Martin Bicko

Odhaľovanie a dokazovanie počítačových trestných činov

Anotácia: Článok je ucelený do jednej tematickej kapitoly, ktorá má šesť podkapitol. Nosnou témou článku je odhaľovanie a dokazovanie počítačovej kriminality v podmienkach legislatívy Slovenskej republiky. V prvej podkapitole autor analyzuje prístupy k vyšetrovaniu trestných činov. V ďalších kapitolách uvádza jednotlivé inštitúty trestného práva využiteľné v rámci vyšetrovania trestných činov počítačovej kriminality. Podrobne analyzuje jednotlivé inštitúty trestného práva, ako sú domová prehliadka a zaistenie stôp, zabezpečenia digitálnej stopy, zaistenie výpočtovej techniky, odňatie počítačových údajov, zaistenie kryptoaktív. V poslednej podkapitole rozpracováva dokazovanie počítačovej kriminality Na dosiahnutie cieľa článku a verifikáciu hypotézy sú využité metódy deskripcie, analýzy, syntézy a dedukcie.

Kľúčové slová: kybernetický útok, počítačová kriminalita, digitálna stopa, vyšetrovanie, kryptoaktivita.

Úvod

Cieľom kybernetických útočníkov môžu byť iný počítač, hardvér, softvér, sieť a pod. Na rozdiel od iných trestných činov je pre kybernetickú kriminalitu typické, že sa odohráva výlučne v kybernetickom priestore, pričom tento priestor nie je možné jednoducho objektívne vnímať. Tak, ako je na páchanie kybernetickej kriminality v kybernetickom priestore nevyhnutné disponovať zariadením, ktoré páchanie trestnej činnosti umožňuje, je dôležité disponovať aj iným zariadením, napríklad počítačom aj na sledovanie diania v kybernetickom priestore. Výpočtová technika teda poskytuje novú technológiu a takisto nové spôsoby, resp. možnosti na páchanie buď už známych trestných činov z reálneho prostredia, alebo aj na páchanie novej trestnej činnosti, ktorú nie je možné páchať v reálnom svete. Ide napríklad o hacking, DDoS útoky, používanie botnetov a pod.[1] Nejde však o jediné špecifikum páchania kybernetickej kriminality, ktorá ju odlišuje od páchania trestnej činnosti klasickou formou. Problémom je aj zaistenie a identifikácia stôp.[2] Digitálne stopy sa totiž vyznačujú nestálou trvácnosťou, t. j. zo strany páchateľa môže jednoducho dôjsť k ich zničeniu. Okrem toho kriminalita páchaná v kybernetickom priestore častokrát presahuje hranice národných štátov, čo zásadným spôsobom sťažuje vyšetrovanie. Ďalším atribútom, ktorý sťažuje vyšetrovanie počítačových trestných činov, je aj samotný spôsob zaistenia údajov. Ide o úkon, ktorý samotný môže vyvolať pochybnosti o tom, že údaje, ktoré sú využité v rámci vyšetrovania a dokazovania, boli zo strany vyšetrovateľa získané adekvátnym postupom (v zmysle legislatívy).

1. Zisťovanie a dokazovanie počítačových trestných činov

1.1 Prístupy k vyšetrovaniu počítačových trestných činov

Prístupy k vyšetrovaniu trestných činov kategorizovala napríklad autorka Mokrá[3]. Tieto prístupy kategorizovala na reaktívne, proaktívne a rušivé.[4] Rozdiel medzi jednotlivými typmi vyšetrovania je spracovaný v tabuľke 1.

[1] KOLOUCH, J. *Cybercrime*, s. 516.
[2] GOEL, S. a kol. *Digital Forensis and Cyber Crime*, s. 184.
[3] MOKRÁ, J. Methodology of detection and investigation of the crime of human trafficking. In: *Projustice* [online]. 2023. [cit. 3. februára 2026]. Dostupné na internete: https://www.projustice.sk/trestne-pravo/metodika-odhalenia-a-vysetrovanie-trestneho-cinu-obchodovania-s-ludmi

Tabuľka 1 Prístupy k vyšetrovaniu trestných činov

Prístup	Charakteristika
Reaktívny	vyšetrovanie vedené obeťou trestného činu
Proaktívne	vyšetrovanie vedené políciou, spravodajstvom
Rušivé	vedené políciou v prípade nemožnosti využitia reaktívneho/proaktívneho vyšetrovania

Zdroj: vlastné spracovanie podľa MOKRÁ[5], J. *Methodology of detection and investigation of the crime of human trafficking.*

Reaktívne vyšetrovanie predstavuje vyšetrovanie, ktoré sa zakladá na výpovedi obete trestného činu. Identifikácia osoby ako obete trestného činu je v rámci vyšetrovania spojená s potrebou okamžitého zásahu vyšetrovateľa a zaistením ochrany obete trestného činu. V rámci reaktívneho vyšetrovania však vzniká pomerne obmedzený priestor na proaktívne vyšetrovanie zamerané na získanie nezávislých dôkazov. Dôležité však je, aby čím skôr došlo k zaisteniu dôkazov, ktoré by sa mohli časom zničiť alebo stratiť. Uvedené platí predovšetkým pre zaistenie počítačových, resp. digitálnych stôp, ktoré môže páchateľ veľmi rýchlo zničiť.[6]

V prípade, že je v rámci reaktívneho vyšetrovania nevyhnutný okamžitý zásah bezpečnostných zložiek, je dôležité, aby bol zásah vrátane prípadného zatýkania páchateľov trestného činu koordinovaný a správne načasovaný. Cieľom zásahu by teda okrem zaistenia dôkazov mala byť aj snaha o maximalizáciu zaistenia čo najväčšieho počtu osôb podozrivých zo spáchania trestného činu. Dôležitým pre zásah je okrem optimálneho načasovania aj podrobný plán zásahu a použitie primeraného počtu techniky a príslušníkov bezpečnostných zložiek.[7]

Základom vedenia reaktívneho vyšetrovania sú informácie získané vypočutím obete trestného činu alebo svedka. Alternatívnou môžu byť aj získané spravodajské informácie. Problematickým aspektom reaktívneho vyšetrovania je však okrem odmietnutia výpovede podozrivej osoby aj potenciálne odmietnutie svedkov či obetí trestného činu vypovedať pred súdom či odvolanie svojej výpovede. Uvedené má však za následok neodsúdenie páchateľa pre nedostatok dôkazov.[8]

Proaktívne vyšetrovanie predstavuje typ vyšetrovania, ktoré je vedené bezpečnostnými zložkami, t. j. policajným vyšetrovateľom. Tento typ vyšetrovania je reflexiou na skutočnosť, že obete trestných činov alebo svedkov nemusia byť pri vyšetrovaní vôbec prítomné. Vyšetrovanie spočíva v zhromažďovaní a následnej analýze informácií, ktoré vyšetrovatelia získajú napríklad od spravodajstva, pričom tieto informácie sú zamerané na páchateľov kybernetickej kriminality, napríklad na hackerov. Na získanie dôkazov sa pri vyšetrovaní okrem štandardných vyšetrovacích techník využívajú aj zvláštne techniky (spravodajstvo,

[4] MOKRÁ, J. Methodology of detection and investigation of the crime of human trafficking. In: *Projustice* [online]. 2023. [cit. 3. februára 2026]. Dostupné na internete: https://www.projustice.sk/trestne-pravo/metodika-odhalenia-a-vysetrovanie-trestneho-cinu-obchodovania-s-ludmi.

