**Jurisprudencija, 1998, t. 9(1); 110-119**

# IV. TEISINĖ INFORMATIKA

## INFORMACINIØ TECHNOLOGIJØ TAIKYMAS TIRIANT NUSIKALTIMUS

**doc. dr. Rimantas Petrauskas,**
**doc. dr. Antanas Keras**

Ateities 20, Lietuvos teisės akademija, 2057 Vilnius
Telefonas 70 03 44
Elektroninis paštas: rpetraus@lpa.lt, keras@ktl.mii.lt

Spaudai pateikta 1998 m. vasario 9 d.

### S a n t r a u k a

Straipsnyje analizuojama naujø informaciniø technologijø taikymo tiriant nusikaltimus Lietuvoje praktika, galimybės ir perspektyvos. Šie klausimai Lietuvoje tik pradedami nagrinėti.

Aptariamas kriminalistinės informacijos sistemø efektyvumas. Didžiausias efektyvumas pasiekiamas, kai naujos technologijos diegiamos ten, kur būtina operatyviausia ir tiksliausia informacija. Lietuvoje šiuos klausimus padeda spręsti naujas tipinis rajonø policijos komisariatø programinės įrangos paketas TIRPAK. Jo kūrimą koordinavo Lietuvos teisės akademija.

Analizė parodė, kad kriminalistiniø informaciniø sistemø saugumo būklė turi įtakos bendram kriminalinės justicijos efektyvumui. Todėl straipsnyje nagrinėjamos kai kurios kriminalistinės kompiuterinės informacijos saugumo problemos, analizuojama informaciniø technologijø taikymo nusikaltimo srityje užsienio patirtis.

Aptartos kriminalistiniø žiniø kompiuteriniø baziø, kompiuterinio trijø matmenø nusikaltimo vietos modelio sudarymo galimybės, skaitmeniniø fotokamerø taikymas tiriant nusikaltimus.

Remiantis užsienio patirties analize, aptariamos informatikos nusikaltimø tyrimo Lietuvoje problemos.

Raktiniai žodžiai: informacinės technologijos, nusikaltimø tyrimas.

Nusikaltimø tyrimo pagrindą sudaro informaciniai procesai – informacijos rinkimas, išsaugojimas, apdorojimas, apibendrinimas, pateikimas. Šiuose informaciniuose procesuose naudojama kriminalistinės informacijos sistema. Informaciniø technologijø taikymas gali padėti tiriant nusikaltimus. Tačiau Lietuvoje šie klausimai iš esmės nenagrinėti. Todėl šio darbo tikslas – išanalizuoti naujø informaciniø technologijø taikymo tiriant nusikaltimus Lietuvoje praktiką, aptarti jø galimybes bei perspektyvas. Tyrimas atliktas taikant užsienio literatūros ir praktinės patirties mokslinės analizės metodą.

## Kriminalistinės informacijos sistemos efektyvumas

Analizuojant kriminalistikos laimėjimų taikymo Lietuvoje praktiką, tiriant bei rengiant darbo gerinimo pasiūlymus, reikėtø nustatyti, kokią įtaką kriminalistinės informacijos sistema turi bendram nusikaltimø tyrimo bei visos kriminalinės justicijos efektyvumui ir kokiais būdais galima jį padidinti. Šiuo tikslu buvo analizuojama literatūra ir užsienio šaliø patirtis. Tačiau literatūroje nebuvo rasta kiekybiškai aprašyto kriminalistinės informacijos sistemos parametrø ir visos kriminalinės justicijos sistemos efektyvumo ryšio.

Literatūroje [1, 2] nurodoma, kad tokios sudėtingos sistemos kaip kriminalinė justicija efektyvumui nustatyti reikia sudėtingos koeficientø sistemos. Kriminalinės justicijos efektyvumo tyrimas padėtø nustatyti ir įvertinti veiksnius, veikiančius visos sistemos efektyvumą. Būtina nustatyti kiekvieno veiksnio įtaką svarbiausiems tikslams pasiekti ir bendram efektyvumui didinti. Dar sunkiau nustatyti šiuo metu kuriamos ir sparčiai besikeičiančios kriminalistinės informacijos sistemos įtaką bendram nusikaltimø tyrimui ir visos kriminalinės justicijos efektyvumui.

Literatūroje [3, 131-154] aprašoma Vokietijos Šlezvigo-Holšteino žemėje kuriama kompiuterizuota policijos pareigūnø darbo vietø sistema. Pažymima, kad šiuolaikiniai kompiuteriai suteikia policijai anksčiau neįsivaizduojamas nusikaltimø tyrimo galimybes. 1988 metais šios Vokietijos žemės Vidaus reikalø ministerijos užsakymu konsultacinė firma atliko specialius tyrimus ir nustatė, kad informatikos ir ryšių technikos plėtra šalies policijai turi strateginæ reikšmæ. To priežastis – policijai vis sunkiau vykdyti užduotis dėl daugėjančių nusikaltimø, didėjančio nusikaltėliø profesionalumo bei augančio tarptautinio nusikalstamumo. Šias problemas spręsti toliau didinant personalą – netikslinga, o pareigūnø darbui efektyvinti reikia plačiai naudoti kompiuterinæ techniką. Šio projekto tikslas buvo suformuluotas taip: naudojant kompiuterinæ techniką, sudaryti pareigūnams sąlygas efektyviau atlikti darbo užduotis ir pasiekti geresniø darbo rezultatø. Siekiant greitesnio šiø tikslø įgyvendinimo, buvo numatyta kuo daugiau pareigūnø atlaisvinti nuo rutiniškos rašymo ir tvarkymo veiklos bei operatyviai pateikti jiems reikiamą tarnybinæ informaciją.

