դարձել է հիմնարար. այն ոչ միայն փոխում է տնտեսության և սոցիալական փոխգործակցության ձևաչափերը, այլև վերածնում պետության կառավարման և անվտանգության ինստիտուտները, ստեղծում նախադրյալներ դրական առումով աննախադեպ տնտեսական և սոցիալական փոփոխությունների համար: Այդ զարգացումները, այնումենայնիվ, իրենց հետ առաջ են բերում նաև նոր խնդիրներ՝ նոր մարտահրավերների առջև կանգնեցնելով թե՛ միջազգային հանրությանը, և թե՛ ներպետական իրավաստեղծ և իրավակիրառ գործունեություն իրականացնող մարմիններին: Ի թիվս այլնի, այդպիսի լրջագույն խնդիր է տեղեկատվական տեխնոլոգիաների կիրառմամբ կատարվող նոր հանցատեսակների տարածումը:

Այս փոփոխությունները հանգեցնում են այնպիսի իրավիճակի, երբ հանցավոր վարքագծի ավանդական սահմանները աստիճանաբար զիջում են իրենց տեղը թվային հարթությունում դրսևորվող հակաիրավական գործողություններին:

Գլոբալացման գործընթացները, այդ թվում՝ տեղեկատվական տեխնոլոգիաների գլոբալացումը, անսահմանափակ հնարավորություններ են ընձեռում անհատների և հասարակության վրա ազդելու համար: Տեղեկատվական տեխնոլոգիաների զարգացման բացասական հետևանքներից մեկը հանցագործության նոր ձևի՝ կիբեռհանցագործության ի հայտ գալն էր ու զարգացումը, երբ համակարգչային համակարգերը կամ համակարգչային ցանցերը հանդես են գալիս որպես հանցավոր հարձակումների օբյեկտ, ինչպես նաև հանցագործություններ կատարելու միջոց կամ մեթոդ[1]:

Այսօր համակարգչային տեղեկատվության և տեխնոլոգիաների անվտանգության ապահովման խնդիրը, այդ թվում՝ քրեաիրավական միջոցներով, աշխարհի զարգացած երկրների մեծ մասում համարվում է ամենախնդրահարույցներից մեկը: Գլոբալ ինտերնետ ցանցը, որը սկզբնապես ուներ ակադեմիական բնույթ, վերածվել է առևտրային միջավայրի, որտեղ առաջնահերթ նշանակություն է ձեռք բերում անվտանգության ապահովումն ու ձևավորվող հարաբերությունների նկատմամբ հնարավոր ոտնձգությունների կանխումը[2]:

Վիրտուալ տարածքում գործող հանցագործների զոհ կարող են դառնալ ոչ միայն ֆիզիկական անձինք, այլև պետություններ: Internet Complaint Center (IC3) կայքը, որը ստեղծվել է 2000 թվականի մայիսին՝ համացանցի օգտատերերի դիմումները գրանցելու նպատակով, դեռևս 2007 թվականի հունիսի 11-ին ստանում էր բազմաթիվ բողոքներ կիբեռհանցագործությունների վերաբերյալ[3]:

Վերջին երկու տասնամյակների ընթացքում քաղաքականության, տնտեսագիտության, գիտու-

թյան, տեխնոլոգիայի և բազմաթիվ այլ ոլորտներում տեղի ունեցած գործընթացները դարձել են ամբողջովին նոր երևույթների ի հայտ գալու հիմնական որոշիչը: Այդպիսի երևույթներից մեկը արագ զարգացող համակարգչային տեխնոլոգիաներն են: Սակայն, ինչպես հայտնի է, յուրաքանչյուր մետաղադրամ ունի իր մութ կողմը, և այս դեպքում այդ մութ կողմը համակարգչային հանցագործությունն էր:

Համակարգչային հանցագործության դեմ պայքարի համար մշակվող մեթոդները հետ են մնում հանցավոր գործունեության մասշտաբներից, ինչը դրանք դարձնում է բարձր լատենտային[4]:

Համակարգչային համակարգի և համակարգչային տվյալների անվտանգության դեմ ուղղված հանցագործությունների վտանգը մեծանում է, երբ հանցագործները ներթափանցում են կարևոր ենթակառուցվածքների, պաշտպանության և մի շարք այլ էական նշանակություն ունեցող օբյեկտների համակարգչային համակարգեր:

Համակարգչում, համակարգչային համակարգում, համակարգչային ցանցում կամ համակարգչային այլ սարքավորման վրա կատարվող հանցագործությունների առանձնահատկություններից բխում է, որ այն դուրս է եկել յուրաքանչյուր երկրի սահմաններից ու վերածվել վերազգային հիմնախնդրի, որի հաղթահարման միակ եղանակը բոլոր պետությունների կողմից դրա արգելմանն ուղղված միջոցառումների և խիստ վերահսկողական մեխանիզմների իրագործումն է:

Հայաստանի Հանրապետությունը 2001 թվականի նոյեմբերի 23-ին Բուդապեշտում ստորագրել և 2006 թվականի մարտի 21-ին վավերացրել է «Կիբեռհանցագործությունների մասին» կոնվենցիան (այսուհետ՝ Բուդապեշտի կոնվենցիա)5, որը կիբեռհանցավորության դեմ պայքարի նյութաիրավական և դատավարական հիմքերի ձևավորման տեսանկյունից հիմնարար նշանակություն ունեցող միջազգային իրավական փաստաթուղթ է:

Բուդապեշտի կոնվենցիայի՝ Եվրոպայի խորհրդի նախարարների կոմիտեի մշակած բացատրական զեկույցի համաձայն՝ այս կոնվենցիայի նպատակներն են՝

1) կիբեռհանցագործություններին առնչվող ներպետական քրեական օրենսդրության ներդաշնակեցումը.

2) կիբեռհանցագործությունների կամ համակարգչային համակարգերի օգնությամբ կատարվող հանցանքների քննության կամ էլեկտրոնային տեսքով ապացույցների ձեռքբերման համար անհրաժեշտ դատավարական գործիքակազմի ապահովումը.

3) միջազգային համագործակցության արագ և արդյունավետ ռեժիմի ձևավորումը[6]:

Հայաստանի Հանրապետության նախագահի՝ 2011 թվականի դեկտեմբերի 29-ին ընդունված՝ «Հայաստանի Հանրապետությունում կազմակերպված հանցավորության դեմ պայքարի արդյունավետության բարձրացման ազգային ծրագիրը հաստատելու մասին» կարգադրության համաձայն՝ *«Կիբեռանվտանգության հզորացումը և կիբեռհանցագործությունների դեմ պայքարը ՀՀ համար ռազմավարական նշանակության խնդիրներ են: Կիբեռհանցագործությունները նոր երևույթ չեն: Դրանց կատարման մեխանիզմները մշտապես փոփոխվում և կատարելագործվում են: Գաղտնիք չէ, որ հանցագործներին հաջողվում է ոչ միայն օգտվել կիբեռտեխնոլոգիական նորույթներից, այլև մշակել և ներդնել դրանք՝ հետապնդելով ինչպես համակարգչային ցանցի օգնությամբ կամ դրա դեմ հանցանք կատարելու, այնպես էլ հանցագործության հետքերը թաքցնելու նպատակ»*[7]:

Կիբեռհանցագործությունների զարգացման տեմպերը մշտապես արդիական են դարձնում դրանց հակազդելու համար անհրաժեշտ օրենսդրական դաշտի ձևավորման խնդիրը, քանի որ միայն մեկ ծրագրային ներթափանցմամբ հնարավոր է կաթվածահար անել պետական կառավարման համակարգերը, ֆինանսական շուկաները կամ կենսական նշանակություն ունեցող ենթակառուցվածքները, ինչն առաջացնում է սպառնալիք ոչ միայն առանձին սուբյեկտների իրավունքների, այլև ամբողջ ազգային անվտանգության համար:

ԹԵ՛ ՀՀ 2003 թվականին ընդունված քրեական օրենսգրքով, և ՀՀ թե՛ 2021 թվականին ընդունված քրեական օրենսգրքով ամրագրվել են համապատասխանաբար «Համակարգչային տեղեկատվության անվտանգության դեմ ուղղված հանցագործությունները» և «Համակարգչային համակարգի և համակարգչային տվյալների անվտանգության դեմ ուղղված հանցագործությունները» վերտառությամբ գլուխները և քրեորեն հետապնդելի արարքները:

Համակարգչային համակարգի և համակարգչային տվյալների անվտանգության դեմ ուղղված քրեորեն հետապնդելի արարքներից է համակարգչային սաբոտաժը (նենգադուլը), որի արդիականությունը պայմանավորված է այն հանգամանքով, որ տեղեկատվական միջավայրը դարձել է նոր իրավական տարածք՝ դժվար վերահսկելի, հաճախ անսահմանելի իրավազորությամբ: Այդ տարածքում իրավական պաշտպանության ավանդական մեխանիզմները կորցնում են իրենց արդյունավետությունը: Արդյունքում առաջանում է իրավակարգավորման և տեխնոլոգիական դինամիկայի միջև բաց՝ իրավական վակուում, որն իր հերթին նպաստում է նման հանցագործությունների արագ տարածմանը:

Բացի այդ, կիբեռհանցագործությունները վերածվում են ոչ միայն տնտեսական շահի գործիքի,

այլև ազդեցիկ մեխանիզմի՝ սպառնալիք ստեղծելով պետությունների ինքնիշխանությանը, տեղեկատվական անկախությանը և հասարակական կայունությանը: Հետևաբար, համակարգչային սաբոտաժի՝ որպես համակարգչային համակարգի և համակարգչային տվյալների անվտանգության դեմ ուղղված քրեորեն հետապնդելի արարքի, ուսումնասիրությունը արդիական է ոչ միայն այն պատճառով, որ այն իրենից ենթադրում է թվային դարաշրջանի նորագույն հանցատեսակ, այլև որովհետև այն մարտահրավեր է նետում քրեական իրավունքի ավանդական սկզբունքներին՝ ստիպելով վերանայել իրավական պատասխանատվության ծավալն ու բովանդակությունը՝ տեխնոլոգիական առաջընթացի և տեղեկատվական միջավայրի փոփոխության համատեքստում:

ՀԵՏԱԶՈՏՈՒԹՅՈՒՆ

2021 թվականի մայիսի 5-ին ընդունված ՀՀ քրեական օրենսգիրքը[8] (այսուհետ՝ ՀՀ ՔՕ), ինչպես նշվեց, 361-րդ հոդվածի ուժով քրեական պատասխանատվություն է նախատեսում, ի թիվս այլնի, համակարգչային սաբոտաժի (նենգադուլի) համար, որպիսին է դիտարկվում համակարգչում, համակարգչային համակարգում, համակարգչային ցանցում կամ համակարգչային այլ սարքավորման վրա պահվող տվյալն առանց օրենքով կամ պայմանագրով կամ իրավաչափ այլ հիմքով նախատեսված թույլտվության ոչնչացնելը, վնասելը, աղավաղելը կամ ուղեփակելը (մեկուսացնելը):

Նախքան հանցակազմի տարրերին անդրադառնալը, բացահայտենք տվյալ հանցագործության դրսևորման համար կարևոր նշանակություն ունեցող մի շարք հասկացություններ, որպիսիք են՝ համակարգիչը, համակարգչային համակարգը, համակարգչային ցանցը և համակարգչային այլ սարքավորումը:

Այսպես, համակարգիչը ծրագրավորվող էլեկտրոնային սարք է, որը կարող է մշակել տվյալներ և կատարել հաշվարկներ[9]: «Համակարգիչ» է համարվում այն սարքը կամ սարքերի համակցությունը (ներառյալ օժանդակ սարքերը, պերիֆերիկ սարքավորումները կամ ենթակառուցվածքները), ինչպես նաև դրան միացված հաղորդակցման համակարգերը, որոնք կարող են իրականացնել տարբեր գործառույթներ, այդ թվում՝ (բայց դրանցով չսահմանափակվելով) բարդ հաշվարկային, թվաբանական կամ տրամաբանական գործողություններ, տեղեկատվության պահպանման կամ որոնման գործողություններ: Համակարգիչը պետք է կարողանա աշխատել արտաքին ֆայլերի հետ, գործարկել մեկ կամ մի քանի գործողություններ, որոնք պարունակում են համակարգչային ծրագրեր կամ էլեկտրոնային հրահանգներ, ապահովել տվյալների մուտքագրում և ելքագրում: Նման գործողությունները կամ հաղորդակցությունները կարող են իրականացվել ինչպես մարդու միջամտությամբ, այնպես էլ առանց դրա՝ տվյալ խնդրի մշակման ընթացքում[10]:

Վերոգրյալից բխում է, որ համակարգիչը էլեկտրոնային այն սարքն է, որը նախատեսված է տվյալների ընդունման, մշակման, պահպանման համար: Այն իրենից ներկայացնում է ֆիզիկական բաղադրիչների՝ պրոցեսոր, հիշողություն, մուտքային/ելքային սարքեր և այլն և ծրագրային ապահովման միասնություն, որը հնարավորություն է տալիս իրականացնել հաշվարկային և տեղեկատվական գործողություններ:

Բուդապեշտի կոնվենցիայի 1-ին հոդվածի «ա» պարբերության համաձայն՝ *համակարգչային համակարգը նշանակում է՝ ցանկացած սարք կամ փոխկապակցվող կամ կապակցվող սարքերի խումբ, որոնցից մեկը կամ մի քանիսը, ծրագրի համաձայն, կատարում են տվյալների ավտոմատ մշակում*:

Բուդապեշտի կոնվենցիայի բացատրական զեկույցի[11] համաձայն՝ «համակարգչային համակարգը» սարք է, որը բաղկացած է ապարատային և ծրագրային ապահովումից և նախատեսված է թվային տվյալների ավտոմատ մշակման համար: Այն կարող է ներառել նաև մուտքային, ելքային և պահպանման միջոցներ: Ընդ որում, համակարգչային համակարգի համար կարևոր չափանիշ է այդ սարքի կողմից տվյալների ավտոմատ մշակման իրականացումը, որը, զեկույցի համաձայն, իրենից ենթադրում է առանց մարդու անմիջական միջամտության կատարվող գործողություն:

Այս կապակցությամբ հետաքրքրական է այն հարցի պարզաբանումը, թե որ հասկացության ներքո պետք է դիտարկել այն իրավիճակը, երբ տվյալների ավտոմատ մշակումն իրականացվի մեկ եզակի սարքի կողմից:

Այսպես, Բուդապեշտի կոնվենցիայի տեսանկյունից որպես համակարգչային համակարգ կարող է դիտարկվել, ինչպես մեկ, այնպես էլ մի քանի սարքերի խումբ, որոնցից մեկի կամ մի քանիսի կողմից իրականացվում է տվյալների մշակում: Համակարգչային համակարգի առանձնահատկությունը, ինչպես և համակարգչի, ի թիվս այլնի, տվյալների մշակումն է, սակայն համակարգչային համակարգի դեպքում այն իրականացվում է բացառապես ավտոմատ եղանակով:

Վերոգրյալից ակնհայտ է, որ քննարկվող իրավիճակի առկայությունը գործնականում կարող է որոշակի դժվարություններ առաջացնել այդ սարքը որպես համակարգիչ կամ համակարգչային համակարգ դիտարկելու տեսանկյունից: Սակայն, հաշվի առնելով այն, որ Բուդապեշտի կոնվենցիայի տեսանկյունից համակարգչային համակարգը կարող է բաղկացած լինել նաև մեկ սարքից, որի առանձ-

նահատկությունը տվյալների ավտոմատ մշակումն է՝ կարծում ենք, որ յուրաքանչյուր դեպքում, երբ մեկ սարքավորման կողմից տվյալների մշակումն իրականացվի ավտոմատ կերպով, այն պետք է դիտարկվի ոչ թե որպես համակարգիչ, այլ համակարգչային համակարգ:

Միաժամանակ, կարևոր է նշել, որ օտարերկրյա պետությունների օրենսդրություններում այսպիսի իրավիճակների կարգավորման համար մշակված մոտեցումներն ավելի պարզ և նպատակահարմար են: Մասնավորապես, ԱՄՆ Թենեսի նահանգի քրեական օրենսգրքով համակարգչային համակարգը դիտարկվում է որպես միացված սարքերի ամբողջություն, որոնք թույլ են տալիս համակարգին կատարել տվյալների մշակման առաջադրանքներ[12]: Այսինքն, որպես համակարգչային համակարգ դիտակվում է բացառապես այդպիսի սարքավորումների խումբը, որպիսի մոտեցումը առավել նպատակահարմար է և գործնականում կբացառի վերը ներկայացված իրավիճակներում հնարավոր տարընկալումները:

Անդրադառնանք համակարգչային ցանցի հասկացությանը: Այն փոխկապակցված համակարգիչների և ծայրամասային սարքերի մի խումբ է, որը թույլ է տալիս օգտատերերին փոխանակել տվյալներ և համագործակցել ցանցի ներսում: Ցանցի հիմնական նպատակն է թույլ տալ օգտատերերին հեշտությամբ մուտք գործել և կիսվել դրանում պարունակվող տեղեկատվությամբ, մասնավորապես՝ սահմանափակել չարտոնված անձանց մուտքը[13]:

Այսինքն, կարելի է եզրակացնել, որ համակարգչային ցանցերի հիմնական գործառույթը ֆայլերի և տվյալների փոխանակումն է, սարքավորումների համատեղ օգտագործումը, ինչպիսիք են տպիչները և սերվերները, ինտերնետին և առցանց ռեսուրսներին մուտք գործելու հնարավորությունը և սարքերի հեռակառավարումը:

Վերոշարադրյալի հիման վրա կարող ենք արձանագրել, որ ի տարբերություն համակարգչային ցանցի, որը տարբեր համակարգիչների և սարքերի միավորում է, որոնք միմյանց հետ կապված են հաղորդակցման միջոցներով՝ բացառապես տեղեկատվություն փոխանակելու և կապի ահահովման համար, համակարգչային համակարգը մեկ ամբողջական միասնական համալիր է, որն իր մեջ ներառում է մեկ կամ մի քանի համակարգիչ, դրանց ծրագրային ապահովումը և իրականացնում է որոշակի գործառույթներ, մասնավորապես՝ տվյալների ավտոմատ մշակում:

Ինչ վերաբերում է համակարգչային այլ սարքավորմանը, որը հաճախ անվանվում է նաև պերիֆիրկ սարքեր, ապա դրանք այնպիսի սարքեր են, որոնք միանում են համակարգչին և ապահովում նրա աշխատանքի ընդլայնումը կամ արտաքին աշխարհի հետ փոխազդեցությունը: Դրանք չեն համարվում համակարգչի հիմնական բաղադրիչներ (ինչպիսիք են պրոցեսորը, հիշողությունը և այլն), բայց առանց դրանց համակարգչի լիարժեք օգտագործումը դժվարանում է, քանի որ այդ սարքերի միջոցով ապահովվում է մի շարք գործողությունների իրականացումը, ինչպիսիք են՝ տվյալների մուտքագրումը (ստեղնաշարեր, մկնիկներ), տեղեկատվության ելքագրումը (մոնիտորներ, տպիչներ), տվյալների պահպանումը(արտաքին կոշտ սկավառակներ)[14]:

Ակնհայտ է, որ համակարգչային սաբոտաժը միջազգայնորեն ճանաչված հիմնախնդիրներից մեկն է, որը խաթարում է տեղեկատվական անվտանգության համակարգը, վտանգում պետական ու հասարակական կառույցների կայունությունը, անմիջական սպառնալիք հանդիսանում ոչ միայն տնտեսական, այլև ազգային անվտանգության համար:

Յուրաքանչյուր հանցակազմ, որն ամրագրված է ՀՀ ՔՕ-ում, իրենից ներկայացնում է որոշակի օբյեկտի դեմ ոտնձգող և դրան վնաս պատճառելու գործողությամբ կամ դրա սպառնալիքով դրսևորվող հանրորեն վտանգավոր արարք: Մեծ նշանակություն ունի նաև, թե որ հանցագործությունների շարքում է այն ներկայացվում, քանի որ նշվածը և հանցակազմի բովանդակությունը մեծապես պայմանավորում են օբյեկտի առկայությունը: Հարկ է նշել, որ այս հանցակազմը ՀՀ ՔՕ-ում ամրագրված է «Համակարգչային համակարգի և համակարգչային տվյալների անվտանգության դեմ ուղղված հանցագործությունների շարքում:

