Jurisprudencija, 1999, t. 12(4); 69-75

V. KRIMINALISTIKA

KOMPIUTERINĖS ĮRANGOS PANAUDOJIMAS EKONOMINIAMS NUSIKALTIMAMS (KAI KURIE KRIMINALISTINĖS CHARAKTERISTIKOS IR TYRIMO METODIKOS YPATUMAI)

Ryšardas Burda

Kriminalistikos katedra, Lietuvos teisės akademija, Ateities g. 20, 2057 Vilnius
Telefonas 71 46 11

Spaudai pateikta 1999 m. rugsėjo 24 d.

Santrauka

Šiame straipsnyje nagrinėjami su kompiuterinės įrangos panaudojimu darant įvairius nusikaltimus susiję klausimai, kriminalistinis šių veikų bei asmenų apibūdinimas, tardomųjų veiksmų atlikimo ypatumai.

Galime teigti, kad kol Baudžiamajame kodekse veikos, kuriose panaudojama kompiuterinė įranga, tiesiogiai neįvardytos kaip nusikaltimai, kompiuterinių nusikaltimų Lietuvoje nėra. Tačiau tai nereiškia, kad panašios veikos nepavojingos visuomenei, valstybei ar asmeniui, ir tai jau ne prielaida, o gyvenimo realijos.

Kriminalistiniu požiūriu asmenis, kurie kompiuterine įranga padaro pavojingus veiksmus, santykinai galime skirstyti į trys grupes: įsilaužėlius pokštininkus (*crackers*), nusikaltėlius (*criminals*) ir vandalus (*vandals*). Atskiruose šaltiniuose jie apibūdinami skirtingai, tačiau juos visus vienija veikų padarymo priemonė – kompiuterinė įranga bei galimi jos panaudojimo būdai.

Kompiuterinės įrangos panaudojimo būdai yra įvairūs, jie nuolat tobulėja ir priklauso nuo naudojamos kompiuterinės ir programinės įrangos lygio.

Dažniausiai atliekami tardomieji veiksmai, kai apžiūrima ir paimama kompiuterinė įranga, yra įvykio vietos apžiūra, krata ir poėmis. Ypač apgalvoti turi būti kaltininko sulaikymo operacijos veiksmai. Atliekant visus paminėtus tardomuosius veiksmus, būtina laikytis kai kurių taisyklių: viena iš jų – kviesti kompiuterinės įrangos specialistą. Kitos taisyklės susijusios su kompiuterinės įrangos apžiūra, jos paėmimu ir informacijos išsaugojimu.

Kai kuriais duomenimis, pirmas kompiuterinės įrangos panaudojimo faktas, kai iš banko buvusioje Tarybų Sąjungoje buvo pagrobti pinigai, Lietuvoje buvo užregistruotas 1979 metais. Tada Vilniuje iš vieno banko buvo pagrobta daugiau kaip 78 tūkst. rb. [1]. Pastaraisiais metais kriminalistikos literatūroje vis daugiau rašoma apie nusikaltimus, kuriems panaudojama kompiuterinė įranga. Šiais klausimais rašė M. Gramatyka, K. J. Jakubski, V. Krylovas, V. Vehovas, J. Baturinas ir kiti [2]. Lietuvoje ši problema tik pradėta nagrinėti [3, 10-13, 28-29]. Tą daryti verčia vis dažnėjančios atskirų įmonių bei asmenų interesus pažeidžiančios veikos, kurios Baudžiamajame kodekse tiesiogiai neįvardytos kaip kompiuteriniai nusikaltimai[1]. Tiesa, jame kaip atskiras kvalifikuojantis veiką požymis yra nurodytas kompiuterinės įrangos panaudojimas darant nusikaltimus. Kriminalistiniu požiūriu tai yra nusikaltimo padarymo būdas, kurio esminis ypatumas yra tai, kad buvo panaudota speciali (ne tik techninė, bet ir programinė) įranga.

[1] Baudžiamojo kodekso projekte išskirti kompiuteriniai nusikaltimai (žr.: Teisės problemos. 1997. Nr. 1.).

