Digitálny dôkaz v trestnom konaní

JUDr. NORBERT HALAS
Právnická fakulta, Trnavská univerzita v Trnave,
Katedra trestného práva a kriminológie

DOI: https://doi.org/10.24132/ZCU.NADEJE.2022.95-104

Kľúčové slová:
digitálny dôkaz, trestné konanie, dokazovanie, zdroje

Úvod

V dôsledku všadeprítomnej digitalizácie našej spoločnosti dochádza k presunu trestnej činnosti do online sféry. Užívatelia počítačových systémov[1] za sebou zanechávajú rozsiahle digitálne stopy, na základe ktorých je možné spätne zistiť rôzne údaje akými sú miesto prihlásenia do internetovej služby, odoslané a prijaté správy, e-mailová komunikácia, záznam hovorov a i. Predmetné informácie môžu byť veľmi užitočné v trestnoprávnom kontexte, najmä pri dokazovaní v trestnom konaní, keďže môžu poskytnúť cenné dôkazy o potenciálnych páchateľoch, svedkoch a pod., a môžu potvrdzovať konkrétnu trestnú činnosť, ktorá je prepojená s počítačovou kriminalitou.[2]

Dokazovanie počítačovej kriminality je aktuálnym problémom v celosvetovom meradle, pričom predmetnou problematikou sa zaoberala aj Rada Európskej

---

1 Podľa čl. 1 písm. a) Dohovoru o počítačovej kriminalite „počítačový systém" znamená zariadenie alebo skupinu vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno zariadenie alebo viaceré zariadenia vykonávajú automatizované spracúvanie údajov na základe programu. Pojem „počítačový systém" si teda nemožno zamieňať s pojmom „operačný systém", ktorým sa chápe súhrnné označenie pre technické a programové prostriedky počítača.

2 K pojmu počítačová kriminalita pozri napr. KOLOUCH, J. *Cybercrime*, 1. vydání, Praha, CZ.NIC, z. s. p. o., 2016, s. 49.

únie a jej Rada pre spravodlivosť a vnútorné veci (SVV),[3] ktorá konštatovala, že počítačová kriminalita sa stáva agresívnejšou a konfrontačnou a zahŕňa mimoriadne rozmanitú škálu kriminálnych aktivít vrátane tradičných trestných činov, ktoré zanechávajú digitálne stopy[4] na ktoré nadväzujú digitálne dôkazy.

Digitálne dôkazy predstavujú budúcnosť dokazovania nie len v trestnom konaní, preto sa v tomto príspevku zaoberáme problematikou vymedzenia pojmu a postavenia predmetného dôkazu v trestnom konaní v slovenskom právnom poriadku. Cieľom predmetného príspevku je poskytnúť prehľad o vymedzení pojmu digitálny dôkaz, jeho potenciálnych zdrojov a základných princípov týkajúcich sa hodnotiacich fáz dokazovania v trestnom konaní, použiteľných aj v právnom poriadku Slovenskej republiky.

Vymedzenie pojmu digitálny dôkaz

Dokazovanie je nosným pilierom trestného konania a predstavuje zákonom upravený postup subjektov trestného konania,[5] vrátane rozhodnutí o procesnom postupe.[6] Samotný pojem „dokazovanie" nie je v slovenskom zákone č. 301/2005 Z.z. Trestný poriadok (ďalej len „Trestný poriadok") priamo definovaný, avšak Trestný poriadok v prvej časti „Všeobecné ustanovenia" upravuje v šiestej hlave inštitút dokazovania, ktorý je spoločný pre všetky štádia trestného konania.[7] Účel dokazovania je takisto upravený v základných zásadách trestného konania a to konkrétne v § 2 ods. 10 Trestného poriadku.[8]

---

3 Viac k Rade pre spravodlivosť a vnútorné veci (SVV) pozri: https://www.consilium.europa.eu/sk/council-eu/configurations/jha/.

4 Effective criminal justice in the digital age – what are the needs – State of Play [online]. 2015 [cit. 28.09.2022]. Dostupné z: https://data.consilium.europa.eu/doc/document/ST-14369-2015-INIT/en/pdf.

5 Podľa § 10 ods. 10 Trestného poriadku subjekt trestného konania je každý, kto má a vykonáva vplyv na priebeh konania a komu tento zákon na uskutočnenie tohto vplyvu priznáva určité procesné práva alebo ukladá povinnosti.