[5] Tamtiež.

[6] KOLOUCH, J. *Cybercrime*, s. 516.

[7] ŠÁNDOR, M. Praktické spôsoby zaisťovania počítačových údajov v trestnom konaní. In: *Poradca policajta*. [online]. 2018. [cit. 3. februára 2026]. Dostupné na internete: https://poradcapolicajta.sk/prakticke-sposoby-zaistovania-pocitacovych-udajov-v-trestnom-konani/

[8] MOKRÁ, J.. Methodology of detection and investigation of the crime of human trafficking. In: *Projustice* [online]. 2023. [cit. 3. februára 2026]. Dostupné na internete: https://www.projustice.sk/trestne-pravo/metodika-odhalenia-a-vysetrovanie-trestneho-cinu-obchodovania-s-ludmi.

nasadenie agenda, odpočúvanie, monitorovanie vybraných priestorov, monitoring finančných transakcií podozrivých osôb a pod.), ktoré však musia byť využité v súlade so zákonom.

Rušivé vyšetrovanie je typom vyšetrovania, ktoré sa využíva v prípade, že nie je možné reaktívne alebo proaktívne vyšetrovanie. Orgány činné v trestnom konaní sa v rámci vyšetrovania snažia narúšať operácie kybernetických zločincov, na čo je nevyhnutné využívať nielen štandardné postupy, ale aj inovatívne taktiky, cieľom ktorých je zabrániť páchaniu ďalšej trestnej činnosti. V rámci vyšetrovania je možné využiť napríklad techniku sledovania osôb podozrivých z páchania trestných činov.[9] Ďalším spôsobom môže byť aj využitie agenta, ktorého úlohou je infiltrácia do siete páchateľov trestnej činnosti (napríklad v prípade, že sa páchatelia zaoberajú výrobou alebo distribúciou detskej pornografie). Rušivé vyšetrovanie je zároveň možné vnímať ako formu prevencie, keďže v rámci tohto typu vyšetrovania je zároveň možné upozorňovať spoločnosť na nelegálnu činnosť vybraných subjektov. Typickým príkladom v kontexte páchania kybernetickej kriminality môže byť poskytovanie informácií príslušníkmi polície potenciálnym obetiam trestných činov o jednotlivých bezpečnostných hrozbách, napríklad phishingu. Preventívne akcie však nemusí realizovať výlučne polícia, ale aj ďalšie inštitúcie, napríklad ministerstvá, finančná správa a pod.[10]

V kontexte prístupov k vyšetrovaniu kybernetickej kriminality vyvodzujeme záver, že podnet na vyšetrovanie môžu orgány činné v trestnom konaní získať od fyzických alebo právnických osôb, ktoré môžu vystupovať ako obete (napríklad obeť phishingu) a aj ako svedkovia spáchania trestného činu. Svedkov je v prípade kybernetickej kriminality možné rozdeliť na dve skupiny, a to na svedkov, ktorí podávajú svoju výpoveď na neodborné otázky (osobné, pracovné, iné pomery obvinenej osoby) a svedkov, ktorí podávajú informácie technického charakteru, napríklad o spôsobe zavedenia dát do počítača, informácie týkajúce sa realizácie vybraných operácií (napríklad zrealizovaného kybernetického útoku a pod.). Zatiaľ, čo prvá skupina svedkov nie je považovaná za odborníkov, druhú skupinu svedkov tvoria odborníci (súdny znalec, IT technik a pod.).

Ďalšie podnety na vyšetrovanie trestnej činnosti páchanej v kybernetickom priestore môžu získať orgány činné v trestnom konaní aj od organizácií, ktoré sa špecializujú na problematiku kybernetickej bezpečnosti a tiež od ďalších organizácií, ktoré orgány činné v trestnom konaní môžu upozorniť na páchanie trestnej činnosti v kybernetickom priestore. Možnosťou získania podnetu pre vyšetrovanie kybernetickej kriminality je aj vlastná operatívna pátracia činnosť orgánov činných v trestnom konaní.

Súhrn podmienok a okolností, ktoré umožňujú páchanie kriminality v kybernetickom priestore, nazýva Kolouch[11] kriminálnou situáciou.[12] Ide o podmienky, ktoré súčasne predurčujú nielen samotný spôsob páchania trestnej činnosti v kybernetickom priestore, ale aj zákonitosti vzniku a zániku digitálnych stôp. Ide predovšetkým o:[13]

a) úroveň právneho režimu, právnu a technickú ochranu dát a počítačových systémov;
b) úroveň rozvoja informačných a komunikačných technológií v konkrétnej lokalite;
c) úroveň technického vybavenia a odbornej pripravenosti orgánov činných v trestnom konaní;
d) špecifiká prostredia, v rámci ktorého dochádza k páchaniu trestnej činnosti;

[9] *§ 113 Zákona č. 301/2005 Z. z. Trestného poriadku*.
[10] MOKRÁ, J. Methodology of detection and investigation of the crime of human trafficking. In: *Projustice* [online]. 2023. [cit. 03.02.2026]. Dostupné na internete: https://www.projustice.sk/trestne-pravo/metodika-odhalenia-a-vysetrovanie-trestneho-cinu-obchodovania-s-ludmi.
[11] KOLOUCH, J. *Cybercrime* s. 516
[12] Tamtiež.
[13] STRAUS, J. a kol. *Kriminalistická metodika,* s. 320.

e) špecifická postavenia páchateľov kybernetických zločinov, pričom je potrebné zdôrazniť, že spravidla ide o odborne zdatných páchateľov trestnej činnosti.

V kontexte vyšetrovania kybernetickej kriminality vyvodzujeme záver, že bez ohľadu na konkrétny typ vyšetrovania je nevyhnutné k tomuto typu kriminality pristupovať špecificky, a to práve z dôvodu existencie viacerých špecifík spojených s vyšetrovaním počítačových trestných činov.[14] Na odhaľovaní počítačových trestných činov, resp. kybernetickej kriminality vo všeobecnosti, by sa zároveň okrem orgánov činných v trestnom konaní mali podieľať aj špecializované tímy zložené z profesionálov na problematiku kybernetickej bezpečnosti a tiež odborníci na informačné a výpočtové technológie.