Kitas svarbus panašių veiksmų aspektas yra tas, kad nusikalstamus veiksmus, kuriems naudojama kompiuterinė įranga, dažniausiai galima priskirti prie ekonominių nusikaltimų. Tai ne tik kompiuterinės informacijos vagystė, bet ir programinės įrangos savanaudiškas platinimas [4], naudojantis kompiuterine įranga nesankcionuotas patekimas į telefono tinklus ir kalbėjimas kitų klientų sąskaita (vadinamieji "telefonų chakeriai") [5, 17-19], pinigų vagystės panaudojant mokėjimo korteles ir pan.

Kriminalistikos literatūroje pasirodė pirmosios nusikaltimų, susijusių su kompiuterinės įrangos panaudojimu, klasifikacijos bei šių nusikaltimų kriminalistinė charakteristika. Apibūdinant kompiuterinius nusikaltimus, analizuojama naudojama įranga, nusikaltimo padarymo būdas ir mechanizmas, duomenys apie nusikaltimo padarymo aplinką bei nusikaltėlio asmenybę. Tačiau pastarojo elemento charakteristikai skiriama nepakankamai dėmesio [6, 63-65].

JAV mokslininkai, tokie kaip R. Poweris, D. Icove'as, K. Segeris, Von W. Storchas, Kanados mokslininkas Arlin J. Cooperis, pateikia apibendrintus duomenis apie asmenis, kurie padaro tokio pobūdžio nusikaltimus, jų psichologinį ir socialinį apibūdinimą, techninės įrangos bei programinio aprūpinimo parametrus ir pan. [7].

Apibendrindami Arlin J. Cooperio ir kitų autorių tyrinėjimus, galime išskirti tris pagrindines asmenų, kurie daro neteisėtus veiksmus, panaudodami kompiuterinę įrangą, grupes:

1. įsilaužėliai pokštininkai (*crackers*);
2. nusikaltėliai (*criminals*);
3. vandalai (*vandals*).

Įsilaužėliai pokštininkai savo ruožtu skirstomi į tuos, kurie veikia grupėmis ir pavieniui. Nusikaltėlių grupes santykinai galima suskirstyti į tuos, kurie šnipinėja, ir tuos, kurie vagia iš finansinių ir kitų įstaigų (įmonių). Vandalai skirstomi į savus ir svetimus. Pirmoji grupė – tai asmenys, dirbantys toje pačioje įstaigoje (įmonėje), kurioje ir daro pažeidimus, o antroji – visi kiti, kas nedirba toje įmonėje (įstaigoje).

Literatūroje pateiktus nusikaltimų padarymo panaudojant kompiuterinę įrangą būdus galima suskirstyti į keturias grupes:

1. perėmimo;
2. nesankcionuotos prieigos;
3. manipuliacijų;
4. kompleksinius.

Šis nusikaltimų padarymo būdų sąrašas nėra išsamus, jis nuolat keičiasi kartu su nuolat besikeičiančia kompiuterine ir programine įranga.

Nusikaltėlio veiksmai gali būti nukreipti į kompiuterinę įrangą, kaip į vertybę arba informacijos šaltinį, ir į kompiuterinę informaciją nepaisant kokioje laikmenoje ir kokio pavidalo ji būtų.

Tiriant nusikaltimus, labai svarbu žinoti nusikaltimo padarymo būdą ir atpažinti tam tikrų būdų atspindžius – pėdsakus. Nusikaltimo padarymo būdus, susijusius su kompiuterinės įrangos panaudojimu, galima skirstyti į tris pagrindines grupes:

1. tiesioginio priėjimo;
2. atokaus priėjimo;
3. mišraus priėjimo.

Antrosios grupės būdus dar galima skirstyti į tiesioginio perėmimo (panaudojant laidinio ryšio priemones arba svetimus slaptažodžius) ir elektromagnetinio perėmimo.

Paliekami pėdsakai paprastai skirstomi į dvi grupes: daiktinius ir intelektinius. Prie daiktinių pėdsakų priskiriamos elektroninės kortelės, elektroniniai raktai, naudotojo identifikavimo įranga pagal pirštų pėdsakus, rankos geometrinius požymius, raštą, balsą. Taip pat šiai grupei priskiriami tradiciniai kriminalistiniai pėdsakai: pirštų, rankų, mikrodalelės, biologiniai asmens pėdsakai ir kt.