6 ČENTÉŠ, J. a kol. *Trestné právo procesné, všeobecná časť*, Heuréka, 2016, s. 328.

7 Okrem toho Trestný poriadok upravuje dokazovanie aj na iných miestach, napr. v § 258 až § 273 Trestného poriadku, kde upravuje dokazovanie na hlavnom pojednávaní.

8 Podľa § 2 ods. 10 Trestného poriadku orgány činné v trestnom konaní postupujú tak, aby bol zistený skutkový stav veci, o ktorom nie sú dôvodné pochybnosti, a to v rozsahu nevyhnutnom na ich rozhodnutie. Dôkazy obstarávajú z úradnej povinnosti. Právo obstarávať dôkazy majú aj strany. Orgány činné v trestnom konaní s rovnakou starostlivosťou objasňujú okolnosti svedčiace proti obvinenému, ako aj okolnosti, ktoré svedčia v jeho prospech, a v oboch smeroch vykonávajú dôkazy tak, aby umožnili súdu spravodlivé rozhodnutie.

V ďalších ustanoveniach Trestný poriadok upravuje demonštratívny výpočet dôkazných prostriedkov využiteľných na účely trestného konania.[9] Napriek takémuto vyčerpávajúcemu výpočtu dôkazných prostriedkov nie sú prípadne vylúčené ani iné dôkazné prostriedky poskytované napr. novými vedeckými poznatkami. Jedinou podmienkou toho, aby dôkazom mohlo byť naozaj „*všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona*" v zmysle § 119 ods. 3 Trestného poriadku je, aby išlo o dôkazy získané zákonným spôsobom. Do úvahy tak prichádzajú najmä najnovšie informačno-technické a iné prostriedky,[10] ktoré sú obsiahnuté v § 10 ods. 20 Trestného poriadku.[11]

Takýmto dôkazom tak môže byť aj digitálny dôkaz, ktorého pojem v slovenskom právnom poriadku nie je priamo upravený. Definovanie digitálnych dôkazov nie je jednoduché nakoľko v súčasnosti neexistuje jasný konsenzus týkajúci sa ich označenia, pretože v odbornej literatúre sa stretávame s pojmami ako „digitálny dôkaz", „elektronický dôkaz" alebo dokonca aj „počítačový dôkaz".[12] Posledný výraz sa častokrát používa výrazne reštriktívnym spôsobom, keď sa odkazuje len na dôkazy týkajúce sa počítača. Pri vymedzení toho, aké označenie je najvhodnejšie na označenie predmetného dôkazu sa musíme pozrieť

---

9 Podľa § 119 ods. 3 Trestného poriadku za dôkaz môže slúžiť všetko, čo môže prispieť na náležité objasnenie veci a čo sa získalo z dôkazných prostriedkov podľa tohto zákona alebo podľa osobitného zákona. Dôkaznými prostriedkami sú najmä výsluch obvineného, svedkov, znalcov, posudky a odborné vyjadrenia, previerka výpovede na mieste, rekognícia, rekonštrukcia, vyšetrovací pokus, obhliadka, veci a listiny dôležité pre trestné konanie, oznámenie, informácie získané použitím informačno-technických prostriedkov alebo prostriedkov operatívno-pátracej činnosti.

10 ČENTÉŠ, J. a kol. *Trestný poriadok. Veľký komentár*. 4. aktualizované vydanie, C. H. Beck SK, 2021, s. 333.

11 Informačno-technickými prostriedkami sa na účely tohto zákona rozumejú elektrotechnické, rádiotechnické, fototechnické, optické, mechanické, chemické a iné technické prostriedky a zariadenia alebo ich súbory použité utajovaným spôsobom pri odpočúvaní a zázname prevádzky v elektronických komunikačných sieťach (ďalej len „odpočúvanie a záznam telekomunikačnej prevádzky"), obrazových, zvukových alebo obrazovo-zvukových záznamov alebo pri vyhľadávaní, otváraní a skúmaní zásielok, ak sa ich použitím zasahuje do základných ľudských práv a slobôd. Na spracúvanie informácií získaných použitím informačno-technických prostriedkov, ich evidenciu, dokumentáciu, ukladanie a vyraďovanie sa vzťahujú osobitné predpisy, ak tento zákon neustanovuje inak. Prevádzkovatelia verejných telefónnych sietí, poskytovatelia elektronických telekomunikačných sietí, poskytovatelia elektronických telekomunikačných služieb, poštový podnik, dopravcovia a iní zasielatelia a ich zamestnanci sú povinní poskytnúť nevyhnutnú súčinnosť pri použití informačno-technických prostriedkov; pritom sa nemôžu dovolávať povinnosti mlčanlivosti podľa osobitných zákonov.