1.2 Domová prehliadka a zaistenie stôp

V rámci vyšetrovania kybernetickej kriminality je v súvislosti s trestným konaním možné vykonať aj domovú prehliadku, resp. prehliadku iných priestorov neslúžiacich na bývanie. Vzhľadom na skutočnosť, že domová prehliadka predstavuje závažný zásah do základných práv a slobôd človeka, je nevyhnutné, aby sa pri jej vykonávaní dodržiaval postup určený Trestným poriadkom a domová prehliadka bola vykonaná z niektorého dôvodu definovaného v § 99 Trestného poriadku. Informácie, na základe ktorých vyšetrovateľ argumentuje vykonanie domovej prehliadky, môžu byť získané z rôznych zdrojov, napríklad na základe výsluchu svedkov, na základe poznatkov kriminálnej polície a pod. Ak vyšetrovateľ nedisponuje hodnovernými informáciami, ale len neoverenými informáciami či indíciami, nie je možné nariadiť domovú prehliadku. Domovú prehliadku je teda v súlade s § 99 Trestného poriadku možné vykonať len v prípade, že existuje dôvodné podozrenie, že v byte alebo inom priestore sa nachádza vec, ktorá je dôležitá pre trestné konanie, resp. sa v tomto priestore skrýva osoba, ktorá je podozrivá zo spáchania trestného činu.[15] Spravidla sa však domová prehliadka vykonáva voči osobám, ktoré sú podozrivé zo spáchania trestného činu, resp. voči obvineným osobám. Ak existuje dôvodné podozrenie, že osoba má pri sebe vec dôležitú pre trestné konanie, je možné vykonať aj osobnú prehliadku.

Príkaz na domovú prehliadku musí byť odôvodnený a zároveň musí byť vyhotovený v písomnej podobe. Môže ho vydať výhradne sudca alebo predseda senátu, resp. v prípravnom konaní sudca na návrh prokurátora. Ak domová prehliadka neznesie odklad, môže príkaz na ňu vydať predseda senátu alebo sudca, v obvode ktorého sa má prehliadka vykonať. Pokiaľ sa príkaz na domovú prehliadku vydá ešte predtým, než sa začne trestné stíhanie alebo v prípravnom konaní, vydá príkaz na domovú prehliadku súd, ktorý bol príslušný na konanie o obžalobe. V prípade, že by takýchto súdov bolo viacej, úkony spojené vydaním príkazu na domovú prehliadku vykoná súd, v ktorého obvode je činný prokurátor, ktorý podal príslušný návrh.[16] V súlade s § 100 ods. 2 Trestného poriadku vykonáva domovú prehliadku bez meškania orgán, ktorý ju nariadil. Alternatívne môže domovú prehliadku vykonať aj policajt, avšak len na základe príkazu orgánu, ktorý túto prehliadku nariadil vykonať.[17]

Špecifikom príkazu na domovú prehliadku je skutočnosť, že proti nemu nie je možné podať opravný prostriedok. Okrem toho oprávnená osoba takisto nemôže namietať vykonanie úkonu, resp. ovplyvniť jeho vykonanie. Oprávnená osoba musí úkon prehliadky strpieť.

[14] ZÁHORA, J. Zaisťovanie digitálnych dôkazov v cezhraničných situáciách. In: *Časopis pro právní vědu a praxi*. 2019, roč. 27, č. 1, s. 53.
[15] *Zákon č. 301/2005 Z. z. Trestný poriadok.*
[16] ZÁHORA, J., I. ŠIMOVČEK, P. POLÁK, P. a kol. *Zákon č. 301/2005 Z. z. Trestný poriadok. Komentár*. s. 1205.
[17] *Zákon č. 301/2005 Z. z. Trestný poriadok*.

Domovú prehliadku alebo prehliadku iných priestorov nie je možné vykonať v konzulárnych miestnostiach, v súkromných miestnostiach diplomatických zástupcov ani v priestoroch diplomatickej misie.[18]

Šamko[19] uvádza, že príkaz na vykonanie domovej prehliadky podľa § 100 Trestného poriadku, resp. príkaz na prehliadku iných priestorov a pozemkov vydaný podľa § 101 Trestného poriadku, môže obsahovať aj opis veci alebo osoby, ktorú je potrebné pri domovej prehliadke zaistiť v prípade, že je známa. Okrem hmotných vecí, ktorými sú v prípade spáchania počítačového trestného činu napríklad počítače, skenery, pevné disky, tlačiarne, USB kľúče či iná výpočtová technika, môže byť v rámci domovej prehliadky zaistená aj finančná hotovosť, cenné papiere, majetková účasť v právnickej osobe, ale aj kryptoaktívum či iná majetková hodnota. Sudca alebo iná oprávnená osoba nemusí v týchto prípadoch vydávať samostatné príkazy na zaistenie konkrétnej veci. Vydanie príkazu na domovú prehliadku bez možnosti zaistenia veci alebo zadržania osoby podozrivej zo spáchania trestného činu, resp. samotného páchateľa trestného činu by bolo iracionálne. Vydávanie osobitných príkazov by zároveň predstavovalo nadbytočné hromadenie jednotlivých príkazov, čo nie je nevyhnutné.[20]

Šándor[21] uvádza, že v rámci domovej prehliadky by mal vyšetrovateľ využiť moment prekvapenia. Ide o dôležitý aspekt domovej prehliadky, cieľom čoho je zamedziť úniku podozrivej osoby, páchateľa trestného činu či zamedziť zničeniu veci, ktorú je potrebné zabezpečiť s cieľom dokázať spáchanie trestného činu.[22] V rámci domovej prehliadky zároveň dochádza k zaisteniu stôp. Stopou sa z hľadiska kriminalistiky rozumie akákoľvek zmena v materiálnom prostredí alebo vo vedomí človeka, pričom táto zmena je zistiteľná, je možné ju zaistiť a zároveň využiť pred súdom ako dôkazný prostriedok.[23]

Súčasťou dôkazného materiálu pri počítačovej kriminalite a čoraz častejšie aj pri iných trestných činoch spojených s páchaním hospodárskej kriminality, majetkových trestných činov a pod. je zásadné zaistenie tzv. digitálnej alebo počítačovej stopy.[24] Za počítačovú stopu je možné považovať zmenu na nosiči informácií, ktorá vznikne v súvislosti so spáchaním trestného činu, pričom pri páchaní trestného činu bola použitá výpočtová technika. Počítačová stopa je identifikovateľná (pomocou súčasných metód a kriminalistických prostriedkov) a nachádza sa na vybranom zariadení, ktoré prislúcha k počítaču. Ide napríklad o vymeniteľné pamäťové médium (CD, DVD, USB kľúč, externý disk a pod.), pevný disk a pod.[25] Počítačová stopa obsahuje vnútornú, funkčnú, dynamickú alebo inú významovú informáciu objektu, pričom objektom, ktorý zanecháva v počítačových stopách danú informáciu, je okrem človeka aj výpočtová technika a tiež samotné dáta.[26]

Smejkal[27] v kontexte stôp určených pre kriminalistickú expertízu nehovorí o počítačovej, ale o digitálnej stope. Dôvodom je skutočnosť, že počítačovú stopu zanecháva