Intelektinius pėdsakus galima suskirstyti į tris grupes:

1. Pėdsakai, rodantys tam tikrus failo struktūros pokyčius. Tai failų bei katalogų pavadinimų, failo dydžio ir turinio, failo standartinių rekvizitų pakeitimas, naujų failų ar katalogų atsiradimas.

2. Anksčiau užprogramuotos kompiuterio ekrano spalvos, vaizdelių, spausdintuvo ar kitos įrangos tarpusavio suderinamumo pakitimai ir pan.
3. Neįprastas kompiuterio darbas: sulėtėjęs operacinės sistemos, pelytės valdymo darbas, netikėtų simbolių atsiradimas, įprastų komandų nestandartinis įvykdymas ir pan.

Gali būti ir kitų pėdsakų – jie priklauso nuo kompiuterinės ir programinės įrangos panaudojimo būdų ir nusikaltimo pobūdžio.

Pradėjus kompiuterinę įrangą naudoti informacijai įrašyti, kaupti ir apdoroti, naujais elementais pasipildė dokumento sąvoka. Atsirado elektroninio dokumento sąvoka.

Dokumentas reiškia bet kokį materialų objektą, kuriame bet kokiu būdu ir bet kokiais ženklais užfiksuota kokia nors informacija [8, 9]. Tai gali būti popierius, kino ar magnetinė juosta, nuotrauka ir pan. Mikroschemos, diskeliai ir kompaktiniai diskai yra specifinio pobūdžio informacijos laikmenos, darbas su kuriomis (įrašymas, taisymas (keitimas)) skiriasi nuo mums iki tol žinomų būdų. Tai nulemia naujų nusikaltimo padarymo būdų atsiradimą.

Mūsų šalyje nėra norminio akto, leidžiančio pripažinti kompiuterinę informaciją dokumentu. Tačiau, tiriant nusikaltimus, kompiuterio duomenis ir kompiuterinę įrangą galima įvertinti kitu aspektu.

Pirmiausia kompiuterinė įranga, panaudota darant nusikaltimus, yra nusikaltimo padarymo priemonė (įrankis), kuri savaime taps daiktiniu įrodymu po to, kai bus paimta, apžiūrėta ir tyrėjas priims procesinį sprendimą. Remiantis pėdsakais, aptiktais ant įvairios įrangos apžiūros metu ir atliekant kitus tardomuosius veiksmus, galima bus nustatyti asmenis, dirbusius su šia įranga. Pėdsakai, atspindintys asmenų intelektualinę veiklą, išlieka kompiuterio atmintyje. Šiuos duomenis galima pateikti kiekvienam žmogui suprantamais ženklais kompiuterinės ekspertizės metu.

Visos šios aplinkybės verčia kriminalistus (mokslininkus bei praktikus), ekspertus rengti naujus nusikaltimų bei kriminalistinių objektų tyrimo metodus.

Nusikaltimams, kuriems panaudojama kompiuterinė technika, kaip ir kitiems ekonominiams nusikaltimams, kruopščiai ruošiamasi. Nusikaltimo pasirengimo stadijai būdingas išankstinis pėdsakų slėpimas arba tokių veiksmų numatymas. Todėl aptikti tokius nusikaltimus pasirengimo stadijoje paprastai yra itin sudėtinga. Tačiau tyrimo organų naudojama programinė įranga leidžia ne tik aptikti nusikaltimo pėdsakus tinkle ar kompiuteryje, kas svarbu įrodinėjant nusikalstamą veiką, bet ir sekti šiuos žingsnius. Todėl nusikaltimų tyrimo sėkmė priklauso nuo to, kiek ir kokios informacijos turi tyrimo institucijos.

Tiriant sukčiavimus ir turtinės žalos padarymą apgaule arba piktnaudžiaujant pasitikėjimu, galimos šios tipinės tyrimo situacijos: nusikaltėlis sulaikytas nusikaltimo vietoje su įkalčiais; nusikaltėlio asmenybė nenustatyta, tačiau žinomas jo nusikaltimo padarymo būdas ir vieta (panaudojus atokius nusikaltimo padarymo būdus); žinomi tik nusikaltimo padariniai.