Kaip nurodoma minėtame šaltinyje, didžiausias efektyvumas pasiekiamas, kai kompiuteriai pirmiausia diegiami ten, kur jie gali atnešti didžiausią naudą tiriant nusikaltimus ir kur būtina tiksliausia ir operatyviausia informacija. Tai liečia visø pirma žemutines policijos grandis, kurios registruoja ir tiria daugiausia nusikaltimø. Tačiau kol kas neaišku, kuriose srityse ir kokiu mastu informatikos ir kompiuteriø taikymas pagerintø policijos ir visos kriminalinės justicijos užduočiø įvykdymą. Įgyvendinant šį projektą, pirmiausia buvo atlikta per metus sukurtø ir apdorotø dokumentø, raštø, telefoniniø ir kitokiø ryšių, įvykiø ir nusikaltimø skaičiaus analizė. Po to buvo atliktas pasirinktø pilotiniø darbo vietø (apie 10 % nuo bendro skaičiaus) visø darbo operacijø chronometražas. Per kelerius metus kompiuterizavus šias pilotines policijos darbo vietas, pasirodė, kad sumažėjo tarnybinėms užduotims atlikti reikalingø pareigūnø darbo sąnaudos.

Kriminalistinės informacijos sistemos efektyvumas priklauso nuo daugelio veiksniø – kompiuterinės technikos, programinės įrangos, ryšiø sistemos būklės, pareigūnø apmokymo, tinkamø informaciniø technologijø pasirinkimo ir pritaikymo nusikaltimø tyrimo reikmėms, tarnybiniø informaciniø mainø norminio pagrindimo, informacijos slaptumo ir apsaugos nuo nesankcionuoto panaudojimo užtikrinimo, optimalaus būtino laiko atskirø tarnybø užduotims atlikti pagrindimo ir kt. Tačiau kol kas neaišku, kurie iš šiø veiksniø svarbiausi ir kiek jie turi įtakos bendrø tikslø įgyvendinimui.~~*Aiðku*~~

Todėl tiriant Lietuvos nusikaltimø tyrimo sistemos efektyvinimo būdus, aktualu visø pirma išanalizuoti kriminalistinės informacijos sistemos būklæ rajonø policijos komisariatuose, kur registruojamas ir tiriamas didžiausias nusikaltimø skaičius. Tokią analizæ iki 1994 metø jau atliko autorius [4, 114-125].

~~Petrauskas R. Kompiuterinės technikos ir progaminės árangos bûklės Lietuvos policijos komisariatuose analizë ir jø vystymosi kryptys// Mokslo darbai. T.2 /Lietuvos policijos akad., V., 1994, p. 114-125.~~

1993 m. gale VRM paskelbë konkursà Informacinës sistemos modernizavimui. 1994 metais su užsienio specialistø pagalba buvo parengta Vidaus reikalø ministerijos Integrinės kompiuterizuotos informacinės sistemos (IKIS) techninė užduotis. Joje buvo numatyta, kad IKIS susidës ið 7 posistemiø, ið kuriø IKIS2 skirta nusikaltimø tyrimui. IKIS kûrimas ir diegimas projekte buvo numatytas nuo 1995 iki 2000 m. Visai sistemai sukurti buvo numatyta nuo 180 iki 230 milijonø litø lëðø, t.y. po 25-50 milijonø litø metams. Pagal ðià techninæ uþduotá nusikaltimø tyrimo posistemës IKIS2 diegimas buvo numatytas tik 1998-1999 m. Taèiau ávertinant, kad respublikos biudþetas gali bûti nepajëgus laiku skirti tokiø dideliø lëðø VRM informacinei sistemai, galima laukti, kad nusikaltimø tyrimo posistemës IKIS2 diegimas uþsitæs bent 2-5 metus ir baigsis ne anksèiau 2001-2004 m. Pati techninė užduotis buvo daugiau orientuota į vertikalios Vidaus reikalø ministerijos informacinės infrastruktūros kūrimą (pačios ministerijos, jos departamentø centralizuotos informacijos ir ataskaitø poreikiø tenkinimas), joje mažai buvo atsižvelgta į horizontalią policijos infrastruktūrą – žemutines nusikaltimø tyrimo grandis rajonø policijos komisariatuose. Analizė parodė, kad IKIS kūrimo biudžete visai nebuvo numatyta lėšø informacinėms struktūroms palaikyti IKIS kūrimo ir diegimo laikotarpiu, kas visai nepriimtina norint užtikrinti bûtinà nuolatinį ir nenutrūkstamą nusikaltimø tyrimo procesą. 1994 metais Lietuvos policijos akademijos ekspertai nurodė, kad atsižvelgiant į esančios Vidaus reikalø ministerijos informacinės sistemos palaikymo būtinybæ ir finansinius išteklius, kuriuos Lietuva galės skirti IKIS projektui, reikia ieškoti moksliškai pagrįstø racionaliø sprendimø ir kurti IKIS dalinio finansavimo sąlygomis, kai visø pirma kompiuterizuojamos darbo vietos ir tokie darbai, kuriems sugaištama daugiausia darbo, laiko bei kurie duoda geriausius rezultatus.

Atlikdama kriminalistinės informacijos sistemos efektyvinimo tyrimus, Lietuvos policijos akademijos Informatikos ir komunikacijø katedra 1994-1996 metais 48 rajonø policijos komisariatuose atliko anketinæ analizæ. Ji parodė, kad policijos komisariatuose naudojama daug skirtingø vietiniø kompiuteriniø duomenø baziø. *Komisarai paþymëjo, kad nusikaltimø tyrimà pagerins:*

*operatyvinës bei darbinës kriminalistinës informacijos kaupimas kompiuterizuotose kriminalistinëse kartotekose,*

*nusikaltimø tyrimo dokumentø ruoðimas kompiuteriu,*

*kriminalistinës informacijos sisteminimas kompiuteriu bei tokios informacijos apsauga,*

*naujø informaciniø technologijø pritaikymas nusikaltimø tyrime (pvz., skaitmeninis fotografavimas),*

*pradinio nusikaltimø tyrimo etapo kompiuterizavimas,*

*visø kriminalistø apmokymas panaudoti kompiuterius ir informacines technologijas nusikaltimø tyrime.*

*Kartu pasiûlyta ávykiø, nusikaltimø, pareiðkimø ir skundø registravimà komisariate kompiuterizuoti, atsisakant neproduktyvios rankinës registracijos. Analizuojant komisariatø darbà, paaiðkëjo, kad policijai kyla sunkumø registruojant ávykius trijose skirtingose registracijos knygose. Iðanalizavus Vokietijos ir Ðvedijos policijos patirtá, buvo rekomenduota komisariatuose atsisakyti trijø registracijos knygø, visus ávykius registruoti vienoje kompiuterinëje duomenø bazëje.*