[18] ZÁHORA, J., I. ŠIMOVČEK, P. POLÁK a kol. *Zákon č. 301/2005 Z. z. Trestný poriadok. Komentár,* s. 1205.
[19] ŠAMKO, P. *Daňové podvodné konania a ich dokazovanie,* s. 420.
[20] Tamtiež.
[21] Tamtiež.
[22] ŠÁNDOR, M. 2018. Praktické spôsoby zaisťovania počítačových údajov v trestnom konaní. In: *Poradca policajta.* [online]. [cit. 3. februára 2026]. Dostupné na internete: https://poradcapolicajta.sk/prakticke-sposoby-zaistovania-pocitacovych-udajov-v-trestnom-konani/
[23] KOLOUCH, J. *Cybercrime*, s. 516.
[24] SMEJKAL, V. *Kybernetická kriminalita,* s. 640.
[25] STRAUS, J. a kol. *Kriminalistická metodika,* s. 320.
[26] PORADA, V. a J. STRAUS. *Kriminalistické stopy. Teorie, metodologie, praxe,* s. 512.
[27] SMEJKAL, V. *Kybernetická kriminalita,* s. 640.

počítač, digitálnu stopu však zanechávajú aj iné elektrotechnické zariadenia.[28] Za digitálnu stopu je možné považovať akékoľvek dáta, ktoré sú uložené alebo prenášané pomocou použitia počítača, pričom tieto dáta podporujú teóriu o tom, ako sa konkrétny trestný čin stal. Okrem toho môžu tieto dáta (v rámci digitálnej stopy) identifikovať a objasniť napríklad zámery páchateľa.[29] Smejkal[30] v kontexte digitálnej stopy zároveň dodáva, že túto stopu zanecháva každé technologické zariadenie, ktoré získava, spracúva, ďalej posúva alebo uchováva dáta. Z kriminalistického hľadiska sú tieto záznamy (digitálnymi) stopami. V oblasti IT ide predovšetkým o stopy, ktoré je možné definovať podľa SWGDE (*Scientific Working Group on Digital Evidence*) ako akékoľvek dáta, resp. informácie, ktoré majú určitú výpovednú hodnotu, pričom tieto dáta sú uložené alebo prenášané v digitálnej podobe. [31] Kolouch uvádza aj ďalšie definície digitálnej stopy. Digitálna stopa môže byť špecifikovaná napríklad ako:[32]

a) akúkoľvek informácia, ktorá je uložená alebo prenášaná v binárnej forme, pričom táto informácia môže byť predložená súdu ako dôkazný materiál;
b) akákoľvek informácia, ktorá môže byť využiteľná ako dôkaz, pričom táto informácia je ukladaná alebo prenášaná v digitálnej podobe (email, digitálna fotografia, elektronicky spracovaný dokument a pod.);
c) akýkoľvek typ dát alebo informácií, ktoré sú prenášané, vytvárané, modifikované alebo ukladané pomocou použitia počítačových systémov, pričom takéto informácie môžu byť dôkazným prostriedkom pred súdom.

Záhora[33] definoval digitálny dôkaz ako „*všetky druhy údajov prenášaných do počítačového systému, z neho alebo v jeho rámci, alebo uchovávaných v elektronickej podobe na príslušnom médiu ako počítačové údaje*.“[34] Medzi tieto údaje, ktoré existujú v elektronickej podobe, patria obsahové údaje (IP adresa, e-mail, používateľské meno) a takisto prevádzkové údaje dôležité pre trestné konanie. Ide o údaje, ktoré sú z pohľadu vyšetrovania kybernetickej kriminality nenahraditeľné. To znamená, že bez týchto údajov nie je možné identifikovať páchateľa trestnej činnosti ani získať informácie o aktivitách, ktoré táto osoba realizovala v kybernetickom priestore.

Digitálna stopa sa oproti klasickým stopám vyznačuje viacerými špecifikami. Ide predovšetkým o objemnosť stopy (t. j. stopa obsahuje značný objem dát; táto charakteristika je však individuálna), dynamiku, existenciu v kybernetickom priestore a tiež pomerne krátku životnosť. Digitálne stopy sú nehmotné, je možné s nimi manipulovať. Akékoľvek prieťahy vo vyšetrovaní tak v konečnom dôsledku môžu viesť k strate digitálnej stopy, čo nevyhnutne znižuje aj celkový potenciál objasnenia kybernetickej kriminality.

[28] Tamtiež.
[29] KOLOUCH, J. *Cybercrime,* s. 516.
[30] SMEJKAL, V. *Kybernetická kriminalita,* s. 640.
[31] Tamtiež.
[32] KOLOUCH, J. *Cybercrime,* s. 516.
[33] ZÁHORA, J. Zaisťovanie digitálnych dôkazov v cezhraničných situáciách. In: *Časopis pro právní vědu a praxi*, s. 52.
[34] Tamtiež.

1.3 Inštitúty zabezpečenia stopy

Záhora uvádza, že v rámci vyšetrovania počítačových trestných činov je možné v súlade s Dohovorom o počítačovej kriminalite využiť viaceré špecifické vyšetrovacie opatrenia. Ide o:[35]

a) urýchlené uchovanie uložených počítačových údajov;
b) urýchlené uchovanie prevádzkových údajov vrátane ich parciálneho sprístupnenia;
c) príkaz na predloženie počítačových údajov;
d) prehliadku a zabezpečenie uložených počítačových údajov;
e) zachytenie obsahových údajov;
f) zhromažďovanie prevádzkových údajov realizované v reálnom čase.[36]

V prípade domovej prehliadky je jej cieľom okrem zaistenia páchateľa, resp. osoby podozrivej zo spáchania trestnej činnosti, aj zaistenie ďalších vecí. V súvislosti s páchaním počítačovej kriminality medzi najviac dôležité inštitúty v zmysle Trestného poriadku patria:

a) vec dôležitá pre trestné konanie;[37]
b) uchovanie, vydanie a odňatie počítačových údajov;[38]
c) zaistenie peňažných prostriedkov;[39]
d) zaistenie kryptoaktíva.[40]

V prípade spáchania počítačového trestného činu je možné stopy zabezpečiť dvomi spôsobmi, a to buď úplným odňatím zariadení (výpočtovej techniky, napríklad počítačov), pri ktorých existuje podozrenie, že boli použité na spáchanie trestnej činnosti, alebo vyhľadaním a zistením potrebných údajov vo vybraných zariadeniach priamo na mieste.[41] Úplné odňatie výpočtovej techniky, ako aj odňatie počítačových údajov v oboch prípadoch predstavuje značný zásah do súkromia osoby. Z uvedeného dôvodu je nevyhnuté, aby súkromie osôb bolo narušené čo najmenej. Počítač alebo iný hmotný nosič, na ktorom sa nachádzajú počítačové údaje, je preto možné odňať len v prípade, ak je uvedený zásah legitímny, legálny a zároveň nevyhnutný.[42]

1.3.1 Zaistenie výpočtovej techniky (veci dôležitej pre trestné konanie)

V súlade s § 89a Trestného poriadku môže vyšetrovateľ zaistiť vec dôležitú pre trestné konanie. Ide o vec, ktorá môže slúžiť na účely dokazovania, prípadne táto vec bola použitá alebo určená na spáchanie trestnej činnosti.[43] Ide predovšetkým o vecné a listinné dôkazy, pričom za vecné dôkazy sa považujú „*predmety, ktorými, alebo na ktorých bol trestný čin spáchaný, ktoré dokazujú alebo vyvracajú dokazovanú skutočnosť a môžu byť prostriedkom na odhalenie alebo zistenie trestného činu alebo jeho páchateľa, ako aj stopy trestného činu*.“[44] Vec dôležitá pre trestné konanie je aj výnos získaný z páchania trestnej