Šiose situacijose, atsižvelgiant į jų pobūdį, atliekami šie tardomieji veiksmai: asmens sulaikymas; įvykio vietos ir įrangos apžiūra; dokumentų, kompiuterinės įrangos ar kompiuterinės informacijos laikmenų poėmis arba krata turint tikslą juos surasti; įtariamojo apklausa; kompiuterinės ir kitos įrangos ekspertizė bei kiti veiksmai.

Trumpai apžvelgsime kai kuriuos iš jų.

Tiriant nusikaltimus, įmanomi du kompiuterinės informacijos paėmimo būdai:

1. kompiuterinės informacijos paėmimas kartu su kompiuterine įranga;
2. kompiuterinės informacijos kopijavimas.

Dažniausiai tiriant nusikaltimus kompiuterinę įrangą galima paimti tik atliekant kratą ar įvykio vietos apžiūrą. Atskirais atvejais ji (pvz., nešiojamieji kompiuteriai) gali būti paimama ir asmens kratos metu sulaikant įtariamąjį.

1. Pasiruošiant kratai ar įvykio vietos apžiūrai būtina laikytis šių taisyklių:

a) niekam neleisti liesti kompiuterinės įrangos;

b) negalima išjunginėti elektros patalpose[1];

[1] Neretai kriminalinės policijos darbuotojai, prieš įeidami į kratomąsias patalpas, atjungia elektrą. Šiuo atveju toks taktinis būdas neleistinas.

c) jei pastate elektra atjungta, būtina ištraukti iš kištukinių lizdų kompiuterinę įrangą, kol ji vėl bus įjungta;

d) tyrėjas neturi liesti kompiuterio klaviatūros, jungiklių, jei nežinomi šių veiksmų padariniai;

e) jeigu patalpose kartu su kompiuterine įranga yra lengvai užsidegančių medžiagų, sprogmenų ir pan., iki darbo su kompiuteriais pradžios būtina šias medžiagas izoliuoti;

f) jei pavojingų medžiagų neįmanoma atskirti nuo kompiuterinės įrangos, būtina evakuoti žmones.

1.1. Prieš pradedant kratą ar įvykio vietos apžiūrą, būtina imtis visų įmanomų apsaugos priemonių:

a) nustatyti visų esančių patalpoje žmonių asmenybes.Tai ypač svarbu norint nustatyti kompiuterinės įrangos specialistus, kuriems tikrinama įmonė (įstaiga) nėra pagrindinė darbovietė;

b) ieškant darbą su kompiuteriu liečiančių užrašų, neleisti pasinaudoti nuotolinio valdymo įrenginiais, kuriais gali būti paveikti kompiuteriai, taip pat būtina atlikti patalpoje esančių žmonių kratą;

c) negalima leisti kratomiesiems pažeisti ar sunaikinti kompiuterinės įrangos, kitų įrenginių, diskelių, diskų ir pan.;

d) būtina išsiaiškinti, ar yra kompiuterinės įrangos apsaugos sistema;

e) svarbu nustatyti, ar yra informacijos sunaikinimo programa, kuria būtų galima nesankcionuotai pasinaudoti;

f) tyrėjas privalo nustatyti, kokia yra patalpoje jam nežinoma techninė įranga.

1.2. Tardomųjų veiksmų atlikimo stadijoje būtina laikytis šių taisyklių:

a) aprašyti ir kitomis priemonėmis užfiksuoti visų objektų, kompiuterinės įrangos ir kitų daiktų išsidėstymą;

b) nustatyti, koks įjungtų kompiuterinių bei kitų ryšio įrenginių tipas, markė, numeriai, kanalai, dažnis ir pan.;

c) aprašyti įrenginių tarpusavio sujungimą (laidus ir jų spalvą, kištukus, esamas ant jų etiketes ir pan.);

d) jeigu kompiuteris įjungtas, pirmiausia išeiti iš veikiančios programos ir tik po to išjungti įrangą iš elektros tinklo;