Apibendrinus policijos komisariatø nuomonæ apie svarbiausiø kriminalistinės informacinės sistemos plėtimo darbø prioritetus bei praktinius poreikius, 1995 metais buvo suformuluota ir pateikta Vidaus reikalø ministerijos Informacijos ir ryšiø departamentui rekomendacija sukurti tipinį rajonø policijos komisariatø programinės įrangos paketą, tenkinantį minimalias informacines komisariato reikmes. Realizuodama šią rekomendaciją, Vidaus reikalø ministerija 1995 metais vasarą pradėjo kurti realizuoti tipinį policijos komisariato programinės įrangos paketpagrindimo, o nuo 1996 m. – ir ą. Šiuos darbus koordinavo Lietuvos teisės akademijos Informatikos ir komunikacijø katedra. 1997 metø viduryje toks paketas, pavadintas TIRPAK, buvo sukurtas ir išbandytas 4 komisariatuose. Nuo 1998 metø šis tipinis programinės įrangos paketas rekomenduotas diegti visuose rajonø

policijos komisariatuose. Visuotinai įdiegus šį paketą, galima laukti Lietuvos kriminalistinės informacijos sistemos efektyvumo padidėjimo.

### Kriminalistinės informacijos apsauga

Užsienio patirties ir literatūros analizė parodė, kad kriminalistiniø informacijos sistemø informacijos saugumas turi įtakos bendram kriminalinės justicijos efektyvumui. Kompiuterizavus kriminalinės justicijos sistemą, pagerėja nusikaltimø tyrimas. Tačiau kartu padidėja informacijos saugumo svarba. Pasaulinė ir šalies praktika parodė, kad nusikaltėliai gali truputį (pakeisdami atskiro nusikaltėlio ar nusikaltimo duomenis) ar net gerokai (įvesdami kompiuterinius virusus į informacinæ sistemą) pabloginti bendrą kriminalinės justicijos efektyvumą. Todėl trumpai panagrinėkime kriminalinės kompiuterinės informacijos saugumo problemas [5].

Kiekvienoje kompiuterinėje sistemoje informacijos apsaugos požiūriu silpniausia, o kartu ir didžiausią grėsmæ kelianti grandis yra žmogus. Vieni žmonės paprasčiausiai neapmokyti dirbti kompiuteriu: jie netyčia gali sunaikinti svarbią informaciją, esančią kompiuteryje, ar trukdyti sistemos darbui. Kiti gali tyčia pažeisti kompiuterio vartojimo taisykles, panaudoti kompiuterinæ sistemą asmeniniams reikalams ~~ar malonumams~~. Treti – tai nusikaltėliai, kurie vagia ar keičia informaciją bei~~ar~~ naikina kompiuterinæ įrangą. Pavojø kompiuteriams ir juose laikomai informacijai kelia ir vartotojai naujokai, nepatenkinti darbuotojai bei profesionalūs nusikaltėliai ar užsienio žvalgybø agentai.

Grėsmė, kurią bet koks asmuo gali sukelti kompiuterinei sistemai, priklauso nuo keliø sąlygø [5]:

- priėjimo prie informacinės sistemos rūšies;
- grėsmės informacinei sistemai lygio;
- asmens motyvacijos.

**Priėjimo prie informacinės sistemos rūšys.** Žala, kurią asmuo gali padaryti informacinei sistemai, didžia dalimi priklauso nuo priėjimo prie kompiuterinės sistemos rūšies. Svarbu žinoti, ar vartotojai turi priėjimą tik prie terminalo, ar ir prie pagrindinio kompiuterio (pastarasis atvejis daug pavojingesnis). ~~Jei vartotojai turi priėjimà ir prie pagrindinio kompiuterio, tai grësmës dydis þymiai iðauga.~~ Be to ~~ûtina þinoti, kad~~, ~~-~~sistemą galima pažeisti ~~ne tik ið terminalo, bet~~ ir iš kitos kompiuterinės sistemos per kompiuterių tinklą: galima užkrėsti virusu, fiziškai pažeisti sistemą ar pavogti informaciją.

Labai svarbu riboti priėjimą prie sistemos, leisti naudotis tik ta informacija, kuri būtina tarnybinėms užduotims sėkmingai atlikti. Apribojant priėjimą, galima ne tik apsisaugoti nuo vagystės, kenkimo ar išlaikyti svarbios informacijos slaptumą, bet ir apsaugoti darbuotojus nuo atsitiktinio informacijos sunaikinimo ar didesnės žalos padarymo.

**Grėsmės informacinei sistemai lygis.** Norint užprogramuoti virusą arba tyčia jį įvesti, būtinos neeilinės informatikos žinios, kuriø dauguma paprastø tarnautojø neturi. Informacinės sistemos administratorius ar programuotojas gali įvesti virusą ar kitą užprogramuotą grėsmæ, kuri ateityje gali sunaikinti visą informacinæ sistemą ar dalį jos informacijos.

Kita vertus, nežinojimas, nemokšiškumas gali stipriai pažeisti sistemą. Pvz., darbuotojas, kuris neturi pakankamai žiniø ir netikrina antivirusinėmis programomis diskeliø, kuriuos naudoja ne tik darbe, kelia grėsmæ visos informacinės sistemos saugumui. Labai pavojingi ir kompiuteriniai žaidimai darbo vietoje. Jie yra dažniausia kompiuteriø užsikrėtimo ~~kompiuteriniais~~ virusais priežastis.

**Asmens motyvacija.** Darbuotojai, kurie mėgsta savo darbą, specialiai negadins informacinės sistemos. Kita vertus, kuo nors nepatenkinti darbuotojai (negavo premijos, nebuvo paaukštinti ar gavo papeikimą už blogą darbą, gresia atleidimas) gali kelti tam tikrą grėsmæ organizacijai.