12 Porovnaj VACCA, R., John: *Computer Forensics: Computer Crime Scene Investigation*, Volume 1, Cengage Learning, s. 7, 2005.

do zahraničia a to na definície popredných organizácii a autorov, ktoré nám poslúžia na formulovanie záverov našej problematiky.

V minulosti „počítačový dôkaz" znamenal bežný výtlačok strany/dokumentu z počítača za pomoci tlačiarne pričom došlo k evidencii takéhoto dôkazu, ktorý sa následne v trestnom konaní chápal ako listinný dôkaz. Počítačová evidencia v súčasnosti predstavuje súhrn uložených údajov z pamäťových médií (HDD, SDD, USB, CD a pod.), zachytené údaje prenášané cez komunikačné linky, e-maily a protokolové súbory generované operačnými systémami. To, čo sa predtým chápalo za počítačový dôkaz, sa v súčasnosti chápe ako bežná pracovná činnosť a zodpovedá konvenčnej koncepcii využitia počítača.[13] V dôsledku toho môžeme konštatovať, že pojem dôkaz v spojení s počítačom sa odvíja od neustáleho objavovania sa nových digitálnych technológií.

Pojmy „digitálny" a „elektronický" sú rozsiahlejšie a vzťahujú sa na všetky digitálne alebo elektronické zariadenia, ktoré sa používajú na páchanie trestnej činnosti. Niektorí autori definujú digitálne dôkazy ako informácie uložené alebo prenášané v digitálnej (binárnej) forme, ktoré je možné následne použiť na súde.[14] Naproti tomu Európska komisia pracuje s pojmom elektronický dôkaz,[15] pod ktorý zahŕňa rôzne druhy údajov v elektronickej forme a to buď „obsahové údaje" alebo „prevádzkové údaje", ktoré sú dôležité pre trestné konanie.[16]

Scientific Working Group on Digital Evidence (skrátene „SWGDE") je vedecká pracovná skupina pre digitálne dôkazy, ktorá celosvetovo spája orgány činné v trestnom konaní, akademické kruhy a komerčné organizácie aktívne pôsobiace v oblasti digitálnej forenznej analýzy s cieľom vytvoriť medzidisciplinárne usmernenia a štandardy pre obnovu, uchovávanie a skúmanie digitálnych dôkazov (pričom sa prikláňa k takémuto pojmu) a ktorá definuje digitálny dôkaz ako informáciu s dôkaznou hodnotou, ktorá je uložená alebo prenášaná v binárnej forme.[17]

---

13 NOVAK, Martin, GRIER, Jonathan, GONZALEZ, Daniel: *New approaches to digital evidence acquisition and analysis* [online]. 2018, [cit. 29.09.2022]. Dostupné z: https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis.

14 NOVAK, Martin, GRIER, Jonathan, GONZALEZ, Daniel: *New approaches to digital evidence acquisition and analysis.*

15 V originály „Electronic evidence".

16 European Commission – *Fact Sheet. Frequently Asked Questions: New EU rules to obtain electronic evidence*, Brussels [online]. 2018 [cit. 01.10.2022]. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/el/MEMO_18_3345.

17 SWGDE: *Digital and Multimedia Evidence (Digital Forensics) as a Forensic Science Discipline* [online]. 2014 [cit. 01.10.2022]. Dostupné z: https://www.swgde.org/documents/published-complete-listing.

Medzinárodná technická norma ISO/IEC 27037:2012 pracuje s pojmom digitálny dôkaz a poskytuje usmernenia pre špecifické činnosti pri nakladaní s nimi, ktorými sú identifikácia, zhromažďovanie, získavanie a uchovávanie potenciálnych digitálnych dôkazov, ktoré môžu mať dôkaznú hodnotu. Poskytuje poradenstvo jednotlivcom, pokiaľ ide o bežné situácie, s ktorými sa stretávajú počas procesu spracovania digitálnych dôkazov, a pomáha organizáciám v ich disciplinárnych postupoch a pri uľahčovaní výmeny potenciálnych digitálnych dôkazov medzi jurisdikciami. Týmto uznáva skutočnosť, že kriminalita, najmä tá počítačová, sa čoraz častejšie pácha s medzinárodným dosahom.