---

[35] ZÁHORA, J. Zaisťovanie digitálnych dôkazov v cezhraničných situáciách. In: *Časopis pro právní vědu a praxi*.2019, roč. 27, č. 1, s. 54.
[36] *Dohovor o počítačovej kriminalite*. [online]. [cit. 3. februára 2026]. Dostupné na internete: https://rm.coe.int/16802fa420
[37] *§ 89a a nasl. Zákona č. 301/2005 Z. z. Trestného poriadku.*
[38] *§ 91 Zákona č. 301/2005 Z. z. Trestného poriadku.*
[39] *§ 95 Zákona č. 301/2005 Z. z. Trestného poriadku.*
[40] *§ 96d Zákona č. 301/2005 Z. z. Trestného poriadku.*
[41] ŠÁNDOR, M. Praktické spôsoby zaisťovania počítačových údajov v trestnom konaní. In: *Poradca policajta*. [online]. 2018. [cit. 3. februára 2026]. Dostupné na internete: https://poradcapolicajta.sk/prakticke-sposoby-zaistovania-pocitacovych-udajov-v-trestnom-konani/
[42] II. ÚS 386/2014.
[43] *Zákon č. 301/2005 Z. z. Trestný poriadok.*
[44] ZÁHORA, J., I. ŠIMOVČEK, P. POLÁK a kol. *Zákon č. 301/2005 Z. z. Trestný poriadok. Komentár,* s. 172.

činnosti, ktorým môže byť napríklad vec získaná trestným činom či vec získaná ako odmena za spáchanie trestného činu.

Pri domovej prehliadke je dôležité zamerať sa predovšetkým na:

1. Zaistenie počítačových systémov vrátane ďalších hmotných veci, ktoré majú tendenciu súvisieť s počítačovou kriminalitou. Ide najmä o počítače, servery, dátové úložiská (externé disky, USB kľúče, mobilné telefóny, tablety, smartfóny, pamäťové médiá, tlačiarne, ale aj ďalšie veci, ktoré primárne nemusia súvisieť so spáchaním trestnej činnosti, avšak aj tieto zariadenia mohli byť na spáchanie trestnej činnosti použité (televízne systémy, ktoré mohli byť využité ako obrazovky/monitory a pod.).
2. Pripojenia jednotlivých počítačových systémov do internetovej siete. Je nevyhnutné, aby vyšetrovateľ, resp. prizvaný znalec, identifikoval spôsob pripojenia jednotlivých systémov do počítačovej alebo internetovej siete a zároveň určil jednotlivých poskytovateľov internetových služieb, ktorí obvinenej osobe alebo páchateľovi trestného činu poskytovali internetové pripojenie. Znalec môže pri analýze pripojení zistiť aj ďalšie skutočnosti, napríklad že počítačový systém využitý páchateľom využíval aj pripojenie k vzdialeným dátovým úložiskám.
3. Pripojenie počítačového systému do lokálnej počítačovej siete. Znalec v uvedenej súvislosti musí identifikovať topológiu siete, vzájomné prepojenie počítačových systémov medzi sebou, ďalej musí identifikovať aj konkrétne umiestnenie jednotlivých počítačových systémov, určiť kompetencie jednotlivých osôb spojené s prístupom do jednotlivých častí počítačovej siete, resp. do informačného systému ako celku,
4. Ďalšie informácie, ktoré sú relevantné pre zaistenie stôp a ďalší priebeh vyšetrovania.[45]

Odňatie výpočtovej techniky predstavuje významný zásah do osobných práv osoby. Ak to nie je nevyhnutné, Šándor[46] v súlade so zásadou primeranosti odporúča neodnímať výpočtovú techniku úplne, ale v mieste vykonávania prehliadky vyhotoviť obraz pevného disku (kópiu súborov alebo pamäte počítača). Na tieto úkony je však potrebné k prehliadke pribrať znalca. Nutnosť pribrať znalca k domovej prehliadke môže byť definovaná aj priamo v príkaze na vykonanie domovej prehliadky, t. j. osoba, ktorá je kompetentná vydať príkaz na domovú prehliadku, môže uviesť, že k domovej prehliadke alebo na prehliadke iných priestorov má byť osobitným uznesením podľa Trestného poriadku[47] uznesením o pribratí znalca pribraný znalec z príslušného odboru, ktorý má vykonať technické a následne znalecké úkony smerujúce k zaisteniu digitálnych, resp. počítačových stôp v konkrétnom rozsahu (jednotky výpočtovej techniky, nosiče dát, počítačové údaje a pod.). Znalec zároveň poskytuje odbornú súčinnosť vyšetrovateľovi priamo v mieste prehliadky, a to na základe jeho požiadaviek.[48]

Pribratie znalca je v prípade počítačových trestných činov dôležité, keďže len znalec dokáže objektívne posúdiť, či je do počítača alebo inej výpočtovej techniky možné vstúpiť priamo v mieste prehliadky a vyhľadať požadované údaje, alebo je potrebné výpočtovú

[45] KOLOUCH, J. *Cybercrime,* s. 516.
[46] ŠÁNDOR, M. Praktické spôsoby zaisťovania počítačových údajov v trestnom konaní. In: *Poradca policajta*. [online]. 2018. [cit 3. februára 2026]. Dostupné na internete: https://poradcapolicajta.sk/prakticke-sposoby-zaistovania-pocitacovych-udajov-v-trestnom-konani/
[47] *§ 142 ods.1 Zákona č. 301/2005 Z. z. Trestný poriadok* (veta prvá)
[48] ŠÁNDOR, M. Praktické spôsoby zaisťovania počítačových údajov v trestnom konaní. In: *Poradca policajta*. [online]. 2018. [cit. 3. februára 2026]. Dostupné na internete: https://poradcapolicajta.sk/prakticke-sposoby-zaistovania-pocitacovych-udajov-v-trestnom-konani/

techniku nachádzajúcu sa v mieste prehliadky zabezpečiť (napríklad ak je prístup do počítača chránený heslom alebo PIN kódom). V kompetencii znalca je zároveň posúdenie skutočnosti, či sa zaistí výpočtová technika ako celok, alebo bude postačujúce vytvoriť a skopírovať súbory.[49]

Odňatie výpočtovej techniky je vhodné v prípadoch, ak by vyhľadanie požadovaných súborov či kopírovanie priečinkov priamo na mieste výkonu prehliadky trvalo dlhší čas, napríklad niekoľko hodín. Uvedená skutočnosť by na jednej strane neúmerne predĺžila prehliadku, na strane druhej by táto skutočnosť negatívne zasiahla aj do práv osoby, u ktorej sa daná prehliadka vykonáva. Predĺženie prehliadky spojené s kopírovaním dát by bolo navyše personálne aj technicky náročné. V uvedenom prípade je vhodnejšie zaistiť výpočtovú techniku ako celok vrátane vytvorenia obrazu pevného disku. Následne, po zaistení veci dôležitej pre trestné konanie, môže znalec pokračovať vo vyhľadávaní digitálnej stopy bez časového obmedzenia, čo mu umožňuje vyhľadať aj skryté či odstránené súbory alebo priečiny, ktoré môžu byť zásadné pre priebeh vyšetrovania.[50]