~~Apmokymas ir atsakomybë.~~ Darbuotojus reikia apmokyti dirbti su kompiuterine sistema. Jie turi būti atsakingi už ją. Visø pirma reikia apmokyti darbuotojus atlikti pagrindines sistemos operacijas. Ne visi saugumo pažeidimai yra tyčiniai, daug jø padaroma dėl paprastø žmogiškø klaidø. Darbuotojai, kurie dirba nerūpestingai ar yra neapmokyti, gali neteisingai įvesti svarbią informaciją ar suklysti perduodami ar pateikdami ją. Darbuotojai turi

žinoti, kad jie atsakingi už savo veiksmus ir kompiuterinės įrangos panaudojimą (terminalai, kompiuterinės bylos, slaptažodžiai). Jie turi suprasti, kad atsako ne vien už techniką, bet ir už jos apsaugą nuo pašaliniø įsikišimo, ir jei bus nustatytas taisykliø pažeidimas, atsakingas už tai asmuo gali būti patrauktas atsakomybėn.~~Net jei darbuotojas teisinsis, kad kaþkas pavogë jo slaptaþodá ar naudojosi jo terminalu kai jis pietavo, vis vien iðliks tam tikras jo atsakomybës laipsnis.~~

LabaiYpaè svarbu ~~labai ap~~riboti priėjimą prie ypač svarbios informacijos ir atsakingø informacinės sistemos vietø, ypač prie pagrindinio kompiuterio. Kai darbuotojas išeina iš darbo, netgi savo noru, būtina pakeisti visus slaptažodžius, su kuriais jis dirbo, ypač jei darbuotojas ėjo privilegijuoto vartotojo pareigas. Kartu reikia patikrinti darbuotojo paliktas kompiuterines bylas ir prireikus jas išsaugoti kitais vardais, kad būtø galima panaudoti ateityje.

## Naujø informaciniø technologijø taikymas tiriant nusikaltimus

Labai svarbu atlikti mokslinius naujø informaciniø technologijø taikymo kriminalistikoje galimybiø tyrimus, kurti ir diegti kriminalistikoje naujausias informacines technologijas, kurios padėtų spręsti nusikalstamumo ir nusikaltimø prevencijos problemas. Tam reikia išanalizuoti užsienio informaciniø technologijø taikymo patirtį, tirti informaciniø technologijø taikymo tiriant nusikaltimus galimybes.

Išanalizavus naujø informaciniø technologijø taikymo tiriant nusikaltimus užsienio patirtį, buvo atkreiptas dėmesys į kelias taikymo galimybes.

**Kompiuterinės kriminalistinės žiniø bazės.** Didžiąją daugumą kriminalinės justicijos uždaviniø pagal sprendimo būdus ir sudėtingumą galima suskirstyti į probleminius ir tipinius.

Tipiniuose kriminalinės justicijos uždaviniuose pakanka pradiniø duomenø kokybinei ir kiekybinei uždavinio analizei. Tokiø uždaviniø sprendimą galima automatizuoti sudarant tipinius sprendimo algoritmus.

Probleminiuose uždaviniuose nepakanka informacijos duomenø kiekybiniø charakteristikø analizei. Tokie uždaviniai sprendžiami kūrybiškai, vadovaujantis intuicija, taikant įvairius euristinius sprendimus. ŧTačiau sprendimo veiksmingumas gali būti labai nevienodaįs. ~~efektyviai, naudojami ávairûs euristiniai sprendimai~~Tokiø uždaviniø sprendimo būdą lemia patirtis, žinios, jø sisteminimas, apibendrinimas, sprendimø formalizavimas, algoritmo sudarymas. Šiam tikslui ~~sëkmingai uþdaviniø sprendimui g~~gali būti panaudotos ekspertinės dirbtinio intelekto sistemos. Ekspertinės sistemos – tai jau ne duomenø, o žiniø bazės. Todėl į ekspertines sistemas įeina ne tik duomenø, faktø rinkiniai, bet ir taisyklės, kaip, remiantis duomenimis, gauti teisingus sprendimus. Šios euristinės taisyklės sudaromos remiantis keliø ar keliolikos konkrečios srities geriausiø specialistø patirtimi. Pagal specialiai parengtas kompiuterines programas visos įvestos žinios apdorojamos. Remiantis jomis, įvedus konkrečią informaciją apie nusikaltimą, pasiūlomas vienas ar keli tikėtiniausi sprendimai. Tinkamiausią sprendimo variantą pasirenka su sistema dirbantis specialistas. Labai svarbu, kad JAV, Vokietijoje, Olandijoje, Anglijos ir kitose šalyse teisės sistemai kuriama keliolika kompiuteriniø žiniø baziø [6]. Paprastesni tokiø žiniø baziø variantai naudojami kaip “intelektualūs patarėjai” ir gali būti sėkmingai panaudoti praktiniame tardytojo darbe analizuojant ir parenkant galimus sprendimus. Šiam tikslui reikia pradėti lietuviškø kriminalistiniø žiniø baziø kūrimo darbus.

Kompiuterinis trijø matmenø nusikaltimo vietos modelio sudarymas aprašytas literatūroje [7]. Šiam tikslui įvykio vietoje iš skirtingø taškø padaromos ir įvedamos į kompiuterį 2-4 nuotraukos. Keitikliu pažymėjus tuos pačius atraminius taškus skirtingose nuotraukose ir panaudojus specializuotą programinæ įrangą, sukuriamas kompiuterinis įvykio vietos trijø matmenø paviršiaus modelis. Tiriant nusikaltimą naudojant šį modelį, kompiuteriu galima tiksliai išmatuoti atstumus tarp bet kuriø įvykio vietos taškø, atspausdinti bet kokius įvykio vietos vaizdus, pjūvius ar projekcijas. Nuo 1994 metø šią informacinæ technologiją svarbiems nusikaltimams tirti diegia federalinė Vokietijos policija. ~~Siekiant ávertinti ðiø~~

~~informaciniø technologijø panaudojimo Lietuvoje ðiuo metu tikslingumà buvo apklausti 5 kriminalistikos specialistai.~~

Tačiau aAparatūros komplektas kompiuterinio trijø matmenø nusikaltimo vietos erdvės modeliui sudaryti kainuoja gana brangiai – apie 8-15 tūkstančiø markiø. Didesnė šios technologijos nauda tik tiriant labai sudėtingus nusikaltimus. Įvertinant tai, kad kol kas kriminalistams Lietuvoje trūksta ir daug paprastesnės bei pigesnės technikos, kol kas nerekomenduotina Lietuvoje diegti šią informacinæ technologiją ir pirkti jai aparatūrą.