Համակարգչային սաբոտաժը, որն իր մեջ ներառում է համակարգչում, համակարգչային համակարգում, համակարգչային ցանցում կամ համակարգչային այլ սարքավորման վրա պահվող տվյալն առանց օրենքով կամ պայմանագրով կամ իրավաչափ այլ հիմքով նախատեսված թույլտվության ոչնչացնելը, վնասելը, աղավաղելը կամ ուղեփակելը (մեկուսացնելը), կարելի է բնորոշել որպես «ստվերային գործընթաց», որն առաջանում է և զարգանում անպատժելիության պայմաններում: Այն լուրջ վտանգ է ներկայացնում տեղեկատվական անվտանգության, տնտեսության, պետական կառավարման և անհատի իրավունքների համար:

Մեր կարծիքով, այս երևույթի դրսևորումը խաթարում է համակարգերի գործառնական ամբողջականությունը, քանի որ նման հարձակումների ընթացքում խափանվում է տեղեկատվական ենթակառուցվածքների բնականոն գործունեությունը, որն էլ կարող է պատճառ հանդիսանալ տեղեկատվական անվտանգության համակարգի, ազգային անվտանգության և հասարակական կարգի ապակայունացման: Տվյալների ոչնչացումը, փոփոխությունը, ուղեփակումը և հանցակազմի օբյեկտիվ

կողմի այլ դրսևորումների իրականացումը ոչ միայն տեխնիկական վնաս են պատճառում, այլև խախտում են համակարգչային համակարգում, համակարգչային ցանցում և համակարգչային այլ սարքավորման վրա պահվող տվյալների պաշտպանության նկատմամբ ձևավորված հասարակական և իրավական հարաբերությունները: Բացի այդ, կարևոր է նշել, որ քննարկվող հանցագործությունը կարող է մեծապես ուղղված լինել նաև թվային տեղեկության գաղտնիության խաթարմանը՝ բացահայտելով անձնական, ծառայողական կամ օրենքով պահպանվող գաղտնիք համարվող տվյալներ:

Վերոգրյալի հաշվառմամբ կարող ենք արձանագրել, որ համակարգչային տեղեկատվության ոլորտում հանցագործությունները բազմօբյեկտ հանցագործություններ են. անմիջական օբյեկտը հանդիսանում է տեղեկատվական անվտանգության համակարգը՝ իր ամբողջության մեջ: Այսինքն՝ այն հարաբերությունները, որոնք ապահովում են համակարգչային տեղեկատվության գաղտնիությունը, ամբողջականությունը և հասանելիությունը: Հիմնական անմիջական օբյեկտի՝ համակարգչային համակարգի և համակարգչային տվյալների անվտանգության հետ մեկտեղ առանձնացվում են լրացուցիչ անմիջական օբյեկտներ.

- հասարակական հարաբերություններ, որոնք ապահովում են անձանց օրինական իրավունքներն ու օրինական շահերը.
- հասարակական հարաբերություններ, որոնք ապահովում են պետական ծառայության օրինական շահերը[15]:

Անդրադառնանք հանցակազմի առարկային, որը հասարակական հարաբերության այն տարրն է, որի վրա ներգործելով, որը ոչնչացնելով կամ վնասելով խախտվում, վնասվում է հանցագործության օբյեկտ հանդիսացող հասարակական հարաբերությունը:

Մասնագիտական գրականությամբ բազմիցս քննարկման առարկա է դարձել քննարկվող հանցագործության առարկայի վերաբերյալ հիմնահարցը: Գիտնականների մի մասը այն մոտեցման կողմնակիցներն են, որ տվյալ հանցագործության առարկա պետք է դիտարկել համակարգչային տվյալը կամ տեղեկատվությունը[16]: Այլ մոտեցման համաձայն՝ «համակարգչային սաբոտաժը» հանցագործության առարկան տեղեկատվական միջավայրն է, այսինքն՝ տեղեկատվության ստեղծման, վերափոխման և սպառման հետ կապված սուբյեկտների գործունեությունը[17]:

Հատկանշական է, որ ՀՀ ՔՕ 361-րդ հոդվածի դիսպոզիցիայում հստակ սահմանվում է, որ հանցակազմի օբյեկտիվ կողմ դիտակվող գործողությունները կատարվում են համակարգչում, համակարգչային համակարգում, համակարգչային ցանցում կամ համակարգչային այլ սարքավորման վրա պահվող տվյալի նկատմամբ: Հետևաբար, պետք է համաձայնել այն տեսաբանների մոտեցմանը, որ ,համակարգչային սաբոտաժե հանցագործության առարկան համակարգչային տվյալն է:

Բուդապեշտի կոնվենցիայի 1-ին հոդվածի «բ» պարբերության համաձայն՝ *«համակարգչային տվյալներ» նշանակում է՝ փաստերի, տեղեկատվության կամ հասկացության հավաքումը այն ձևով, որը հարմար է համակարգչային համակարգերում մշակման համար, ներառյալ այն ծրագրերը, որոնք ապահովում են համակարգչային համակարգի գործառույթների իրականացումը:*

Վերոգրյալ կարգավորումից կարելի է եզրակացնել, որ համակարգչային տվյալի ներքո կարող է դիտարկվել ցանկացած տվյալ, տեղեկություն, անգամ ծրագիր, որոնք մշակվում, պահվում կամ փոխանցվում են համակարգչային համակարգի, ցանցի կամ այլ սարքավորման միջոցով: Այսինքն, համակարգչային տվյալը իրենից ենթադրում է ցանկացած թվային տեղեկություն, որը գոյություն ունի համակարգչային միջավայրում և ենթակա է մշակման:

ՀՀ ՔՕ-ն որպես հանցագործության օբյեկտիվ կողմի դրսևորումներ նախատեսում է հանցագործության առարկան առանց օրենքով կամ պայմանագրով կամ իրավաչափ այլ հիմքով նախատեսված թույլտվության ոչնչացնելը, վնասելը, աղավաղելը կամ ուղեփակելը (մեկուսացնելը): Նկարագրված հանցակազմը ձևական է, այսինքն, նախատեսված չեն օբյեկտիվ կողմի հատկանիշ հանդիսացող այնպիսի հետևանքներ, որոնց առաջացումը կվկայեր հանցագործության ավարտի մասին, ուստի օբյեկտիվ կողմի դրսևորումն արդեն իսկ վկայում է օրենսդրությամբ պաշտպանվող հասարակական հարաբերությունների դեմ ուղղված սպառնալիքի մասին: Օբյեկտիվ կողմի դրսևորման համար կարևոր է ապօրինության չափանիշը, որը վերաբերում է օբյեկտիվ կողմի բոլոր դրսևորումներին: Մասնավորապես, որպեսզի վերը թվարկված գործողություններից որևէ մեկի կատարումը հանգեցնի քրեական պատասխանատվության, անհրաժեշտ է, որ այն կատարված լինի առանց օրենքով կամ պայմանագրով կամ իրավաչափ այլ հիմքով նախատեսված թույլտվության: Ստացվում է, բոլոր այն դեպքերում, երբ անձը կատարում է գործողություն, որի համար չունի ոչ մի իրավական հիմք՝ ոչ օրենքի, ոչ կնքված պայմանագրի, ոչ էլ որևէ այլ օրինական լիազորության տեսքով (օրինակ՝ իրավասու մարմնի թույլտվություն), կատարված գործողությունը համարվում է հակաիրավական և հանգեցնում քրեական պատասխանատվության:

Անդրադառնանք ՀՀ ՔՕ 361-րդ հոդվածով ամրագրված հանցակազմի օբյեկտիվ կողմի դրսևորումներին: Այսպես, համակարգչային տվյա-

լը «ոչնչացնելը» օբյեկտիվ կողմի դրսևորումը մեր կարծիքով, տեղեկատվության սեփականատիրոջը կամ այն տիրապետողին ամենաէական և ամենամեծ վնաս հասցնող գործողություններից մեկն է:

Որոշ գիտնականներ կարծում են, որ համակարգչային տեղեկատվության ոչնչացումը պետք է հասկանալ որպես դրա լիակատար ֆիզիկական վերացում[18], մյուսները՝ «տեղեկատվության լրիվ կամ մասնակի ջնջում մեքենայական ընթերցվող կրիչից»[19]: Այլ տեսաբանների կարծիքով համակարգչային տեղեկատվության ոչնչացումը դիտարկվում է որպես այդպիսի տվյալների հեռացում համակարգչային հիշողությունից կամ էլեկտրոնային կրիչից, երբ դրան հետագայում հասանելիություն ստանալը անհնար է՝ անկախ դրանց վերականգնման հնարավորությունից[20]:

Մեր կարծիքով համակարգչային տվյալի ոչնչացումը պետք է մեկնաբանել որպես ցանկացած գործողություն՝ ուղղված այդպիսի տվյալը ամբողջությամբ կամ մասամբ համակարգչի հիշողությունից, էլեկտրոնային կրիչից կամ այլ ցանցային միջավայրից վերացնելուն, որի հետևանքով դրանք դառնում են անվերականգնելի և օգտագործման համար ոչ պիտանի: Այսինքն, հանցակազմի՝ «ոչնչացնելը» օբյեկտիվ կողմի դրսևորման պարագայում գործ ունենք համակարգչային տվյալի գոյության կորստի հետ:

Այս կապակցությամբ հատկանշական է, որ մասնագիտական գրականությամբ բազմիցս քննարկման առարկա է դարձել այն հիմնահարցը՝ արդյոք ոչնչացված համակարգչային տվյալի վերականգնման դեպքում այդ գործողությունը պետք է որակել որպես ավարտված հանցագործություն, թե հանցագործության փորձ[21]: Մեր կարծիքով, քանի որ քննարկվող հանցակազմը ձևական է և հանցագործության ավարտը կապվում է արարքի կատարման պահով, սույն դեպքում համակարգչային տվյալի ոչնչացման փաստը, անկախ դրա հետագայում վերականգնվելու հանգամանքից, ինքնին վկայում է ավարտված հանցագործության մասին: Այսինքն, համակարգչային տվյալը հետագայում վերականգնելու փաստը ուղղակիորեն չի կարող հանգեցնել հանցավորի կողմից արդեն իսկ կատարված գործողության, այն է՝ «ոչնչացնելու» փաստի վերացման:

Համակարգչային տվյալը ուղեփակելը (մեկուսացնելը) որպես հանցակազմի օբյեկտիվ կողմի դրսևորում քննարկելիս, կարևոր է նշել, որ մասնագիտական գրականությունը այս գործողության վերաբերյալ դիտարկել է տարբեր սահմանումներ, սակայն տեսաբանների մեծամասնության կարծիքով այդպիսին պետք է դիտարկել համակարգչային տվյալը իր նպատակային նշանակությամբ ստանալու կամ օգտագործելու անհնարինության իրավիճակը՝ այդպիսի տվյալի ամբողջական պահպանված լինելու վիճակում[22]:

Մեր կարծիքով, համակարգչային տվյալի ուղեփակումը (մեկուսացումը) համակարգչի կամ համակարգչային համակարգի, ցանցի կամ այլ սարքավորման վրա ազդեցություն է, որը հանգեցնում է համապատասխան տվյալը տիրապետողի, դրան հասանելիություն ունեցող անձի՝ համակարգչային տվյալի հետ օրինական գործողություններ կատարելու կարողության ժամանակավոր կամ մշտական դադարեցման, սակայն, որի պարագայում այդ տվյալը չի ոչնչանում կամ վնասվում, այլ վերանում է դրան հասանելիություն ստանալու հնարավորությունը: Երբ համակարգչային տվյալը ժամանակավորապես ուղեփակվում է, դրան ի սկզբանե հասանելիություն ունեցող անձը այլևս չի կարողանում որևէ գործողություն կատարել դրա հետ, իսկ մշտապես ուղեփակվելու պարագայում, օրինակ, երբ հանցագործը բարդ և անընդհատ փոփոխվող մուտքի կոդ է սահմանում այդ տվյալ մուտք գործելու համար կամ այն տեղափոխում մեկ այլ սերվեր և այլն, տվյալին հասանելիությունը կարող է ընդհանրապես վերանալ:

Անդրադառնանք օբյեկտիվ կողմի հաջորդ դրսևորմանը՝ համակարգչային տվյալը վնասելուն: Օբյեկտիվ կողմի այս դրսևորման նախատեսումը որոշակի դժվարություններ է առաջացնում կատարված հանրորեն վտանգավոր արարքի քրեաիրավական որակման շրջանակներում, քանի որ այս օբյեկտիվ կողմին զուգահեռ, ՀՀ ՔՕ-ն քրեականացրել է նաև համակարգչային տվյալները փոփոխելը և աղավաղելը: Մասնագիտական գրականության և տարբեր երկրների օրենսդրությունների ուսումնասիրությունը վկայում են այն մասին, որ շատ հաճախ օբյեկտիվ կողմի հիշյալ դրսևորումները նույնացվում են:

Մասնավորապես, ԱՄՆ Կալիֆոռնիա նահանգի քրեական օրենսգիրքը նս քրեականացրել է համակարգչային համակարգի և համակարգչային տվյալների անվտանգությունը խաթարող մի շարք գործողություններ՝ ի թիվս այլնի, նախատեսելով, որ արարքը քրեորեն հետապնդելի է, եթե անձը գիտակցաբար և առանց թույլտվության օգտագործում է մեկ կամ մի քանի էլեկտրոնային նամակներ կամ գրառումներ ուղարկելու համար մեկ կամ մի քանի անհատի, կորպորացիայի կամ կազմակերպության ինտերնետային դոմեյնի անունը կամ պրոֆիլը և դրանով իսկ վնաս է հասցնում կամ վնաս է պատճառում համակարգչին, համակարգչային տվյալներին, համակարգչային համակարգին կամ համակարգչային ցանցին:

Հատկանշական է, որ նույն օրենսգրքով բացահայտվում է նաև վնաս հասկացությունը և այդպիսին է դիտարկվում համակարգչային համակարգի, համակարգչային ցանցի, համակարգչային

ծրագրի կամ տվյալների ցանկացած փոփոխությունը, ջնջումը, ոչնչացումը, որը պայմանավորված է համակարգչային համակարգի, ցանցի կամ ծրագրի օրինական օգտատերերի մուտքի մերժմամբ[23]:

Ակնհայտ է, որ ԱՄՆ Կալիֆոռնիա նահանգի օրենդրությամբ վնասել եզրույթը ավելի լայն է և ընդգրկում է նույնիսկ «ոչնչացնել» օբյեկտիվ կողմի դրսևորումը:

Մեծ Բրիտանիայի «Համակարգչային չարաշահման մասին» 1990 թվականի օրենքի 3-րդ հոդվածի 6-րդ մասով[24] ևս սահմանվում է, որ համակարգչի բովանդակության փոփոխությունը չի կարող համարվել որևէ համակարգչի կամ համակարգչային կրիչի վնաս, եթե դրա ազդեցությունը այդ համակարգչի կամ համակարգչային կրիչի վրա չի խաթարում դրա ֆիզիկական վիճակը:

Այսինքն, սույն կարգավորումից ստացվում է, որ Մեծ Բրիտանիայի օրենսդրությամբ ևս համակարգչային տվյալի վնասում գործողությունը մեկնաբանվում է այդպիսի տվյալների բովանդակությունը փոփոխելու միջոցով, պայմանով, որ այն հանգեցնի համակարգչի կամ սկավառակի, համակարգչային կրիչի ֆիզիկական վիճակի վրա խախտման:

ԱՄՆ-ում «Համակարգչային հանցագործությունների մասին» օրենքի համաձայն վնասը իրենից ենթադրում է տվյալների, ծրագրի, համակարգի կամ տեղեկատվության ամբողջականության կամ մատչելիության ցանկացած խախտում[25]:

Վերոգրյալից ակնհայտ է, որ համակարգչային տվյալը վնասելու գործողությունը միջազգային տիրույթում մեկնաբանվում է տվյալը փոփոխելու, ոչնչացնելու, որոշ դեպքերում նույնիսկ ուղեփակելու գործողությամբ, այդ իսկ պատճառով հանցագործությունների որակման գործընթացում հնարավոր խնդիրների բացառման նպատակով կարևոր է քննարկման առարկա դարձնել «վնասել», «աղավաղել», «փոփոխել» եզրույթների հասկացությունը:

Ինչպես արդեն իսկ նշվեց ՀՀ ՔՕ-ն առանձին հանցակազմով քրեականացրել է նաև համակարգչային տվյալը փոփոխելու գործողությունը և, ի տարբերություն, համակարգչային սաբոտաժի, քննարկվող հանցագործությունը նախատեսվել է որպես նյութական հանցակազմ, այսինքն հանցագործությունը ավարտված դիտարկելու համար պահանջվում է, որ համակարգչային տվյալը փոփոխելը վնաս պատճառի օրենքով պաշտպանվող սուբյեկտների իրավունքներին, ազատություններին և օրինական շահերին:

Նշյալից ակնհայտ է, որ ներպետական իրավական կարգավորումներով ևս վնաս հասկացությունը լայն է և ընդգրկուն, ներառում է փոփոխելու գործողությունը, քանի որ ՀՀ ՔՕ-ն որպես փոփոխելու վերջնարդյունք նախատեսել է վնասի պատճառումը:

Վերոշարադրյալից բխում է, որ միջազգային և ներպետական իրավական կարգավորումները ,վնասե և ըստ այդմ «վնասել» եզրույթները ավելի լայն են դիտարկում, այլ ոչ թե բացառապես նյութական վնասի առաջացման տեսանկյունից: Այս մոտեցումը պայմանավորված է այն հանգամանքով, որ համակարգչային տվյալները նյութական առարկաներ չեն, այլ ունեն գործառնական արժեք և դրանց հասցված ցանկացած միջամտություն, որը խաթարում է վերջիններիս ամբողջականությունը, ճշգրտությունը, կամ օգտագործելիությունը իրավական տեսանկյունից դիտվում է որպես վնաս պատճառելու ձև: Այս տրամաբանությամբ գործողությունները, ինչպիսիք են «փոփոխելը», «աղավաղելը», նույնիսկ որոշ դեպքերում «ուղեփակելը» առաջացնում են վերը ներկայացված հետևանքները և դիտարկվում որպես վնաս պատճառելու իրավական արդյունք: Այսինքն, թվարկված գործողությունների կատարումը, ինքնին, կարող է դիտարկվել «վնասել» եզրույթի ներքո:

Հետևաբար, կարծում ենք աննպատակահարմար է համակարգչային տվյալը փոփոխելը առանձին հանցակազմով նախատեսելը, և գործնականում, կատարված հանրորեն վտանգավոր արարքների քրեաիրավական որակման շրջանակներում առաջացող հնարավոր խնդիրներից խուսափելու նպատակով առաջարկում ենք կամ կատարել օրենսդրական փոփոխություն, այն է՝ նախատեսել քրեական պատասխանատվություն համակարգչային տվյալը, ի թիվս այլնի, վերացնելու համար, որի ներքո կդիտարկվեն դրանք աղավաղելու և փոփոխելու գործողությունները, կամ Օրենսգրքում օգտագործված եզրույթները մեկնաբանել հետևյալ կերպ:

Մասնագիտական գրականությունը պարունակում է համակարգչային տվյալի փոփոխություն տերմինի բազմաթիվ սահմանումներ[26], սակայն, գերակշռում են այն կարծիքները, որ այս գործողությունը իրենից ենթադրում է տվյալի բովանդակային փոփոխություն: Մենք ևս կարծում ենք, որ համակարգչային տվյալի փոփոխություն ասելով պետք է հասկանալ դրանց բովանդակային փոփոխությունները, որոնք չեն կրի տեխնիկական բնույթ:

Համակարգչային տվյալների վնասում ասելով պետք է հասկանալ միջամտություն համակարգչային տեղեկատվության նկատմամբ, դրա կառուցվածքային ամբողջականության խախտում, որի արդյունքում դրանք կորցնում են իրենց բնականոն գործառնական հատկությունները կամ դառնում են օգտագործման համար ոչ անհրաժեշտ և պիտանի, ընդ որում, առանց դրանց բովանդակության փոփոխման կամ լիակատար ոչնչացման: Այսինքն, սույն գործողության պարագայում խախտվում է այդ տվյալների կառուցվածքը կամ ամբողջակա-