Digitálny dôkaz ďalej možno definovať ako akékoľvek údaje, ktoré môžu slúžiť ako dôkaz, bez ohľadu na to, či sú uložené alebo generované, spracované alebo prenášané elektronickým zariadením.[18] Zahŕňa tak „údaje o obsahu", ako sú e-maily, textové správy alebo fotografie, ako aj „údaje bez obsahu", ako sú údaje o predplatiteľoch a prevádzkové údaje (napr. smerovanie alebo načasovanie správy). Takéto údaje uchovávajú rôzni poskytovatelia služieb vrátane poskytovateľov elektronických komunikácií a internetových služieb. Zatiaľ čo vyšetrovanie trestných činov (cezhraničné aj miestne) má tendenciu sa čoraz viac spoliehať na túto formu dôkazov, orgány činné v trestnom konaní a súdy sa často stretávajú s ťažkosťami pri prístupe k nim.[19]

Tieto vymedzenia sú všeobecné akceptované na medzinárodnej scéne a preto je príznačné priklonenie sa k používaniu pojmu digitálny dôkaz, aj vzhľadom na medzinárodný dosah počítačovej kriminality. Digitálny dôkaz je teda akákoľvek informácia vygenerovaná, spracovaná, uložená alebo prenášaná v digitálnej forme, ktorú môže súd akceptovať ako smerodajný dôkaz, ako aj iné možné kópie pôvodných digitálnych informácií, ktoré majú dôkaznú hodnotu, na ktorú sa súd môže odvolať.

Digitálne dôkazy poskytujú jedinečné informácie, ktoré by inak nemuseli byť dostupné v konkrétnej forme alebo z iných zdrojov. Na ilustráciu môžu digitálne

---

[18] BIASIOTTI, Angela, Maria: A proposed electronic evidence exchange across the European Union, In. *Digital Evidence and Electronic Signature Law Review*, 14 [online]. 2017 [cit. 02.10.2022]. Dostupné z: https://journals.sas.ac.uk/deeslr/article/view/2337/2289.

[19] Podľa Komisie v digitálnom veku páchatelia trestnej činnosti čoraz viac využívajú technologické služby na plánovanie a páchanie trestných činov. V dôsledku toho sa elektronické dôkazy stávajú nevyhnutnými na boj proti trestnej činnosti: v súčasnosti sa digitálne údaje používajú v 85 % vyšetrovaní trestných činov a v takmer dvoch tretinách (65 %) vyšetrovaní, kde sú relevantné, je potrebné predmetnú žiadosť adresovať poskytovateľom služieb so sídlom v inej jurisdikcii. Pozri hodnotenie Komisie, SWD(2018) 118 final, s. 13 [online]. 2018 [cit. 02.10.2022]. Dostupné z: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018SC0118&from=EN

dôkazy uvádzať názov inštitúcie alebo meno autora, dátum vytvorenia súboru a jeho posledného uloženia, dátum poslednej tlačenej verzie, vykonané zmeny atď. Iné digitálne dôkazy môžu odhaliť aktivitu na počítači pred a po vypracovaní alebo odoslaní kľúčového súboru.

Potenciálne zdroje digitálnych dôkazov

Poskytnúť rozsiahly zoznam všetkých potenciálnych zdrojov digitálnych dôkazov a ich významu v trestnom konaní je nad rámec tohto príspevku avšak pre celistvosť problematiky môžeme v krátkosti ilustrovať jednotlivé zdroje, ktoré možno použiť v trestnom konaní na účely dokazovania:[20]

- hlavné záznamy o transakciách – zaraďujeme sem všetky nákupy, predaje a iné zmluvné dojednania,
- hlavné obchodné záznamy – patria sem nie len záznamy o transakciách, ale aj všetky dokumenty a údaje, ktoré budú pravdepodobne potrebné na dodržanie právnych a regulačných požiadaviek spojených s obchodno-právnymi vzťahmi,
- E-mailová návštevnosť – E-maily môžu poskytnúť dôležité dôkazy o formálnych a neformálnych kontaktoch podozrivej osoby, resp. páchateľa,
- záznamy uchovávané tretími stranami – napr. poskytovateľ cloud computingu,[21]
- vybrané jednotlivé osobné počítače – v prípade podozrenia zo spáchania trestného činu môžu orgány činne v trestnom konaní zaistiť takého osobné počítače ako vec dôležitú pre trestné konanie za účelom dokazovania,
- vybrané mobilné telefóny/smartfóny, tablety/PDA zariadenia apod. – tieto zariadenia môžu obsahovať značné množstvo dát,