**Skaitmeninis fotografavimas.** Kita informaciniø technologijø taikymo kryptis yra nusikaltimo vietos vaizdo digitalizavimas ir saugojimas kompiuterio atmintyje. Tai galima atlikti dviem būdais:

– fotoaparatais, fiksuojančiais vaizdą ant magnetiniø informacijos atmintiniø,

– vaizdo kameromis, naudojant skaitmeninius signalo keitiklius.

Pirmuoju atveju aparatu daroma iki 12-24 nuotraukø [8]. Prijungus skaitmeninį fotoaparatą kabeliu prie kompiuterio, nuotraukø vaizdai perrašomi į kompiuterio magnetinį diską. Naudojantis kompiuteriu, nuotraukas galima peržiūrėti, tvarkyti, analizuoti, spausdinti spausdintuvais, perduoti kompiuterinio ryšio kanalais. Fotoaparato atmintinė gali būti išvalyta bet kuriuo metu. Kai kurie aparatai turi skystø kristalø ekranus kadrams peržiūrėti fotografavimo vietoje bei papildomas keičiamas magnetines korteles.

Antruoju atveju gauti vaizdo kameros vaizdai ar atskiri kadrai iš pradžiø digitalizuojami, po to užrašomi į kompiuterio magnetinį diską. Šios informacinės technologijos naudojamos JAV, Olandijos, Vengrijos ir kitø šaliø policijoje.

Abiejø informaciniø technologijø pranešimai yra:

– prireikus galima labai greitai (praktiškai per kelias minutes) atspausdinti įvykio vietoje padarytas nuotraukas;
– telefono ar radijo ryšiu per kelias minutes įvykio vietoje padarytas nuotraukas galima persiøsti į rajono centrą ar ministeriją;
– panaudojant specialią programinæ įrangą, galima greitai atpažinti kompiuterinius vaizdus (pirštø, batø, padangø ir kt. pėdsakø, rašysenos);
– išnaudojant didelæ vaizdo kamerø skiriamąją gebą, įvykio vietoje galima naudoti iki 1500 kartø didinantį kompiuterinį mikroskopą;
– išnaudojant kompiuterio galimybes, įvykio vietoje galima palyginti du vaizdus ir spalvinį filtravimą.

Tiriant nusikaltimus, skaitmenines fotokameras galima panaudoti:

– sulaikytiems asmenims ir nusikaltėliams fotografuoti;
– nusikaltimo, įvykio vietai dokumentuoti;
– teismo ekspertizei.

Skaitmeninėmis fotokameromis galima labai operatyviai fiksuoti nusikaltėliø bei įtariamøjø portretus ir nusikaltimo vietos fotografijas ir išsaugoti juos kompiuterio magnetiniame diske. Kartu labai paspartėja reikiamø portretø bei nuotraukø paieška kompiuterinėje kartotekoje. Tokios skaitmeninės fotokameros nuo 1995 metø buvo įdiegtos Šiauliø m. policijos komisariatuose ir labai pasiteisino. Paruošus programinæ įrangą, kompiuteriniu fotoaparatu buvo pradėti fotografuoti įtariamieji ir nusikaltėliai. Tekstinėje duomenø bazėje prie tokio asmens duomenø pridedama pastaba, kad duomenø banke yra saugoma ir nusikaltėlio nuotrauka. Šiuo metu Šiauliø VPK kompiuteryje jau sukaupta daugiau kaip 800 tokiø nuotraukø. Policijos darbas tapo operatyvesnis, lengviau identifikuoti sulaikytus asmenis. Šiuo metu tokias skaitmenines fotokameras galima rekomenduoti diegti kitiems komisariatams.

## Informatikos nusikaltimø tyrimo problemos

Šiandien greta tradiciniø nusikaltimø atsiranda ir naujø, susijusiø su šiuolaikinėmis informacinėmis technologijomis ir naujais mokslo laimėjimais. Šiuo metu sparčiai besivystančios informacinės technologijos taikomos praktiškai visose žmonijos veiklos srityse. Paskutinius dešimtmečius daugybė finansinės, karinės ir kitokios informacijos, specifiniai biznio duomenys ir netgi informacija apie asmeninius ryšius yra saugoma kompiuteriuose ir perduodama kompiuteriø tinklais. Bankai kompiuteriø tinklais per dieną perveda trilijonus do-

leriø. Visa ši perduodama informacija nėra patikimai apsaugota nuo pasikėsinimø. Sparčiai plėtojantis informacinėms technologijoms, atsirado ir nemažą žalą padaro naujo tipo nusikaltimai naudojant kompiuterius ir kompiuteriø tinklus.

Su kompiuteriais susijæ nusikaltimai (angl. – *Computer crime* arba *computer related crime*) yra nauja ir palyginti mažai tyrinėta sritis. Šio tipo nusikaltimus apibrėžiantys terminai dar nėra galutinai nusistovėjæ nei užsienio šalyse, nei Lietuvoje. Remiantis literatūra [9], tokiais nusikaltimais galima laikyti visas tyčines veikas, vienaip ar kitaip susijusias su kompiuteriais, informatikos ar tolimųjų ryšių sistemomis, kai nukentėjæs asmuo patyrė ar galėjo patirti žalą, o nusikaltimo subjektas turėjo ar galėjo turėti iš to naudos. Mes toliau vartosime terminą “informatikos nusikaltimai”, nors ateityje jis ir gali keistis.

Niekas nežino tikslaus kompiuteriniø nusikaltėliø skaičiaus, bet yra informacijos, jog tokiø nusikaltimø padaroma žala siekia milijardus doleriø. Tokiø nusikaltimø jau esama ir Lietuvoje. Prieš kiek laiko Lietuvos televizija paminėjo faktą, kad iš vieno valstybinio registro – šiuolaikinio duomenø banko – pavogtas naujas galingas kompiuteris ir jame sukaupti duomenys apie grąžinamą nuosavybæ. Tiesioginiai nuostoliai dėl informacijos praradimo vertinami maždaug dviem milijonais litø. Dar apie pusæ milijono litø kainuoja pats kompiuteris. Be to, ~~privati~~slapta ~~asmenis liečianti (privati)~~ informacija apie grąžinamą nuosavybæ pateko į nusikalstamo pasaulio rankas ir gali būti panaudota šantažui, reketavimui bei kitoms nusikalstamoms veikoms.