նությունը, որն էլ հանգեցնում է դրանք օգտագործելու անհնարինության, օրինակ, երբ խափանվում է ֆայլի կամ տվյալների բազայի կառուցվածքը, համապատասխան ֆայլը «փչանում է» և հնարավոր չի լինում մուտք գործել այդտեղ պարունակվող տվյալ ֆայլի կառուցվածքի վնասման պատճառով, հանգեցնում է տվյալների մասնակի կորստի՝ առանց բովանդակությունը փոխելու:

Այսինքն, տվյալների վնասման դեպքում դրանց բովանդակությունը մնում է անփոփոխ, սակայն այլևս խաթարվում է դրանք ճիշտ մշակելու կամ այլ կերպ օգտագործելու համակարգչային համակարգի, ցանցի կամ այլ սարքավորման աշխատանքը:

Պատկերացնենք մի իրավիճակ, երբ հանցավորը համակարգչային տվյալի վնասման համար օգտագործի հատուկ ծրագրային կամ գործիքային միջոցներ, օրինակ՝ հատուկ ծրագրային վիրուսներ և հանցավորի կողմից դիտավորությամբ վնասվի համակարգչային տվյալը (օրինակ՝ այլևս հնարավոր չլինի բացել բանկային համակարգում հաճախորդների տվյալների բազան կամ խախտվի ֆայլի կառուցվածքը): Սույն դեպքում, արարքը կորակվի հանցագործությունների համակցությամբ, մասնավորապես ՀՀ ՔՕ 363-րդ հոդվածի 1-ին և 361-րդ հոդվածի 1-ին մասերով, քանի որ օգտագործվել էր հատուկ ծրագրային միջոց համակարգչային տվյալի վնասման համար և որպես վերջնարդյունք դիտավորությամբ այդ տվյալը վնասվել էր:

Անդրադառնանք համակարգչային տվյալը «աղավաղելու» գործողությանը: Հատկանշական է, որ բացատրական բառարանում աղավաղել բառը ներկայացվում է, ի թիվս այլնի, որպես փոփոխել: Այսինքն, այս եզրույթի համատեքստում ևս խնդիր է առաջանում հանցագործությունների որակման գործընթացում:

Մեր կարծիքով «աղավաղել» գործողության ներքո պետք է դիտարկել այնպիսի գործողությունները, որոնց հետևանքով տվյալը, թեև ձևականորեն մնում է համակարգում, այնուամենայնիվ, այլևս չի արտացոլում իրական կամ սկզբնական բովանդակությունը, այսինքն, խեղաթյուրվում է այդ տվյալի ճշգրտությունը, օրինակ, երբ մուտքագրված տվյալները խառնվում են կամ այդ տվյալի ձևաչափը փոխվում է:

Այսինքն, ի տարբերություն փոփոխելու, որի դեպքում կատարվում է տվյալի բովանդակային փոփոխություն, և ի տարբերություն վնասելու, որի դեպքում խաթարվում է դրանք ճիշտ մշակելու կամ այլ կերպ օգտագործելու համակարգչային համակարգի, ցանցի կամ այլ սարքավորման աշխատանքը և հնարավոր չի լինում մուտք գործել համակարգչային տվյալներ, աղավաղելու դեպքում համակարգչային տվյալը ձևականորեն առկա է, սակայն բովանդակային ճշգրտությունը խաթարված:

Որպես օրինակ ներկայացնենք միջազգային պրակտիկայում տեղի ունեցած մի դատական գործ: Այսպես, Գերմանիայի դաշնային դատարանը Urteil vom 10.11.1999 – 1 StR 637/98 գործի շրջանակներում արձանագրել էր, որ կորպորատիվ աշխատողը փոխել էր արտադրական ծրագրային միջավայրի պարամետրերը՝ առանց թույլտվության, ինչի հետևանքով տվյալների հաշվարկները խեղաթյուրվել էին: Այս գործողությունը դատարանը գնահատել էր որպես համակարգչային տվյալի աղավաղում և դիտարկել որպես պատճառված վնաս:

Բացի վերը շարադրված հիմնական հանցակազմերից ՀՀ ՔՕ-ն պատասխանատվություն է նախատեսում նաև միևնույն օբյեկտի դեմ ուղղված, միևնույն առարկան ունեցող և օբյեկտիվ կողմերով դրսևորվող որակյալ հանցակազմի համար: Նախքան որակյալ հանցակազմերին անդրադառնալը հանցակազմի օբյեկտիվ կողմի դրսևորումների քննարկման համատեքստում հարկ է անդրադառնալ նաև մասնագիտական գրականությամբ բազմիցս քննարկման առարկա դարձած այն հիմնահարցին՝ արդյոք համակարգչային տվյալների պատճենահանումը, օրինակ՝ համակարգչային տվյալի վերաշարադրումը, դրա կրնօրինակումը կամ փոխանցումը ցանկացած նյութական կամ էլեկտրոնային կրիչի վրա, որպես առանձին գործողություն և ոչ որպես այլ գործողության հետևանք հանգեցնում է քրեական պատասխանատվության, թե ոչ:

Համակարգչային տվյալի պատճենահանումը համակարգչային տեղեկատվության անալոգը անօրինական կերպով ստեղծելու և այն ցանկացած ֆիզիկական միջավայր փոխանցելու գործընթաց է՝ պահպանելով սկզբնական տվյալների (տեղեկատվության) բոլոր առկա պարամետրերը: Համակարգչային տվյալը կարող է գոյություն ունենալ ոչ միայն էլեկտրական ազդանշանների տեսքով, այլև մեխանիկական, թվային, օպտիկական, լազերային, քվանտային, մոլեկուլային և այլ ֆիզիկական ձևերով: Հետևաբար, համակարգչային տեղեկատվության պատճենը կարող է ունենալ բնօրինակին նույնական բովանդակություն, բայց ունենալ տարբեր ֆիզիկական ձև: Օրինակ, տեղեկատվությունը պատճենվել և փոխանցվել է ճկուն սկավառակից, կոշտ սկավառակից կամ ֆլեշ կրիչից (համակարգչային տեղեկատվություն էլեկտրական ազդանշանների տեսքով) CD կամ DVD սկավառակի (համակարգչային տեղեկատվություն օպտիկական կամ լազերային-օպտիկական ազդանշանների տեսքով): Համակարգչային տեղեկատվության ֆիզիկական ձևը փոխվել է, բայց պատճենված տեղեկատվության բովանդակությունը մնում է նույնը[27]:

Հատկանշական է, որ ներպետական օրենսդրությամբ համակարգչային տվյալների պատճե-

նահանումը որպես առանձին գործողություն քրեականացված չէ: ՀՀ ՔՕ-ն քննարկվող հանցակազմը որակյալ դարձնող հանգամանքները սահմանելիս ամրագրել է, որ ավելի խիստ քրեական պատասխանատվություն է նախատեսվում այն դեպքում, երբ վերը քննարկված օբյեկտիվ կողմը հանդիսացող արարքների դրսևորման հետևանքով առաջանում է, ի թիվս այլնի, առանձնակի արժեք ունեցող տվյալի պատճենահանում: Այսինքն, սույն դեպքում պատճենահանումը դիտարկվում է որպես ՀՀ ՔՕ 361-րդ հոդվածի 1-ին կամ 2-րդ մասով նախատեսված արարքի հետևանք և առաջացնում ավելի խիստ քրեական պատասխանատվություն, երբ դրանց կատարման արդյունքում առաջանում է տվյալի պատճենահանում:

Միևնույն, կարևոր է նշել, որ գործնականում հնարավոր են այնպիսի իրավիճակներ, երբ հանցավորի դիտավորությունը ուղղված լինի բացառապես համակարգչային տվյալը պատճենահանելուն, առանց այն ոչնչացնելու, վնասելու, աղավաղելու կամ ուղեփակելու, որի պարագայում առկա օրենսդրական բացը հնարավորություն է տալիս խուսափել քրեական պատասխանատվությունից: Հետևաբար, անտրամաբանական է օրենսդրի մոտեցումը առավել խիստ քրեական պատասխանատվություն նախատեսել օբյեկտիվ կողմի կատարման արդյունքում որպես վրա հասող «պատճենահանում» հետևանքի համար՝ չքրեականացնելով դրա՝ որպես առանձին դրսևորվելու հանգամանքը:

Հատկանշական է, որ միջազգային պրակտիկայի ուսումնասիրությունը ևս վկայում է այն մասին, որ պատճենահանումը որպես օբյեկտիվ կողմի առանձին դրսևորում նախատեսելը նպատակահարմար է և արդիական: Մասնավորապես, ԱՄՆ Կալիֆոռնիա նահանգի քրեական օրենսգրքի[28] 502-րդ հոդվածի «c» բաժնի 2-րդ մասը քրեական պատասխանատվություն է նախատեսում համակարգչային տվյալների պատճենահանման համար:

Վերոշարադրյալի հիման վրա առաջարկում ենք Օրենսգրքի 361-րդ հոդվածի 1-ին մասով որպես հանցակազմի օբյեկտիվ կողմի դրսևորում նախատեսել և քրեականացնել նաև համակարգչային տվյալը պատճենահանելու գործողությունը:

Անդրադառնանք հանցակազմը որակյալ դարձնող հանգամանքներին: Այսպես, ՀՀ ՔՕ 361-րդ հոդվածի 2-րդ մասը քննարկվող հանցակազմը ծանրացնող հանգամանքեր է դիտարկել ՀՀ ՔՕ 361-րդ հոդվածի 1-ին մասով նախատեսված արարքը կատարելը, որը զուգորդվել է համակարգիչ, համակարգչային համակարգ կամ համակարգչային ցանց առանց թույլտվության մուտք գործելով կամ անզգուշությամբ առաջացրել է առանձնապես խոշոր չափերի գույքային վնաս, հիմնարկի կամ կազմակերպության գործունեության խաթարում, վթար կամ աղետ, առանձնակի արժեք ունեցող տվյալի ոչնչացում, փոփոխություն, ուղեփակում (մեկուսացում) կամ պատճենահանում կամ այլ ծանր հետևանք:

Նշյալից ակնհայտ է, որ այս ծանրացնող հանգամանքների դրսևորման պարագայում, որոշ դեպքերում, կարող է առաջանալ քննարկվող հանցագործության և ՀՀ ՔՕ 359-րդ հոդվածով նախատեսված «Համակարգիչ, համակարգչային համակարգ կամ համակարգչային ցանց ներթափանցելը» վերտառությամբ հանցագործության հատում: Մասնավորապես, երբ հանցավորը դիտավորությամբ ոչնչացնի կամ վնասի համակարգչային տվյալը և դա զուգորդվի համակարգիչ, համակարգչային համակարգ կամ համակարգչային ցանց ներթափանցելով, արարքի որակման առնչությամբ գործնականում կարող են առաջանալ անհստակություններ:

Մեր կարծիքով, սույն դեպքում արարքը հանցագործությունների համակցությամբ որակելու հանգամանքը բացառվում է, քանի որ ՀՀ ՔՕ 361-րդ հոդվածի 2-րդ մասի 1-ին կետով սահմանված ծանրացնող հանգամանքի ձևակերպումն արդեն իսկ վկայում է, որ համակարգիչ, համակարգչային համակարգ կամ համակարգչային ցանց առանց թույլտվության մուտք գործելով «համակարգչային սաբոտաժը» հանցակազմի օբյեկտիվ կողմի դրսևորումները կատարելը համարվում է քննարկվող հանցակազմի բաղկացուցիչ մաս: Հետևաբար, արարքը պետք է որակվի միայն ՀՀ ՔՕ 361-րդ հոդվածի 2-րդ մասի 1-ին կետով՝ հաշվի առնելով նաև այն, որ ՀՀ ՔՕ 359-րդ հոդվածով նախատեսված հանցագործության համար նախատեսված է ավելի մեղմ պատիժ, քան «համակարգչային սաբոտաժը» հանցագործության համար:

Ավելին, ՀՀ ՔՕ 361-րդ հոդվածի 3-րդ մասը առավել խիստ քրեական պատասխանատվություն է նախատեսում այն դեպքում, երբ 361-րդ հոդվածի 1-ին կամ 2-րդ մասով նախատեսված արարքն առաջացրել է առանձնապես խոշոր չափերի գույքային վնաս, հիմնարկի կամ կազմակերպության գործունեության խաթարում, վթար կամ աղետ, առանձնակի արժեք ունեցող տվյալի ոչնչացում, փոփոխություն, ուղեփակում (մեկուսացում) կամ պատճենահանում կամ այլ ծանր հետևանք:

Նշյալ ծանրացնող հանգամանքի և ՀՀ ՔՕ 361-րդ հոդվածի 2-րդ մասի 2-րդ կետով նախատեսված ծանրացնող հանգամանքների տարբերությունը կայանում է դիտավորության դրսևորման մեջ, մասնավորապես, այն դեպքում, երբ վրա հասող հետևանքների նկատմամբ հանցավորը դրսևորում է ազգուշություն, արարքը որակվում է ՀՀ ՔՕ 361-րդ հոդվածի 2-րդ մասով, դիտավորության դրսևորման պարագայում՝ նույն հոդվածի 3-րդ մասով:

Կարևոր է ուշադրություն դարձնել նաև այն հանգամանքին, որ այդ ծանրացնող հանգամանքների որակման համար որպես պարտադիր պայման է դիտարկվել առանձնապես խոշոր չափերի գույքային վնասի պատճառումը կամ առանձնակի արժեք ունեցող տվյալի ոչնչացումը, փոփոխությունը, ուղեփակումը կամ պատճենահանումը:

Այսինքն, գույքային վնասի առաջացման դեպքում օրենսդիրը սույն հանցակազմի պարագայում արարքի քրեականացումը պայմանավորել է բացառապես առանձնապես խոշոր չափի գույքային վնասի առկայությամբ, որպիսի մոտեցման պարագայում, ստացվում է, որ հանցավորի կողմից օբյեկտիվ կողմի դրսևորումները դիտավորությամբ կատարելը, որը առաջացնում է խոշոր չափերի գույքային վնասի պատճառում, պետք է որակվի հասարակ հանցակազմով՝ ՀՀ ՔՕ 361-րդ հոդվածի 1-ին մասով: Մինչդեռ, օրենսդրի այս մոտեցումն անտրամաբանական է, մասնավորապես այն պայմաններում, երբ մի շարք հանցագործությունների (269-րդ, 279-րդ, 280-րդ, 282-րդ հոդվածներ) պարագայում խոշոր չափերի գույքային վնասի պատճառումը ևս դիտարկվել է որպես հանցակազմը ծանրացնող հանգամանք:

Ինչ վերաբերում է առանձնակի նշանակություն ունեցող տվյալներին, ապա որպես այդպիսին կարող են դիտարկվել պետական քաղաքական, տնտեսական, ռազմական, սոցիալական կամ անվտանգության հետ կապված ցանկացած այլ տվյալ, որի կորուստը, փոփոխությունը կամ բացահայտումը կարող է լուրջ վնաս պատճառել:

Ստացվում է, որ գործող ՀՀ ՔՕ-ն հստակ ամրագրում է թե՛ համակարգչային սաբոտաժի դրսևորումները՝ այդպիսիք դիտարկելով դրանք ոչնչացնելը, վնասելը, աղավաղելը կամ ուղեփակելը, և թե՛ արարքը ծանրացնող հանգամանքների սպառիչ ցանկը:

Անդրադառնանք քննարկվող հանցակազմի սուբյեկտին առնչվող առանձնահատկություններին: Օրենսգրքով ամրագրված «համակարգչային սաբոտաժ» հանցագործության համար քրեական պատասխանատվությունը առաջանում է, եթե այն կատարվում է իրավաբանական անձի կողմից կամ էլ ֆիզիկական անձի կողմից, բայց վերջինիս պատասխանատվության ենթարկելու համար կարևոր է հանցանքը կատարելու պահին արդեն իսկ 16 տարին լրացած լինելը և մեղսունակ վիճակում գտնվելը: Ինչ վերաբերում է իրավաբանական անձի քրեական պատասխանատվությանը, ապա այն նոր ինստիտուտ է քրեական իրավունքում: Ի սկզբանե քրեական օրենսգիրքը պատասխանատվություն նախատեսում էր միայն ֆիզիկական անձանց համար, իսկ 2021 թվականին ընդունված քրեական օրենսգրքով կարգավորվեցին իրավաբանական անձի քրեական պատասխանատվության հիմքերի, նրա նկատմամբ կիրառվող քրեաիրավական ներգործության միջոցների և այլ հարցեր: Միաժամանակ, կարևոր է նշել, որ ՀՀ ՔՕ 123-րդ հոդվածը սահմանում է իրավաբանական անձի քրեական պատասխանատվության հիմքերը: Օրինակ, իրավաբանական անձի քրեական պատասխանատվությունը կարող է առաջանալ այն դեպքում, երբ դրա գործունեության վրա ազդելու իրավասություն ունեցող անձի դրդմամբ համակարգչային տվյալները ոչնչացվեն:

Ինչպես նշվեց ՀՀ ՔՕ-ն նախատեսել է հանցակազմը որակյալ դարձնող հանգամանքների սպառիչ ցանկ, որը հնարավորություն չի տալիս որպես այդպիսին դիտարկել նաև այլ հանգամանքներ: Մասնավորապես, չի բացառվում, որ սույն հանցանքը կատարելու համար ստեղծված լինի հանցավոր կազմակերպություն կամ այն կատարվի երկու կամ ավելի անձանց դիտավորյալ համատեղ մասնակցությամբ՝ մի խումբ անձանց կողմից նախնական համաձայնությամբ:

Այսպես, մի խումբ անձանց կողմից նախնական համաձայնությամբ կամ հանցավոր կազմակերպության կողմից համակարգչային սաբոտաժի կատարումը ավելի մեծացնում է հանցանքն ավարտին հասցնելու հանցավորների մտադրությունը իրականացնելու հնարավորությունը և արարքի հանրային վտանգավորությունը: Այսինքն, սույն դեպքում գործ ունենք ավելի համախմբված, միասնական դիտավորություն ունեցող անձանց կողմից հանցանքի կատարման հետ, որոնք գործում են նախապես պլանավորված, մշակված մեթոդների հիման վրա, որոնք հեշտացնում են հանցանքի կատարումը:

Վերոգրյալի հիման վրա առաջարկում ենք որպես հանցակազմի ծանրացնող հանգամանքներ նախատեսել արարքի կատարումը մի խումբ անձանց կողմից նախնական համաձայնությամբ և հանցավոր կազմակերպության կողմից:

ԵԶՐԱԿԱՑՈՒԹՅՈՒՆ

Համակարգչային սաբոտաժը միջազգայնորեն ճանաչված հիմնախնդիրներից մեկն է, որը խաթարում է տեղեկատվական անվտանգության համակարգը, վտանգում պետական ու հասարակական կառույցների կայունությունը, անմիջական սպառնալիք հանդիսանում ոչ միայն տնտեսական, այլև ազգային անվտանգության համար:

Այն դուրս է եկել յուրաքանչյուր երկրի սահմաններից ու վերածվել վերազգային հիմնախնդրի, որի հաղթահարման միակ եղանակը բոլոր պետությունների կողմից դրա արգելմանն ուղղված միջոցառումների և խիստ վերահսկողական մեխանիզմների իրագործումն է:

Համակարգչային սաբոտաժը քրեականացնող օրենսդրության կատարելագործման նպատակով

ներկայացնում ենք հետևյալ առաջարկները և եզրահանգումները.