1.3.2 Uchovanie, vydanie a odňatie počítačových údajov

Nevyhnutným dôkazom, ktorý je potrebné zaistiť v prípade počítačových trestných činov, je tzv. digitálna, resp. počítačová stopa. Ide o typ stopy, ktorý je dôležitý nielen pri odhaľovaní a dokazovaní počítačových trestných činov, ktorých cieľom je počítač (t. j. trestný čin neoprávneného obohatenia, trestný čin neoprávneného prístupu do počítačového systému, neoprávnený zásah do počítačového systému alebo počítačového údaja a pod.) a trestných činov s aktívnym využitím počítača (trestné činy spojené s porušovaním autorského práva, trestné činy sexuálneho zneužívania a trestné činy spojené s pornografiou), ale aj pri trestných činoch, pri páchaní ktorých má počítač vedľajšiu úlohu. V uvedenom kontexte ide napríklad o trestné činy proti majetku, trestné činy páchané v hospodárskej oblasti a pod.[51]

Možnosť nielen odňať (ale napr. aj uchovať, vyhotoviť kópie a pod.) počítačové údaje ako jeden z dôkazov je upravený v § 91 Trestného poriadku.[52] Uvedené ustanovenie implementuje príslušné články Dohovoru o počítačovej kriminalite[53], podľa ktorého každá zmluvná strana, ktorá prijala dohovor, bola povinná prijať opatrenia nevyhnutné na to, aby príslušným orgánom bolo umožnené nariadiť uchovanie špecifikovaných počítačových údajov uložených prostredníctvom počítačového, resp. informačného systému a v prípade, že je to nutné, nariadiť aj vydanie týchto údajov príslušným orgánom. Osoba, ktorá sa nachádza na území zmluvnej strany, je zároveň podľa Dohovoru o počítačovej kriminalite povinná predložiť špecifikované počítačové údaje, ktoré má v držbe alebo pod kontrolou v počítačovom systéme alebo na inom nosiči (externý disk a pod.).[54]

Inštitút uchovania, vydania a odňatia počítačových údajov predstavuje výrazný zásah do súkromia osôb, u ktorých sa má tento inštitút realizovať. V tomto prípade je však zásah do súkromia relevantný, keďže verejný záujem na objasnení trestnej činnosti prevažuje nad

[49] KOLOUCH, J. *Cybercrime,* s. 516.
[50] ŠÁNDOR, M. Praktické spôsoby zaisťovania počítačových údajov v trestnom konaní. In: *Poradca policajta*. [online]. 2018. [cit. 3. februára 2026]. Dostupné na internete: https://poradcapolicajta.sk/prakticke-sposoby-zaistovania-pocitacovych-udajov-v-trestnom-konani/
[51] KOLOUCH, J. *Cybercrime,* s. 516.
[52] *Zákon č. 301/2005 Z. z. Trestný poriadok.*
[53] *Dohovor o počítačovej kriminalite*. [online]. [cit. 3. februára 2026]. Dostupné na internete: https://rm.coe.int/16802fa420
[54] STRAUS, J. a kol. 2008. *Kriminalistická metodika*. Plzeň: Aleš Čeněk, 2008, s. 320.

právom jednotlivca a ochranou jeho súkromia.[55] Je však dôležité, aby právo na súkromie bolo narušené v čo najmenšej možnej miere, pričom k odňatiu hmotných nosičov, na ktorých sa tieto dáta nachádzajú, je možné len v prípade, že uvedený zásah je legitímny, legálny a zároveň nevyhnutný.[56] Výpočtovú techniku pri prehliadke tak nie je v odôvodnených prípadoch nevyhnutné zaistiť.[57]

Príkaz na uchovanie, vydanie a odňatie počítačových údajov musí okrem všeobecných náležitostí uvedených v § 181 Trestného poriadku (označenie orgánu, o ktorého rozhodnutie ide, skutok s uvedením právnej kvalifikácie trestného činu a pod.) obsahovať aj ďalšie náležitosti konkretizujúce tieto dáta.[58] Príkaz teda obsahuje typ údajov, lehotu vydania, formu, v akej majú byť tieto údaje vydané (text, online súbor, napríklad internetová stránka) a tiež konkrétny nosič dát (USB disk, CD-R a pod.). Príkaz musí zároveň obsahovať aj odôvodnenie, keďže podľa Ústavného súdu SR je konkrétny príkaz bez náležitého odôvodnenia opierajúceho sa o konkrétne skutočnosti nepreskúmateľný, a teda svojvoľný.[59] Ak náležité odôvodnenie príkazu absentuje, nie je možné zodpovedne posúdiť primeranosť zásahu do práva sťažovateľa na súkromie.[60]

Ustanovenie § 91 Trestného poriadku umožňuje zaistenie dvoch druhov počítačových údajov, a to buď vlastné počítačové údaje užívateľa, alebo prevádzkové údaje.[61]

Vlastné počítačové údaje sú definované v Dohovore o počítačovej kriminalite ako akékoľvek znázornenie faktov, pojmov alebo informácií, a to vo forme vhodnej na spracovanie v informačnom systém vrátane programu, ktorý umožňuje nariadiť výkon vybranej funkcie počítačovým systémom.[62] Vhodnosť údajov na spracovanie v rámci počítačového systému znamená, že počítačové údaje musia byť uložené vo forme umožňujúcej ich okamžité spracovanie počítačovým systémom, t. j. v priamo spracovateľnej podobe. Ide napríklad o grafické, audiovizuálne, textové súbory, databázy, počítačové programy a pod. Nie je podstatné, či sú tieto dáta umiestnené na serveroch, v osobných počítačoch, ako obsah internetových stránok a pod.[63]

Prevádzkové údaje sa podľa Dohovoru o počítačovej kriminalite vzťahujú na identifikáciu používateľa.[64] Ide o akékoľvek počítačové dáta súvisiace s komunikáciou prostredníctvom informačného (počítačového) systému, resp. dáta generované počítačovým systémom, ktorý tvoril súčasť reťazca komunikácie, a to vrátane uvedenia pôvodu, cieľa, času, objemu, trasy, dátumu, trvania komunikácie alebo typu základnej služby. Prevádzkové údaje sa vzťahujú na užívateľa vrátane konkrétneho prenosu informácií v sieti. Ide o dáta, ktoré netvoria obsah komunikácie, t. j. v rámci komunikácie predstavujú len pomocné dáta.