Informatikos nusikaltimams būdinga, kad oficialioji teisėsaugos organø statistika neatspindi tikros padėties. Literatūroje [9] nurodoma, kad nukentėjæ asmenys kreipiasi į teisėsaugos organus vos dėl 5 proc. padarytø informatikos nusikaltimø. Tokia pat ir FBI Nacionaliniø kompiuteriniø nusikaltimø tyrimø grupės nuomonė, kad 85-97 proc. kompiuteriniø nusikaltimø neiškyla į viešumą. Neseniai, atliekant JAV Gynybos departamento finansuotus tyrimus [10], buvo bandoma įsibrauti į 8932 informacines sistemas. 7860 įsibrovimø buvo sėkmingi. Tik 390 sistemø vadybininkai (iš minėtø 7860) užfiksavo įsibrovimą į sistemą ir tik 19 iš jø pranešė apie įsibrovimą. Apie pastebėtus įsibrovimus į sistemą ar kompiuterį paprastai nepranešama todėl, kad organizacijos dažnai bijo, jog jø darbuotojai, klientai ir akcininkai praras pasitikėjimą, jeigu sužinos, kad į firmos kompiuterį buvo įsibrauta, kad neužtikrinama informacijos apsauga.

Kadangi pastaraisiais metais kompiuteriai ir kompiuteriø tinklai Lietuvoje plačiai paplito, analizuojant užsienio šaliø patirtį, artimiausiu metu galima laukti vienaip ar kitaip su kompiuteriais susijusiø nusikaltimø skaičiaus ryškaus padidėjimo. Pavyzdžiui, Olandijoje nuo 1986 metø per 6 metus tokiø nusikaltimø skaičius išaugo nuo 1-2 iki daugiau kaip 400 per metus. Tačiau, nagrinėjant tokius nusikaltimus, kyla įvairiø teisiniø, kriminalistiniø, techniniø ir kt. problemø. Kadangi viena iš ypatingø tokiø nusikaltimø savybiø yra tarptautinai informaciniai ryšiai, visø pirma panaudojant kompiuteriø tinklus, tiriant informatikos nusikaltimus dažnai kyla daugybė sunkumø, su kuriais iki tol nebuvo susiduriama tiriant kitokius nusikaltimus: nukentėjæs gali būti vienoje šalyje, o nusikaltėlis – visai kitoje. Pavyzdžiui, Rusijos pilietis, neišvykdamas iš Peterburgo, apiplėšė JAV esantį banką. Padaryta apie milijono doleriø žala. Ryšium su staigiu informatikos nusikaltimø skaičiaus didėjimu Olandijoje, Anglijoje, Japonijoje, JAV ir kitose šalyse sukurti specializuoti teisėsaugos darbuotojø kolektyvai, kurie užsiima tokiø nusikaltimø problemomis.

Kaip nurodyta literatūroje [11], Europos Tarybos Ministrø kabinetas 1989 metais priėmė rekomendaciją R 89(9) ET šaliø vyriausybėms, kurioje siūlo peržiūrint ar kuriant įstatymus atsižvelgti į Europos komiteto nusikaltimø problemoms tirti pranešimą apie su kompiuteriais susijusius nusikaltimus. Šiame pranešime pateikiami du su tokiais nusikaltimais susijusiø veikø sąrašai. Europos Tarybos nariams leidžiama savarankiškai spręsti, kaip ir kiek pasinaudoti šiuo pasiūlymu. Minimaliame sąraše išvardytos 8 pavojingesnės veikos. Papildomas sąrašas apima keturias mažiau pavojingas veikas, kurios įtraukiamos į leidžiamus įstatymus, bet nėra privalomos. Žemiau pateikiame šiuos sąrašus.

Minimalus sąrašas (būtinas suvienodinant ET šaliø kriminalinæ politiką, susijusią su kompiuteriniais nusikaltimais):

1. Sukčiavimas, susijæs su kompiuteriais (*Computer-related fraud*).
2. Kompiuterinė klastotė (*Computer forgery*).

3. Kompiuteriniø duomenø ar programø sunaikinimas ar sugadinimas (*Damage to computer data or computer programs).*
4. Kompiuterinis sabotažas (*Computer sabotage*).
5. Neleistinas įsibrovimas į kompiuterinæ sistemą ar kompiuterių tinklą (*Unauthorised access*).
6. Neleistinas informacijos nuskaitymas (*Unauthorised interception*).
7. Neleistinas apsaugotos kompiuterinės programos atkūrimas (*Unauthorised reproduction of a protected computer program).*
8. Neleistinas integrinės mikroschemos topografijos atkūrimas (*Unauthorised reproduction of a topography).*

Papildomas sąrašas:

1. Kompiuteriniø duomenø ar kompiuteriniø programø pakeitimas *(Alteration of computer data or computer programs).*
2. Kompiuterinis šnipinėjimas (*Computer espionage*).
3. Neleistinas kompiuterio panaudojimas (*Unauthorised use of computer*).
4. Neleistinas apsaugotos kompiuterinės programos panaudojimas (*Unauthorised use of a protected computer program*).

Į šias rekomendacijas būtina atsižvelgti ir Lietuvoje.

Vykdant šį mokslinį darbą, buvo atlikta Europos šalių literatūros ir įstatymø, liečiančiø kompiuterinius nusikaltimus, analizė [12; 13; 14; 15]. Šios analizės pagrindu suformuluoti pasiūlymai buvo perduoti naujojo Lietuvos baudžiamojo kodekso rengimo grupei. Buvo analizuojami Baudžiamojo kodekso naujo skyriaus "Nusikaltimaiø informacijos saugumui (nusikaltimaiø informatikai)" ~~skyriaus~~ įvairūs variantai, siūlomi pakeitimai. Lietuvos Respublikos baudžiamojo kodekso projektas, kuriame pirmą kartą numatoma atsakomybė už nusikaltimus informacijos saugumui (nusikaltimus informatikai) buvo paskelbtas Valstybės žiniose, 1996 m. Nr. 117 [16, 61-62].

Toliau aptarsime kai kuriuos informatikos nusikaltimø tyrimo ypatumus.