1. Կատարել օրենսդրական փոփոխություն, այն է՝ նախատեսել քրեական պատասխանատվություն համակարգչային տվյալը, ի թիվս այլնի, վերացնելու համար, որի ներքո կդիտարկվեն դրանք աղավաղելու և փոփոխելու գործողությունները, կամ ՀՀ ՔՕ-ում օգտագործված եզրույթները մեկնաբանել հետևյալ կերպ:

Համակարգչային տվյալի փոփոխություն ասելով պետք է հասկանալ դրանց բովանդակային փոփոխությունները, որոնք չեն կրի տեխնիկական բնույթ:

Համակարգչային տվյալների վնասում ասելով պետք է հասկանալ միջամտություն համակարգչային տեղեկատվության նկատմամբ, դրա կառուցվածքային ամբողջականության խախտում, որի արդյունքում դրանք կորցնում են իրենց բնականոն գործառնական հատկությունները կամ դառնում են օգտագործման համար ոչ անհրաժեշտ և պիտանի, ընդ որում, առանց դրանց բովանդակության փոփոխման կամ լիակատար ոչնչացման: Այսինքն, սույն գործողության պարագայում խախտվում է այդ տվյալների կառուցվածքը կամ ամբողջականությունը, որն էլ հանգեցնում է դրանք օգտագործելու անհնարինության,

Այսինքն, տվյալների վնասման դեպքում դրանց բովանդակությունը մնում է անփոփոխ, սակայն այլևս խաթարվում է դրանք ճիշտ մշակելու կամ այլ կերպ օգտագործելու համակարգչային համակարգի, ցանցի կամ այլ սարքավորման աշխատանքը:

«Աղավաղել» հասկացության ներքո պետք է դիտարկել այնպիսի գործողությունները, որոնց հետևանքով տվյալը, թեև ձևականորեն մնում է համակարգում, այնուամենայնիվ, այլևս չի արտացոլում իրական կամ սկզբնական բովանդակությունը, այսինքն, խեղաթյուրվում է այդ տվյալի ճշգրտությունը:

2. ՀՀ ՔՕ 361-րդ հոդվածի 1-ին մասով որպես հանցակազմի օբյեկտիվ կողմի դրսևորում նախատեսել և քրեականացնել նաև համակարգչային տվյալը պատճենահանելու գործողությունը:

3. Որպես հանցակազմի ծանրացնող հանգամանքներ նախատեսել արարքի կատարումը մի խումբ անձանց կողմից նախնական համաձայնությամբ և հանցավոր կազմակերպության կողմից:

4. Գույքային վնասի առաջացման դեպքում օրենսդիրը սույն հանցակազմով արարքի քրեականացումը պայմանավորել է բացառապես առանձնապես խոշոր չափի գույքային վնասի առկայությամբ, որպիսի մոտեցման պարագայում, ստացվում է, որ հանցավորի կողմից օբյեկտիվ կողմի դրսևորումները դիտավորությամբ կատարելը, որը առաջացնում է խոշոր չափերի գույքային վնասի պատճառում, պետք է որակվի հասարակ հանցակազմով՝ ՀՀ ՔՕ 361-րդ հոդվածի 1-ին մասով: Սինչդեռ, օրենսդրի այս մոտեցումն անտրամաբանական է, մասնավորապես այն պայմաններում, երբ մի շարք հանցագործությունների (ՀՀ ՔՕ 269-րդ, 279-րդ, 280-րդ, 282-րդ հոդվածներ) պարագայում խոշոր չափերի գույքային վնասի պատճառումը ևս դիտարկվել է որպես հանցակազմը ծանրացնող հանգամանք:

[1] Տե՛ս, Номоконов В.А., Тропина Т.Л.. Киберпреступность как новая криминальная угроза, криминология интернет-пространства УДК 343.9 ББК 67.51, 2012, էջ 45:
[2] Տե՛ս, Волеводз А.Г. Волеводз Д.А. Уголовное законодательство об ответственности за компьютерные преступления: ОПЫТ РАЗНЫХ СТРАН, Правовые вопросы связи. – 2004. – № 1. – С. 37-48.
[3] Տե՛ս, Номоконов В. А., Тропина Т.Л.. Киберпреступность как новая криминальная угроза, криминология интернет-пространства УДК 343.9 ББК 67.51, 2012, էջ 45:
[4] Տե՛ս, Апкаев Д. М. Преступления в сфере компьютерной информации / Д. М. Апкаев, А. С. Мельников // Пенитенциарное право: юридическая теория и правоприменительная практика. – 2019. – № 1 (19). – С. 74–76.
[5] Տե՛ս, Կիբեռհանցագործությունների մասին կոնվենցիա, Սկզբնաղբյուրը՝ ՀՀԱԳՆՊՏ 2008.02.11/9(17), Բուդապեշտ, ընդունվել է՝ 23.11.2001, ուժի մեջ է մտել՝ 01.02.2007:
[6] Տե՛ս, Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001, European Treaty Series - No. 185
[7] Հասանելի է հետևյալ հղմամբ՝ https://www.arlis.am/documentview.aspx?docid=121592 (վերջին մուտք՝ 15.10.2025թ.):
[8] Տե՛ս, ՀՀ քրեական օրենսգիրք, ՀՕ-199-Ն, Տեղեկագիր 2021.05.17-2021.05.30, ընդունվել է 05.05.2021, ուժի մեջ է մտել 01.07.2022.

[9] Հասանելի է հետևյալ հղմամբ, https://book.kbsu.ru/theory/chapter2/1_2.htm (վերջին մուտք՝ 20.10.2025թ.):
[10] Տե՛ս, Tennessee Code § 39-14-601 — Definitions (Computer Network / System) https://law.justia.com/codes/tennessee/title-39/chapter-14/part-6/section-39-14-601/?utm_source. (վերջին մուտք՝ 01.11.2025թ.):
[11] Տե՛ս, Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001, էջ 5:
[12] Տե՛ս, Tennessee Code § 39-14-601 — Definitions (Computer Network / System) https://law.justia.com/codes/tennessee/title-39/chapter-14/part-6/section-39-14-601/?utm_source. (վերջին մուտք՝ 01.11.2025թ.):
[13] Հասանելի է հետևյալ հղմամբ՝ https://gb.ru/blog/vidy-kompjuternyh-setej/ (վերջին մուտք՝ 22.09.2025թ.):
[14] Հասանելի է հետևյալ հղմամբ՝ https://www.ittelo.ru/news/chto-takoe-periferiynoe-oborudovanie/?srsltid=AfmBOorLjKe-oiiyL3Hqve0UzonjFRkLydOmQe8dxnjgYYXOSBB58Dix (վերջին մուտք՝ 18.09.2025թ.):
[15] Տե՛ս, Николаевич Е. К. «Противодействие компьютерной преступности: теория, законодательство, практика», МОСКВА – 2021, 307:
[16] Տե՛ս, Лебедева В. М. Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. д.ю.н., председателя Верховного Суда Российской Федерации. Москва: Норма, 2006. С. 704; Уголовное право России. Особенная часть: учебник / под ред. И. Э. Звечаровского. Москва: Норма: Инфра-М, 2010. С. 730. Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью (уголовно-правовые и криминологические проблемы) : 12.00.08 : дис. ... канд. юрид. наук. Москва, 2005. С. 50; Степанов-Егиянц В. Г. Указ. соч. С. 125.
[17] Տե՛ս, Радченко В. И., Михлина А. С. Комментарий к Уголовному кодексу Российской Федерации / под ред.. Санкт-Петербург: Питер, 2008. С. 563.
[18] Տե՛ս, Дворецкий М. Ю. Преступления в сфере компьютерной информации (уголовно – правовое исследование) : 12.00.08 : дис. … канд. юрид. наук. Волгоград, 2001. С. 84;
Лебедева В. М. Комментарий к Уголовному кодексу Российской Федерации / под общ.ред. доктора юридических наук, Председателя Верховного Суда Российской Федерации и доктора юридических наук, профессора Ю. И. Скуратова. Москва, 2002. С. 733. (Автор главы – к.ю.н. С.А. Пашин).
[19] Տե՛ս, Кадникова Н. Г. Комментарий к Уголовному Кодексу Российской Федерации (постатейный) / под общ. ред. д.ю.н., проф. Москва: Книжный мир, 2005. С. 691. (Автор главы – к.ю.н. А.В. Пушкин).
[20] Տե՛ս, Наумова А. В. Комментарий к Уголовному кодексу Российской Федерации / под ред. доктора юридических наук, проф.. Москва, 1996. С. 664 (Автор главы – д.ю.н., проф. С.В. Бородин).
Попов А.Н. Комментарий к Уголовному кодексу Российской Федерации / под ред. В. И. Радченко, А. С. Михлина. Санкт-Петербург: Питер, 2008. С.566.
Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий: монография. Москва: Юрлитинформ, 2015. С.100; Степанов-Егиянц В. Г. Указ. соч. С. 176.
[21] Տե՛ս, Быков В. М., Черкасов В. Н. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ // Российский судья. 2012. № 5. С. 14-19; Сало И. А. Указ. соч. С.104.
[22] Տե՛ս, Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий: монография. Москва: Юрлитинформ, 2015. С. 100; Степанов-Егиянц В. Г. Указ. соч. С. 176.
Տե՛ս, Радченко В. И., Михлина А. С. Комментарий к Уголовному кодексу Российской Федерации / под ред.. Санкт-Петербург: Питер, 2008. С. 566. (Автор главы – д.ю.н., проф. А.Н. Попов).
[23] Տե՛ս, California public law, art 502, section B(10) https://california.public.law/codes/penal_code_section_502#10-%E2%80%9Cinjury%E2%80%9D-means-any-alteration-deletion-damage-or-destruction (í»ñçÇÝ Ùáõïù՝ 20.09.2025Ã.):
[24] Տե՛ս, Computer Misuse Act 1990 https://www.legislation.gov.uk/ukpga/1990/18/enacted?utm_source (վերջին մուտք՝ 21.09.2025թ.):
[25] Տե՛ս, Computer Fraud and Abuse Act, 18 U.S.C. § 1030, 1996, art 18 https://www.law.cornell.edu/uscode/text /18/1030 (վերջին մուտք՝ 25.09.2025թ.):
[26] Տե՛ս, Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: ООО Издательство «Юрлитинформ», 2002. С. 69);
Տե՛ս, Копырюлин А. Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты: 12.00.08 : дис. … канд. юрид. наук. Тамбов, 2007. С. 17);
Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: 12.00.08 : дис. канд. юрид. наук. Москва, 2007. С. 57);
[27] Տե՛ս, Николаевич Е. К. «Противодействие компьютерной преступности: теория, законодательство, практика» МОСКВА – 2021, С 324:
[28] Տե՛ս, California Penal Code Part 1. Of Crimes and Punishments Title 13. Of Crimes Against Property Chapter 5. Larceny. 502. Unauthorized access to computers, computer systems and computer data.