---

20 SOMMER, Peter: *Digital Evidence, Digital Investigations and E-Disclosure: A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers*, The Information Assurance Advisory Council (IAAC), Third Edition, s. 25–27 [online]. 2012 [cit. 02.10.2022]. Dostupné z: https://cryptome.org/2014/03/digital-investigations.pdf

21 Cloud computing je na internete založený model vývoja a používania počítačových technológií. Možno ho charakterizovať aj ako poskytovanie služieb alebo programov uložených na serveroch s tým, že používatelia k nim môžu pristupovať napríklad pomocou webového prehliadača alebo klienta danej aplikácie a používať prakticky odkiaľkoľvek.

- vybrané dátové médiá – väčšina používateľov počítačov archivuje všetky svoje aktivity alebo ich časť na externých pamäťových médiách (napr. CD, DVD, USB, externý HDD alebo SDD a i.),
- denníky riadenia prístupu – všetky počítačové systémy okrem tých najjednoduchších vyžadujú pred povolením vstupu heslo alebo autentifikačné zariadenie. Zvyčajne môžu byť tieto systémy riadenia prístupu nakonfigurované tak, aby uchovávali záznamy o tom, kedy boli vydané používateľské mená a heslá, kedy boli heslá zmenené, kedy boli zmenené a/alebo ukončené prístupové práva k počítačovému systému. Okrem toho mnohé systémy uchovávajú aj záznamy o prístupoch alebo prinajmenšom o neúspešných prístupoch. Tieto protokoly, za predpokladu, že sú správne spravované a uchovávané, sú silným dôkazom sledovania aktivity v počítačovom systéme,
- interné súbory a protokoly – všetky počítače obsahujú súbory, ktoré pomáhajú definovať, ako má operačný systém a rôzne jednotlivé programy fungovať,
- protokoly internetových aktivít – jednotlivé počítače uchovávajú záznamy o nedávnom prístupe na web vo forme súboru histórie a vyrovnávacej pamäte uloženej v priečinku dočasných internetových súborov.

Základné princípy týkajúce sa hodnotiacich fáz dokazovania

K získavaniu digitálnych dôkazov je potrebné vymedziť aj základne zásady postupov takéhoto získavania, ktoré by neodporovali právnemu poriadku toho-ktorého štátu, aj keď ide o rozdielne právne úpravy. Na takéto účely skupina toho času G8 (dnes G7) navrhla šesť základných zásad pre postupy týkajúce sa získavania digitálnych dôkazov, ktoré sú použiteľné aj v právnom poriadku Slovenskej republiky:[22]

1. Pri nakladaní s digitálnymi dôkazmi sa musia uplatňovať všetky všeobecné forenzné a procesné princípy ustanovené právnym poriadkom toho-ktorého štátu.
2. Po zaistení digitálnych dôkazov musia byť prijaté opatrenia, účelom ktorých by bola nezameniteľnosť takýchto dôkazov.

[22] VACCA, R., John: *Computer Forensics: Computer Crime Scene Investigation,* s. 673.

3. Ak je potrebné, aby osoba, ktorá vyšetruje trestnú činnosť mala prístup k originálnym digitálnym dôkazom, mala by byť na tento účel vyškolená.
4. Všetky činnosti súvisiace so zaistením, prístupom, uchovávaním alebo prenosom digitálnych dôkazov musia byť plne zdokumentované, uchovávané a dostupné na preskúmanie.
5. Jednotlivec je zodpovedný za všetky kroky podniknuté v súvislosti s digitálnymi dôkazmi.
6. Každá agentúra, ktorá je zodpovedná za zaistenie, prístup, uchovávanie alebo prenos digitálnych dôkazov, je zodpovedná za dodržiavanie týchto zásad.