**Kompiuteriniø nusikaltimø tyrimas.** Kompiuteriniø nusikaltimø tyrimas paprastai yra sudėtingesnis nei kitø nusikaltimø tipø tyrimas. Jis reikalauja specialaus techninio pasirengimo ir labai priklauso nuo specialisto, liudytojo parodymø. Kompiuteriniø nusikaltimø tyrimas turi paaiškinti labai sudėtingus techninius veiksmus teisėjams, nes jie paprastai mažai žino apie kompiuterius bei jø veikimą. Liudytojams gali reikėti paaiškinti, kodėl neteisėtas informacijos perrašymas ar nesankcionuotas pasinaudojimas programine įranga ar kompiuterine sistema yra ne mažiau svarbus, o kartais net svarbesnis negu materialiø daiktø vagystė ar kiti panašūs nusikaltimai. Kuo sudėtingesnis informatikos nusikaltimas, tuo sunkiau jį ištirti ir bylą pateikti teismui.

**Kompiuteriniø įkalčiø problema.** Tiriant informatikos nusikaltimus, daug įkalčiø yra kompiuterinėje informacijoje. Tokiø įkalčiø pasitaiko ir tiriant įprastus nusikaltimus, kai naudojami skaitmeniniai fotoaparatai ar, pvz., magnetinio diskelio informacija. Visa ši informacija yra skaitmeninė ir gali būti nesunkiai pakeista kompiuteriniais įrenginiais, todėl labai aktuali įkalčiø autentiškumo problema.

Ryšium su tuo 1991 metais JAV Federalinio kompiuteriniø kriminaliniø tyrimø komiteto posėdyje buvo atliktas teismo eksperimentas [5]. Komitetą įsteigė keletas federaliniø ir valstybės įstatymø priežiūros įstaigø darbuotojø, kurie vieni pirmøjø įvertino naujø atsirandančiø technologijø nusikaltėliams teikiamas galimybes ir naujas įstatymø priežiūros pareigūnams iškylančias problemas. Eksperimento metu buvo pademonstruota, kad standartiniu kompiuteriu galima lengvai ~~iš esmės~~ pakeisti tai, kas pavaizduota kompiuterinėje nuotraukoje, taigi faktiškai falsifikuoti įkalčius.

~~*Agentams ir prokurorams buvo parodyta nuotrauka kûno, susirietusio ant grindø, su krûtinėje þiojėjanèia þaizda. Kitoje kambario pusėje ant grindø gulėjo didelis pistoletas. Ant balto sienos virð aukos kûno aukos krauju uþraðyti þodþiai "Að vël þudysiu. Jûs niekada manæs nesugausite."*~~

~~*Taèiau ði nuotrauka, skirtingai nuo áprastiniø nuotraukø, sukurta ne filmavimo kamera, o skaitmeniniu fotoaparatu. Visas vaizdas buvo sudarytas ið dvejetainiø skaièiø, vienetø ir nuliø, kurie gali bûti pakeisti be pëdsako. Tada du teismo agentai, panaudodami komercinæ*~~

~~programinæ árangà, pradëjo keisti skaièius. Jie "nuvalë" sienà, panaikindami kruvinus bodþius. Po to uþdarë þaizdà krûtinëje, vietoj to palikdami ið aukos smilkinio tekanèià kraujos srovelæ. Galiausiai jie ádëjo ginklà á aukos rankà. Tokiu bûdu byla bûtø iðspræsta: raporte áraðyta, kad auka nusiþudë, o nuotrauka tai "árodys". Ðios demonstracijos tikslas buvo akivaizdus: ne tik negalima pasitikëti áprastinëmis fotografijomis, kuriø patikimumas nustatytas senu bûdu, taèiau ir bet kuris agentas gali bûti apkvailintas, jeigu jis arba ji nëra pakankamai gerai susipaþinæ su naujom informacinëm technologijom ir negali ávertinti sudëtingø skaitmeniniø pakeitimø galimybës. Esmë ta, kad nëra negatyvo, o pakeitimai atliekami be jokiø pëdsakø.~~

Autentiškumo problemos neapsiriboja vien kompiuterinėmis nuotraukomis. Pavyzdžiui, kai kurios paketø pristatymo tarnybos šiuo metu leidžia klientams pasirašyti už gautus paketus rankiniame aparatėlyje, kuris sukuria skaitmeninæ gavėjo parašo kopiją. Tokiu atveju lengva perduoti informaciją į kompiuterį, tačiau galima kompiuteriu atkurti parašą. Jeigu minėtas rankinis aparatas išmatuoja ir įrašo pasirašiusiojo rašiklio prispaudimo lygį, ir kompiuteris atgamina parašą rašaliniu spausdintuvu, kompiuterinė kopija atrodys absoliučiai autentiška net ir pačiam parašo autoriui.

Nepaisant pateiktø pavyzdžiø, daugeliu atvejø elektroniniai įrodymai – nuotraukos ar dokumentai – iš tikrøjø gali būti identifikuojami remiantis skiriamosiomis charakteristikomis ir gali būti veiksmingai panaudoti kriminalistikoje. Įvykio liudytojas gali taip pat lengvai identifikuoti skaitmeninæ asmens fotografiją kaip ir įprastinæ nuotrauką. Teismui turi būti svarbus liudytojo sugebėjimas tiksliai pastebėti ir atsiminti asmenį, nuotrauką, vaizdą ar dokumentą, kurį jis gali palyginti su teismo turimu variantu ir pan. Tačiau tai yra nauja, dar nepakankamai ištirta sritis, kurią neabejotinai būtina tirti.

LietuvojeTodël kompiuteriniø įkalčiø autentiškumo problema taip pat yra labai aktuali ir todėlreikia šia kryptimi reikėtø pradėti rimtus tyrimus.