ՕԳՏԱԳՈՐԾՎԱԾ ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. ՀՀ քրեական օրենսգիրք, ՀՕ-199-Ն, Միասնական կայք 2021.05.17-2021.05.30, ընդունվել է 05.05.2021, ուժի մեջ է մտել 01.07.2022:
2. Բուդապեշտի կոնվենցիա, Հիմնական ակտ (01.02.2007-մինչ օրս), ՀՀԱԳՆՊՏ 2008.02.11/9(17), Եվրոպայի խորհուրդ, ընդունվել է 23.11.2001, ուժի մեջ է մտել 01.02.2007.
3. California public law, art 502, section B(10) https://california.public.law/codes/penal_code_section_502#10-%E2%80%9Cinjury%E2%80%9D-means-any-alteration-deletion-damage-or-destruction (վերջին մուտք՝ 20.09.2025թ.):
4. Computer Fraud and Abuse Act, 18 U.S.C. § 1030, 1996, art 18 https://www.law.cornell.edu/uscode/text/18/1030 (վերջին մուտք՝ 25.09.2025թ.):
5. Computer Misuse Act 1990 https://www.legislation.gov.uk/ukpga/1990/18/enacted?utm_source (վերջին մուտք՝ 21.09.2025թ.):
6. Explanatory Report to the Convention on Cybercrime Budapest, 23.XI.2001.
7. Tennessee Code § 39-14-601 — Definitions (Computer Network / System) https://law.justia.com/codes/tennessee/title-39/chapter-14/part-6/section-39-14-601/?utm_source. (վերջին մուտք՝ 01.11.2025թ.):
8. Апкаев, Д. М. Преступления в сфере компьютерной информации / Апкаев Д. М., Мельников А. С. // Пенитенциарное право: юридическая теория и правоприменительная практика. – 2019. – № 1 (19).
9. Быков В. М., Черкасов В. Н. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ // Российский судья. 2012. № 5.
10. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. Москва: ООО Издательство «Юрлитинформ», 2002.
11. Волеводз. А.Г. Волеводз Д.А. Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран, Правовые вопросы связи. – 2004. – № 1.
12. Дворецкий М. Ю. Преступления в сфере компьютерной информации (уголовно – правовое исследование) : 12.00.08 : дис. … канд. юрид. наук. Волгоград, 2001.
13. Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью (уголовно-правовые и криминологические проблемы) : 12.00.08 : дис. ... канд. юрид. наук. Москва, 2005. С. 50; Степанов-Егиянц В. Г. Указ. соч.
14. Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий: монография. Москва: Юрлитинформ, 2015. Степанов-Егиянц В. Г. Указ. соч.
15. Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: 12.00.08 : дис. … канд. юрид. наук. Москва, 2007.
16. Кадникова Н. Г. Комментарий к Уголовному Кодексу Российской Федерации (постатейный) / под общ. ред. д.ю.н., проф. Москва: Книжный мир, 2005.
17. Копырюлин А. Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты, 12.00.08, дис. … канд. юрид. наук. 2007.
18. Лебедева В. М. Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. д.ю.н., председателя Верховного Суда Российской Федерации. Москва: Норма, 2006. С. 704; Уголовное право России. Особенная часть: учебник / под ред. И. Э. Звечаровского. Москва: Норма: Инфра-М, 2010. С. 730. .
19. Наумова А. В. Комментарий к Уголовному кодексу Российской Федерации / под ред. доктора юридических наук, проф.. Москва, 1996. (Автор главы – д.ю.н., проф. С.В. Бородин);
20. Николаевич Е. К. «Противодействие компьютерной преступности: теория, законодательство, практика», МОСКВА – 2021.
21. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза, криминология интернет-пространства УДК 343.9 ББК 67.51, 2012.
22. Попов А.Н. Комментарий к Уголовному кодексу Российской Федерации / под ред. В. И. Радченко, А. С. Михлина. Санкт-Петербург: Питер, 2008.
23. https://www.arlis.am/documentview.aspx?docid=121592. (վերջին մուտք՝ 15.10.2025թ.):
24. https://book.kbsu.ru/theory/chapter2/1_2.html. (վերջին մուտք՝ 20.10.2025թ.):
25. https://gb.ru/blog/vidy-kompjuternyh-setej/. (վերջին մուտք՝ 22.09.2025թ.):

References

1. HH qreakan o’rensgirq, HO’-199-N, Miasnakan kayq 2021.05.17-2021.05.30, y’ndownvel e’ 05.05.2021, owjhi mej e’ mtel 01.07.2022:
2. Bowdapeshti konvencia, Himnakan akt (01.02.2007-minch o’rs), HHAGNPT 2008.02.11/9(17), Evropayi xorhowrd, y’ndownvel e’ 23.11.2001, owjhi mej e’ mtel 01.02.2007.
3. A.G.Volevodz D.A.Volevodz Ugolovnoe zakonodatel’stvo ob otvetstvennosti za komp’juternye prestuplenija: opyt raznyh stran, Pravovye voprosy svjazi. – 2004. – № 1.

4. Apkaev D. M. Prestuplenija v sfere komp'juternoj informacii / D. M. Apkaev, A. S. Mel'nikov // Penitenciarnoe pravo: juridicheskaja teorija i pravoprimenitel'naja praktika. – 2019. – № 1 (19).
5. Bykov V. M. Cherkasov V. N. Novyj zakon o prestuplenijah v sfere komp'juternoj informacii: st. 272 UK RF // Rossijskij sud'ja. 2012. № 5.
6. Dobrovol'skij D. V. Aktual'nye problemy bor'by s komp'juternoj prestupnost'ju (ugolovno-pravovye i kriminologicheskie problemy) : 12.00.08 : dis. ... kand. jurid. nauk. Moskva, 2005. S. 50; Stepanov-Egijanc V. G. Ukaz. soch.
7. Dvoreckij M. Ju. Prestuplenija v sfere komp'juternoj informacii (ugolovno – pravovoe issledovanie) : 12.00.08 : dis. … kand. jurid. nauk. Volgograd, 2001.
8. Efremova M.A. Ugolovnaja otvetstvennost' za prestuplenija, sovershaemye s ispol'zovaniem informacionno-telekommunikacionnyh tehnologij: monografija. Moskva: Jurlitinform, 2015. Stepanov-Egijanc V. G. Ukaz. soch.
9. Kadnikova N. G. Kommentarij k Ugolovnomu Kodeksu Rossijskoj Federacii (postatejnyj) / pod obshh. red. d.ju.n., prof. Moskva: Knizhnyj mir, 2005.
10. Kopyrjulin A. N. Prestuplenija v sfere komp'juternoj informacii: ugolovno-pravovoj i kriminologicheskij aspekty, 12.00.08, dis. … kand. jurid. nauk. 2007.
11. Lebedeva V. M. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii / pod obshh. red. d.ju.n., predsedatelja Verhovnogo Suda Rossijskoj Federacii. Moskva: Norma, 2006. S. 704; Ugolovnoe pravo Rossii. Osobennaja chast': uchebnik / pod red. I. Je. Zvecharovskogo. Moskva: Norma: Infra-M, 2010. S. 730.
12. Naumova A. V. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii / pod red. doktora juridicheskih nauk, prof.. Moskva, 1996. (Avtor glavy – d.ju.n., prof. S.V. Borodin);
13. Nikolaevich E. K. «Protivodejstvie komp'juternoj prestupnosti: teorija, zakonodatel'stvo, praktika», MOSKVA – 2021.
14. Nomokonov V. A., Tropina T.L. Kiberprestupnost' kak novaja kriminal'naja ugroza, kriminologija internet-prostranstva UDK 343.9 BBK 67.51, 2012.
15. Popov A.N. Kommentarij k Ugolovnomu kodeksu Rossijskoj Federacii / pod red. V. I. Radchenko, A. S. Mihlina. Sankt-Peterburg: Piter, 2008.
16. Volevodz A. G. Protivodejstvie komp'juternym prestuplenijam: pravovye osnovy mezhdunarodnogo sotrudnichestva. Moskva: OOO Izdatel'stvo «Jurlitinform», 2002.
17. Zinina U. V. Prestuplenija v sfere komp'juternoj informacii v rossijskom i zarubezhnom ugolovnom prave: 12.00.08 : dis. … kand. jurid. nauk. Moskva, 2007.

Анаит Бабаханян
Помощник Генерального прокурора Республики Армения

РЕЗЮМЕ

Уголовная ответственность за компьютерный саботаж

Преступления, совершаемые на компьютере, в компьютерной системе, компьютерной сети или на других компьютерных устройствах, вышли за пределы границ отдельных государств и превратились в транснациональную проблему. Единственным способом её преодоления является осуществление всеми государствами мер, направленных на её пресечение, и внедрение строгих контрольных механизмов.

В настоящей статье проведено исследование состава преступления, предусмотренного Уголовным кодексом Республики Армения статьёй под названием «Компьютерный саботаж».

В статье изучены и проанализированы уголовно-правовая характеристика рассматриваемого состава преступления, его элементы, а также выявлены проблемные правовые положения, которые на практике могут создавать определённые препятствия при уголовно-правовой квалификации деяния. По результатам проведённого анализа представлены законодательные предложения, направленные на совершенствование уголовного законодательства в данной сфере.

***Ключевые слова**: Будапештская конвенция о киберпреступности, компьютерный саботаж, компьютер, компьютерная система, компьютерная сеть.*

Anahit Babakhanyan
Assistant to Prosecutor General of the RA

SUMMARY
Criminal liability for computer sabotage

Crimes committed on a computer, in a computer system, computer network, or other computer devices have crossed the borders of individual states and have turned into a transnational issue. The only way to overcome this problem is through the implementation by all states of measures aimed at its prevention and the establishment of strict control mechanisms.

This article presents a study of the crime set forth in the Criminal Code of the Republic of Armenia, under the article titled “Computer Sabotage”.

The article examines and analyzes the criminal-law characteristics of the offence in question, its constituent elements, and identifies problematic legal provisions that may, in practice, create certain obstacles in the criminal-legal qualification of the act. As a result of the conducted analysis, legislative proposals have been presented with the aim of improving the criminal legislation in this field.

Key words: *Budapest Convention on Cybercrime, computer sabotage, computer, computer system, computer network.*

Ընագիրը ներկայացվել է 13.11.2025թ.
Ընդունվել է տպագրության 18.11.25թ.