e) išeinant iš programų, aprašinėti kiekvieną operaciją su įrenginiais ir fiksuoti monitoriuje rodomą vaizdą;

f) jei yra apsaugos sistema, nustatyti slaptažodžius, kitus algoritmus, įėjimo ir išėjimo į kompiuterio programas būdus;

g) išjungti visus kompiuterius iš elektros tinklo;

h) neperžiūrinėti programų ar duomenų bazių tardomųjų veiksmų atlikimo vietoje;

i) sudėtingose situacijose kviesti informatikos specialistą ir jokiu būdu neprašyti pagalbos įmonės personalo;

j) būtina apžiūrėti ir paimti visą kratomojoje įmonėje (įstaigoje) esančią kompiuterinę įrangą;

k) atsargiai naudoti metalo ieškiklius (ne arčiau kaip 1 m atstumu), elektromagnetines priemones, galingus šviesos prietaisus ar kitą specialiąją techniką;

l) ieškant ant kompiuterinės įrangos ir kitų objektų (diskelių, kompaktinių diskų ir pan.) pirštų pėdsakų, draudžiama naudoti magnetinius šepetėlius arba kitiems pėdsakams surasti elektrostatinius ieškiklius (EPI-2);

m) darbo vietose būtina ieškoti ir paimti visus darbą su kompiuteriu liečiančius užrašus;

n) paimamą kompiuterinę įrangą, norint apsaugoti nuo nesankcionuoto naudojimo, būtina užantspauduoti. Kompiuterio maitinimo lizdą bei jungiklius reikia užklijuoti tyrėjo užpildytais ir pasirašytais lapeliais;

o) diskelius, kompaktinius diskus reikia aprašyti (nurodyti markę, pavadinimą, užrašus ant lipduko ir pan.) ir paimti kartu su pakuote arba dėžute, kurioje saugomi, atskirus diskelius įpakuoti į aliuminio foliją ir užantspauduoti pagal bendrąsias taisykles.

Atliekant asmens sulaikymo su įkalčiais taktinę operaciją, būtina imtis visų įmanomų priemonių ir neleisti įtariamiesiems sunaikinti kompiuteryje esančios informacijos. Tai galima padaryti nedelsiant atitraukiant juos nuo kompiuterių.

Norint užtikrinti kompiuterinės įrangos ir joje esančios informacijos saugumą, galima taikyti vieną iš trijų saugumo užtikrinimo būdų:

1. paimti visą kompiuterinę įrangą;
2. kompiuterinę įrangą išjungti ir užantspauduoti;
3. kompiuterinę įrangą išjungti ir užtikrinti jos fizinę apsaugą.

Pirmuoju atveju, paimant kompiuterinę įrangą, reikia laikytis jau išvardytų taisyklių.

Antrasis ir trečiasis būdai taikomi, kai kompiuterinės įrangos paimti neįmanoma. Šioje situacijoje atlikus tardomąjį veiksmą, kompiuterinė įranga išjungiama ir užantspauduojama, patalpoje atjungiama elektra, o elektros skydelis užantspauduojamas. Trečiojoje situacijoje patalpos, kuriose yra kompiuteriai, saugomos policininko, kol bus atlikta ekspertizė arba tyrėjas duos kitą nurodymą.

Tiriant tokio pobūdžio nusikaltimus, gali būti atliekami tardomieji eksperimentai norint patikrinti, ar galima patekti į patalpas, kuriose yra kompiuterinė įranga, į kompiuterių tinklą, elektromagnetinio perėmimo galimybę, ar galima atlikti tam tikras operacijas su kompiuterine ir programine įranga ir pan.

Atliekant tyrimą taip pat skiriamos kompiuterinės įrangos [9, 4, 22], kompiuterinės spausdinimo įrangos [10, 64-75] bei programinės įrangos ekspertizės.