## Išvados

1. Nusikaltimø tyrimo veiksmingumas priklauso nuo kriminalistinės informacijos sistemos efektyvumo. Augant nusikaltimø skaičiui, didėjant nusikaltėliø profesionalumui ir tarptautiniam nusikalstamumui, pareigūnø darbui efektyvinti tikslinga plačiai naudoti kompiuterinæ techniką.
2. Norint operatyviai ištirti nusikaltimus, svarbu turėti išsamią, teisingą, greit pasiekiamą kriminalistinæ informaciją apie anksčiau padarytus nusikaltimus bei su jais susijusius asmenis ir daiktus. Didžiausias efektyvumas pasiekiamas, kai pirmiausia kompiuteriai diegiami rajoninėse policijos grandyse, kurios registruoja ir tiria daugiausia nusikaltimø ir kur būtiniausia operatyviausia informacija. Kriminalistinės informacijos sistemos efektyvumas priklauso nuo daugelio veiksniø – kompiuterinės technikos, programinės įrangos, ryšiø sistemos būklės, pareigūnø apmokymo, tinkamø informaciniø technologijø pasirinkimo ir pritaikymo nusikaltimø tyrimo reikmėms, tarnybiniø informaciniø mainø norminio pagrindimo, informacijos slaptumo ir apsaugos nuo nesankcionuoto panaudojimo užtikrinimo ir kt. Būtina toliau tæsti šios srities tyrimus Lietuvoje.
3. Tipinio rajonų policijos komisariatų programinės įrangos paketo TIRPAK įdiegimas padidins Lietuvos kriminalistinės informacijos sistemos veiksmingumą ir leis komisariatams keistis kriminalistine informacija tarpusavyje.
4. Nepakankama kriminalinės justicijos informaciniø sistemø informacijos saugumo būklė gali daugiau ar mažiau pabloginti bendrą kriminalinės justicijos efektyvumą. Todėl kuriant tokias informacines sistemas ir jas naudojant būtina imtis specialiø priemoniø kriminalistinės informacijos saugumui užtikrinti.
5. Kompiuterinės kriminalistiniø žiniø bazės gali būti sėkmingai panaudotos tardytojo darbe analizuojant ir parenkant galimus sprendimus. Šiam tikslui reikia pradėti lietuviškø kompiuteriniø kriminalistiniø žiniø baziø kūrimo darbus.
6. Skaitmeninės fotokameros leidžia labai operatyviai fiksuoti nusikaltėliø bei įtariamøjø portretus ir nusikaltimo vietos fotografijas ir išsaugoti juos kompiuterio atmintyje. Kartu labai paspartėja reikiamø portretø bei nuotraukø paieška kompiuterinėje kartotekoje. To-

kios skaitmeninės fotokameros rekomenduotos diegti Lietuvos policijoje ir labai pasiteisino.

7. Kompiuterinius įkalčius (skaitmenines fotonuotraukas, duomenis magnetiniuose diskeliuose ir pan.) standartiniu kompiuteriu ~~lengai~~ galima lengvai pakeisti, falsifikuoti ~~áprastiniais kompiuteriniais árenginiais~~. Todėl labai aktuali tampa kompiuteriniø įkalčiø autentiškumo ir jø apsaugos problema. Lietuvoje reikia pradėti šios srities mokslinius tyrimus.
8. Pastaraisiais metais Lietuvoje labai išsiplėtė kompiuteriø ir kompiuteriø tinklø naudojimas. Remiantis užsienio šaliø patirties analize, galima prognozuoti, kad artimiausiu metu Lietuvoje smarkiai padidės susijusiø su kompiuteriais nusikaltimø skaičius. Tokie nusikaltimai gali padaryti tiek didelius materialinius nuostolius, tiek ir pakenkti valstybės institucijø normaliai veiklai ar net valstybės saugumui. Šie nusikaltimai gali būti tarptautinio pobūdžio. Ateityje būtina Lietuvoje tæsti šios srities mokslinius tyrimus ir remiantis užsienio šaliø patirtimi parengti specialią metodiką informatikos nusikaltimams tirti bei rengti informatikos nusikaltimø tyrimo specialistus.

□□□

## LITERATŪRA


1. **Schwartz R.** Judicial Objectivity and Quantitative Analysis. - Modern Uses of Logic in Law, Sept. 1983.
2. **Петрухин И. Л., Батуров Г. П., Морщакова Т. Г.** Теоретические основы эффективности правосудия. – М., Наука, 1979.
3. **Kobza J.** Planung und Realization von DV-Projekten im Lande Schlezwig-Holstein am Bespiel des Pilotprojektes Computerunter-stutztes Arbeitsplatzsystem, Munster, PFA, 1993.
4. **Petrauskas R**. Kompiuterinės technikos ir programinės įrangos būklės Lietuvos policijos komisariatuose analizė ir jø vystymosi kryptys // LPA Mokslo darbai. - V., 1994. - T. 2.
5. **Federal** guidance for searching and seizing computers. US Department of Justice, 1994.
6. **Advanced** topics of Law and Information Technology. V.Vandenberghe (ed.). Kluwer Law publ., Deventer, 1989.
7. **Computerunterstutzte** Einzelbildaauswertung fur Polizeiliche Unfall-Skizzen. Polizei des Saarlandes, Saarbrucken, 1992.
8. **Canon**, Minolta, Fuji, Medium ir kt. firmø katalogai, 1994-1997.
9. **Rose F.** La criminalite informatique a l'orizon 2005. Analyse perspective. - France, 1994.
10. **Power R.** Current and Future Danger: a CSI Primer on Computer Crime and Information Warfare. Computer Security Institute, US, 1995.
11. **Csonka P.** Council of Europe Activities in the Field of Computer Related Crime // Legal Aspects of Computer-Related Abuse. - Poznan, 1994.
12. **Computers** and Crime. Functionality and Evidence. The Interpol Computer Crime Working group. - 1994.
13. **Belgian**, Dutch, German, French Law on Computer Related Crime.
14. **Computer** Crime. Computer Security Techniques. US Department of Justice. - 1992.
15. **Computer** Related Crime. - FBI Academy Library, July, 1992.
16. **Valstybės žinios.** - 1996. - Nr. 117.
17. **Icove D., Seger K.** Computer crime. Crimefighter's handbook, O'Reilly and Ass. Inc., 1995.


□□□

## *Application of Information Technologies to Crime Investigation*

***Assoc. Professor, Dr. R. Petrauskas, Assoc. Professor, Dr. A. Keras***

*Law Academy of Lithuania*

### *SUMMARY*

*Gathering information, its processing and analysis, preparation of various documents make up a large part of crime investigation activities. The employment of the new information technologies and systems can considerably facilitate crime investigation.*

*The article analyses the experience of foreign countries in this field and the state-of-the-art and possibilities of application of new information technologies to crime investigation in Lithuania.*

*The problems of safety of Lithuanian police information system are discussed. The article analyses the difficulties of investigation of computer crimes in Lithuania.*