---

[55] ZÁHORA, J., I. ŠIMOVČEK, P. POLÁK a kol. 2025. *Zákon č. 301/2005 Z. z. Trestný poriadok. Komentár*, 1205 s.
[56] *II. ÚS 386/2014*.
[57] ŠÁNDOR, M. Praktické spôsoby zaisťovania počítačových údajov v trestnom konaní. In: *Poradca policajta*. [online]. 2018. [cit. 3. februára 2026]. Dostupné na internete: https://poradcapolicajta.sk/prakticke-sposoby-zaistovania-pocitacovych-udajov-v-trestnom-konani/
[58] *§ 181 Zákona č. 301/2005 Z. z. Trestný poriadok.*
[59] *II. ÚS 78/2019.*
[60] *II. ÚS 53/2010.*
[61] *§ 91 Zákona č. 301/2005 Z. z. Trestný poriadok.*
[62] Dohovor o počítačovej kriminalite. [online]. [cit. 3. februára 2026] Dostupné na internete: https://rm.coe.int/16802fa420.
[63] ZÁHORA, J., I. ŠIMOVČEK, P. POLÁK a kol. *Zákon č. 301/2005 Z. z. Trestný poriadok. Komentár*, 1205 s.
[64] Dohovor o počítačovej kriminalite. [online]

V praxi ide o IP adresu užívateľa, telefónne číslo, druh koncového zariadenia a pod.[65] Podľa zákona o elektronických komunikáciách sa prevádzkové údaje, ktoré sa týkajú účastníkov a používateľov, nesmú uchovávať, pričom podnik poskytujúci tieto služby je povinný tieto údaje po skončení prenosu bezodkladne zlikvidovať alebo anonymizovať.[66] Povinnosť uchovávať prevádzkové, lokalizačné údaje a údaje týkajúce sa komunikujúcich strán je podnik poskytujúci tieto služby povinný uchovávať len v prípadoch uvedených v zákone, resp. v prípade, ak sa na tieto údaje vzťahuje dodatočný súhlas súdu (podľa zákona o elektronických komunikáciách) alebo príkaz súdu podľa trestného poriadku.

V kontexte zaistenia počítačových údajov je následne dôležité aj ich uchovanie. Inštitút uchovania počítačových údajov znamená, že je dôležité zabrániť ich poškodeniu, vymazaniu alebo pozmeneniu. Údaje, ktoré boli zaistené, musia byť uchované celistvo. Šándor v kontexte zaistenia počítačových údajov, resp. digitálnych stôp uvádza, že pri ich zaistení znalec využíva špeciálny program overujúci integritu súborov, tzv. MD5 (md5sum). Program prostredníctvom špeciálneho kľúča vytvorí digitálny odtlačok súborov umiestnených na disku počítača, ktorý zároveň prepočíta na kontrolnú sumu. Uvedenú sumu je dôležité poznamenať do zápisnice o prehliadke. Práve táto suma totiž potvrdzuje, že s dátami, ktoré boli získané zo zaistenej výpočtovej techniky, žiadna osoba ďalej nemanipulovala, t. j. zaistené dáta sú identické s dátami, ktoré boli zaistené v mieste výkonu prehliadky. Akákoľvek manipulácia s dátami (vymazanie alebo pridanie súboru, premenovanie priečinku a pod.) by mala za následok zmenu prepočítanej kontrolnej sumy.[67] Použitie špeciálneho softvéru znalcom je tak v konečnom dôsledku v záujme vyšetrovateľa, keďže v priebehu vyšetrovania nemôžu vzniknúť pochybnosti o tom, že dáta z výpočtovej techniky boli následne pozmenené.

1.3.3 Zaistenie kryptoaktíva

Zaistenie kryptoaktíva (v minulosti kryptomeny alebo aj virtuálna mena) je špecifikované v § 96d Trestného poriadku. Predseda senátu alebo prokurátor (v prípade prípravného konania) môže vydať príkaz na zaistenie kryptoaktíva v prípade, ak zistené skutočnosti nasvedčujú skutočnosti, že kryptoaktívum (napríklad Bitcoin) predstavuje nástroj trestnej činnosti, resp. ide o výnos z trestnej činnosti. Inštitút zaistenia kryptoaktíva teda predstavuje špecifickú formu zaistenia nástrojov, resp. výnosov, ktoré mohli byť získané trestnou činnosťou.[68]

Za kryptoaktívum sa podľa definície Národnej banky Slovenska považuje decentralizovane vydávané digitálne aktívum založené na kryptografii.[69] Kryptoaktívum spravidla funguje na blockchainovej technológii. Pre kryptoaktíva je typická vysoká volatilita, absencia centralizovaného riadiaceho orgánu a v neposlednom rade aj vysoký inovačný

[65] ZÁHORA, J., I. ŠIMOVČEK, P. POLÁK a kol. 2025. *Zákon č. 301/2005 Z. z. Trestný poriadok. Komentár*. Bratislava: ASPI, 2025, 1205 s.
[66] *§ 111 ods. 1 Zákona č. 452/2021 Z. z. o elektronických komunikáciách*.
[67] ŠÁNDOR, M. Praktické spôsoby zaisťovania počítačových údajov v trestnom konaní. In: *Poradca policajta*. [online]. 2018. [cit. 3. februára 2026]. Dostupné na internete: https://poradcapolicajta.sk/prakticke-sposoby-zaistovania-pocitacovych-udajov-v-trestnom-konani/
[68] Zákon č. 301/2005 Z. z. Trestný poriadok.
[69] NÁRODNÁ BANKA SLOVENSKA. In: *Čo sú kryptoaktíva?* [online]. 2025. [cit. 3. februára 2026]. Dostupné na internete: https://nbs.sk/dohlad-nad-financnym-trhom/fintech/financne-technologie/co-su-kryptoaktiva/

potenciál.[70] Kryptoaktíva sú v súčasnosti regulované viacerými nástrojmi. V EÚ ide predovšetkým o nariadenie Európskeho parlamentu a Rady známe ako MiCA.[71]

V prípade, že vec neznesie odklad (napríklad ak na základe zistených skutočností vyšetrovateľa je možné argumentovať, že páchateľ trestnej činnosti pripravuje prevod kryptoaktíva), môže prokurátor vydať príkaz na zaistenie kryptoaktíva ešte predtým, než sa začne trestné stíhanie. Neznesenie odkladu je v tomto prípade zákonnou podmienkou pre vydanie príkazu prokurátorom. Príkaz však musí potvrdiť do 48 hodín sudca, v opačnom prípade je príkaz neplatný a zaistenie sa zruší.

1.4 Dokazovanie počítačových trestných činov

Dokazovanie je upravené v § 119 a nasl. Trestného poriadku. V rámci trestného konania je nevyhnutné dokázať predovšetkým:[72]

a) či sa skutok stal a či aj skutočne tento skutok vykazuje znaky trestného činu;
b) aký aktér tento skutok spáchal a z akej pohnútky, resp. pohnútok;
c) aká je závažnosť spáchaného trestného činu, aké boli príčiny vedúce k jeho spáchaniu a za akých podmienok bol tento trestný čin spáchaný;
d) osobné pomery páchateľa trestného činu, a to v rozsahu, ktorý je nevyhnutý na identifikáciu druhu a výmeru trestu, uloženie ochranného opatrenia alebo iného rozhodnutia;
e) následok trestného činu a výšku škody, ktorá bola trestným činom spôsobená;
f) aký bol výnos zo spáchanej trestnej činnosti, aké prostriedky sa použili na jej spáchanie, kde boli výnosy z trestnej činnosti umiestnené, aká je ich povaha, stav, hodnota;
g) aké sú majetkové pomery páchateľa trestného činu (s cieľom identifikovať možnosti odňatia výnosov, ktoré získal trestnou činnosťou).