Išvados

Apibendrindami tai, kas parašyta, galime teigti, kad nusikaltimams, kuriems panaudojama kompiuterinė įranga, būdingi tam tikri ypatumai. Nusikaltėlio kriminalistinė charakteristika yra nevienareikšmė. Nusikaltimo padarymo būdai priklauso nuo turimos kompiuterinės ir programinės įrangos lygio. Tam tikri nusikaltimų padarymo būdų požymiai panašūs į bendruosius ekonominių nusikaltimų požymius. Tiriant sukčiavimus ir turtinės žalos padarymą apgaule arba piktnaudžiaujant pasitikėjimu, kuriems buvo panaudota kompiuterinė įranga, rekomenduojama laikytis taisyklių, apsaugančių kompiuterinę informaciją. Kompiuterinė įranga yra gana sudėtingas kriminalistinis objektas, kurį tiriant būtina panaudoti specialias žinias.

☞☞☞

LITERATŪRA

1. **Николаев К.** "Хакеры" и "кракеры" идут на смену медвежатникам? (обзор некоторых противоправных деяний, связанных с применением компьютерной техники) // http://www.fakt.ru/arhiv/num01/hackers.html.
2. Žr. **Pornografia** dziecięca w Internecie // Problemy kryminalistyki. Nr. 217. 1998. P. 76-79.; **Gramatyka M.** Piractwo komputerowe. Modus operandi // Problemy kryminalistyki Nr. 216. 1998. P. 11-18.; **Jakubski K. J.** Przestępczśc komputerowa – podział i definicja // Problemy kryminalistyki. Nr. 217. 1998. P. 31-38.; **Батурин Ю. М.** Проблемы компьютерного права. – М., 1991.; **Вехов В. Б.** Компьютерные преступления. Способы совершения. Методики расследования. – М., 1996; **Крылов В. В.** Информационные компьютерные преступления. Квалификация. Методика расследования. Основные нормативные акты. – М., 1997.
3. **Burda R., Gudmonas S.** Modernios technologijos – modernūs nusikaltimai. Nusikaltimų, kuriems naudojama kompiuterinė technika, kriminalistinis apibūdinimas ir tardomųjų veiksmų ypatumai // Justitia. 1998. Nr. 4.
4. **Arbušauskas R.** Policija dar nesidomi programų piratais // Laikinoji sostinė. 1998 12 17.

5. **Зеленин А.** Нокдаун хакеру // Милиция. № 7. 1999.
6. **Крылов В. В.** Информационные компьютерные преступления. Квалификация. Методика расследования. Основные нормативные акты. – М., 1997.
7. **Power R.** Curent and Future Danger: A CSI Primer on Computer Crime and Information Warfare. San Francisco, 1995.; Arlin Cooper J. Computer and Communication Security. N.Y., 1989.; Icover D., Seger K., Von W. Storch. Computer crime. JAV: O' Reilli Inc., 1995.
8. **Palskys E.** Kriminalistinis dokumentų tyrimas. – V., 1978.
9. **Teismo** ekspertizių skyrimo klausimai. Informacinis laiškas. – V., 1996.
10. **Deringas A., Rinkevičienė Z., Sakalauskas L.** Kompiuteriniais spausdintuvais išspausdintų dokumentų kriminalistinis tyrimas // Kriminalinė justicija: LTA mokslo darbai. – V., 1997. T. 7-8.

☞☞☞

Use of computer engineering in crimes against economy (some features criminal of the characteristic and technique of investigation)

R. Burda

Criminalistics Department, Law Academy of Lithuania

SUMMARY

Issues analysed under this article are related to usage of computer equipment for committing various crimes, criminal characterisation of such acts persons and peculiarities of interrogation acts.

Presumption can be made that as long as the Criminal Code does not directly indicate acts committed using computer equipment as crime, it may be asserted that computer crimes do not exist in Lithuania. Though it does not mean that such acts are not dangerous to society, state or individuals, and this is no longer a presumption but reality.

Persons that commit dangerous actions using computer equipment can be relatively divided into three groups: crackers, criminals and vandals. Different sources provide different definitions though they are all united by the same means of committing criminals acts – computer equipment and possible ways of using it.

Ways of using computer equipment are multiple and they are constantly improving and depend upon the level of hardware and software.

The most common acts of interrogation when computer equipment is examined and confiscated are following: examination of place of event, search of the place and seizure. General regulations are applicable to the acts of interrogation indicated above. One of them is calling for a computer (hardware and software) specialist. Other regulations are related to examination of computer equipment, its seizure and preserving information.