Tento súbor zásad môže slúžiť ako pevný základ pri manipulácií s digitálnymi dôkazmi a osoba, ktorá s nimi manipuluje, musí k ním pristupovať tak, aby nedošlo k zmene, zámene alebo zničeniu takto získaných dôkazov. Týmto by boli eliminované námietky zo strán obhajoby týkajúce sa pozmeňovania digitálnych dôkazov. Žiadne opatrenie zo strany orgánov činných v trestnom konaní by nemalo zmeniť, resp. zameniť údaje uložené na počítači alebo pamäťovom médiu, na ktoré sa možno následne odvolávať na súde.

Za výnimočných okolností, keď osoba považuje za potrebné získať prístup k pôvodným údajom uloženým v počítači alebo na pamäťovom médiu, musí byť na to kompetentná a musí byť schopná poskytnúť dôkazy vysvetľujúce význam a dôsledky svojho konania. Mal by sa vytvoriť a uchovať revízny záznam alebo iný záznam všetkých procesov aplikovaných na digitálne dôkazy. Nezávislá tretia strana by mala byť schopná preskúmať tieto procesy a dosiahnuť rovnaký výsledok. Orgány činné v trestnom konaní majú celkovú zodpovednosť za zabezpečenie dodržiavania zákona a týchto zásad.

Digitálne dôkazy, aj keď nie sú v Trestnom poriadku priamo definované, tak sa na ne vzťahujú rovnaké právne ustanovenia dokazovania. Je tak na orgánoch činných v trestnom konaní, aby preukázali to, že nedošlo k zmene/zámene digitálnych dôkazov a sú totožné ako boli získané. Jedna z hlavných otázok týkajúcich sa digitálnych dôkazov sa týka postupu ich zhromažďovania, hodnotenia a predloženia súdu.

Na rozdiel od nejednoznačných alebo neurčitých právnych predpisov v Slovenskej republike majú komparačné právne systémy veľmi presný postup týkajúci sa digitálnych dôkazov. Napríklad americký Národný inštitút spravodlivosti (NIJ)[23]

[23] V originály The National Institute of Justice.

vo svojom „Electronic Crime Scene Investigation: A Guide for First Responders“ opisuje štvorfázový proces, ktorý pozostáva z nasledujúcich fáz:[24]

1. Zbierka – vyhľadávanie, rozpoznávanie, zhromažďovanie a dokumentácia digitálnych dôkazov.
2. Skúmanie – vysvetlenie pôvodu a významu dôkazu, hľadanie informácii.
3. Analýza – hľadí sa na výsledok skúmania významu digitálneho dôkazu a na dôkaznú hodnotu pre konkrétny prípad.
4. Reporting – oboznámenie získaného digitálneho dôkazu.

Záver

Účelom tohto príspevku bolo poskytnúť stručný prehľad všeobecných definícií digitálnych dôkazov s cieľom identifikovať možné zdroje digitálnych dôkazov a vypracovať základné princípy týkajúce sa získavania a hodnotenia týchto dôkazov s cieľom zaobchádzanie s nimi v trestnej legislatíve. Vzhľadom na všetky nedostatky v slovenskom Trestnom poriadku, pokiaľ ide o digitálne dôkazy, zastávame názor, že je potrebná novelizácia Trestného poriadku so zavedením definície digitálneho dôkazu, aby nedochádzalo k odlišným výkladom zo strany orgánov činných v trestnom konaní a rovnako aj súdov. Takisto je potrebné poskytnúť presný postup zhromažďovania, manipulácie, uchovávania a predloženia predmetných dôkazov.

Tiež sa domnievame, že je potrebné implementovať špecifické princípy, ktoré riešia hodnotenie digitálnych dôkazov v trestnom konaní a ktoré môžu pomôcť cezhraničnému prístupu ku digitálnym dôkazom.

[24] U.S. Department of Justice Office of Justice Programs: (2001) Electronic Crime Scene Investigation: A Guide for First Responders, written and Approved by the Technical Working Group for Electronic Crime Scene Investigation, Washington, USA.

***

Abstract

Digital evidence in criminal proceeding

The contribution in question concerns a certain issue of digital evidence and the definition of its terms, while the author of the contribution was based on definitions found mainly in foreign literature. The paper further discussed individual potential sources of digital evidence, which, due to the breadth of the topic, the author briefly discussed and listed examples of sources. To acquire digital evidence, it is necessary to pay attention to the basic principles of this acquisition, which did not conflict with the legal order of any country, even if the legal regulations are different.