V rámci dokazovania je možné využiť viaceré zaisťovacie prostriedky, ktoré sa používajú na účel realizácie úkonov trestného konania, napríklad predvolanie a predvedenie obvineného[73] za účelom výsluchu obvinenej osoby,[74] prípadne výsluchu svedkov.[75]

Dokazovanie je však špecifické pre každý druh kriminality, pričom v prípade kybernetickej kriminality je nevyhnutné zistiť aj:[76]

a) či bol spáchaný iba jeden alebo viaceré trestné činy;
b) informácie týkajúce sa útoku (ak bol spáchaný napríklad DoS, DDoS útok), predovšetkým čas spáchania útoku, štruktúra a dĺžka útoku, zdroje útoku, škoda spôsobená kybernetickým útokom, a to bez ohľadu na to, či ide o primárnu alebo sekundárnu škodu;
c) informácie o počítačovom systéme páchateľa trestného činu (aký počítačový systém bol v rámci siete koncovým prípojným bodom, na ktorom informačnom systéme došlo

[70] HOSP, J. *Kryptomeny,* s. 39 – 40.
[71] *Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937*.
[72] ZÁHORA, J., I. ŠIMOVČEK, P. POLÁK a kol. 2025. *Zákon č. 301/2005 Z. z. Trestný poriadok. Komentár*, 1205 s.
[73] *§ 120 Zákona č. 301/2005 Z. z. Trestného poriadku*.
[74] *§ 121a nasl. Zákona č. 301/2005 Z. z. Trestného poriadku*.
[75] *§ 131 a nasl. Zákona č. 301/2005 Z. z. Trestného poriadku*.
[76] KOLOUCH, J. *Cybercrime*, s. 516.

k realizácii protiprávneho konania, ktoré počítačové systémy sa stali cieľom útoku, aká je verzia operačného systému, aký softvér bol pri útoku využitý, aké počítačové systémy/softvéry boli napadnuté, spôsob pripojenia počítača do počítačovej siete a pod.);

d) informácie o dátach (akú povahu majú poškodené, odcudzené alebo potlačené dáta, čo sa nachádza na zaistených zariadeniach, aký softvér je nainštalovaný v zabavených počítačových systémoch);
e) informácie o páchateľovi (akým spôsobom spáchal trestný čin, či ide o jedného alebo viacerých páchateľov, aké znalosti má páchateľ trestného činu o informačných a komunikačných technológiách, aký mal páchateľ motív spáchať trestný čin a pod.);
f) aké boli okolnosti, ktoré umožnili spáchanie trestného činu;
g) informácie o nastavení počítačového systému, dátových úložiskách, oprávneniach nastavených na napadnutých počítačových systémoch a pod.

Výsluch obvinenej osoby sa riadi všeobecnými pravidlami definovanými v Trestnom poriadku.[77] V prípade spáchania počítačového trestného činu je však potrebné zistiť aj viaceré špecifické skutočnosti, medzi ktoré patria napríklad pomery obvineného (osobné, majetkové, aká je zárobková činnosť obvinenej osoby), informácie týkajúce sa úmyslu, ktoré páchateľa viedli k spáchaniu trestného činu, informácie o tom, či sa na spáchaní trestného činu podieľala iba jedna osoba alebo viaceré osoby, či obvinená osoba pri spáchaní počítačového trestného činu využila prvky sociálneho inžinierstva alebo aj ďalšie iné netechnické prostriedky. Medzi ďalšie špecifické skutočnosti, ktoré sa zisťujú v prípade spáchania počítačového trestného činu, patrí aj identifikácia mechanizmov spojených so zásahom do informačného systému alebo programového vybavenia informačného systému, akým spôsobom sa páchateľ trestného činu dozvedel o tom, akú konkrétnu činnosť má vykonať, akým spôsobom sa túto činnosť snažil zamaskovať apod.

Veľmi dôležitým je pri spáchaní počítačového trestného činu aj znalecký posudok vrátane výsluchu znalca, ktorý musí byť prítomný v prípade zaisťovania stôp týkajúcich sa kybernetickej kriminality. Účasť znalca sa môže vyžadovať *de facto* z dvoch dôvodov, ktorými je buď obhliadka znalca na mieste činu (pričom znalec má v tomto prípade poradnú, konzultačnú úlohu), alebo samotné zaistenie počítačových systémov a dát. Hlavné využitie znalca však spočíva v jeho vlastnej znaleckej činnosti, výstupom ktorej je znalecký posudok. V posudku sa znalec vyjadruje predovšetkým k nasledovnej problematike:[78]

1. Základná identifikácia a charakteristika hardvérovej konfigurácie skúmaného informačného systému.
2. Výsledok skúmania nosičov, na ktorých sa nachádzali zaistené dáta. Znalec pre potreby súdu vytvára kópiu týchto dát.
3. Zadokumentovanie a rozdelenie zaistených dát a ich rozdelenie.
4. Súborová štruktúra údajov, a to vrátane zmazaných súborov, ktoré znalec v rámci štruktúry dát samostatne vyznačí.
5. Obnova zmazaných dát na zaistených dátových nosičoch informácií.
6. Vyhľadanie zaheslovaných alebo inak zašifrovaných súborov, možnosť ich dešifrovania a zadokumentovanie výsledku.
7. Zadokumentovanie užívateľských účtov počítačového systému, určenie prístupových práv k účtom, a to vrátane prístupových hesiel k týmto účtom.
8. Identifikácia parametrov internetového pripojenia a tiež nastavení, ktoré boli pri spáchaní počítačového trestného činu používané.

[77] *§ 121a nasl. Zákona č. 301/2005 Z. z. Trestného poriadku.*
[78] KOLOUCH, J. *Cybercrime,* s. 516.

9. Zadokumentovanie emailovej komunikácie, selekcia emailových správ. Zadokumentovanie ďalšej internetovej komunikácie realizovanej cez rôzne programy, a to nielen komunikácie uloženej v počítačovom systéme, ale aj komunikácie z obnovených dát.
10. Analýza súborov vytvorených v MS Office, uvedenie dostupných informácií z týchto súborov.
11. Vyhľadanie dát s vybranými slovnými reťazcami (určené vyšetrovateľom).
12. Vyhľadanie súborov v rámci archivačných programov, extrakcia dát z týchto programov.
13. Analýza grafických súborov, uvedenie dostupných informácií.
14. Zadokumentovanie histórie navštívených internetových stránok nachádzajúcich sa v jednotlivých internetových prehliadačoch.
15. Vytvorenie výpisu vrátane náhľadu vybraných súborov a zložiek so špecifickým obsahom (napríklad súbory s detskou pornografiou).
16. Spracovanie výpisu nainštalovaného softvéru vrátane jeho rozdelenia na voľné šíriteľný softvér a komerčný softvér. V prípade, že ide o komerčný softvér, identifikuje znalec vlastníka autorských práv, cenu licencie a prípadné ďalšie náležitosti (zastúpenie vlastníka autorských práv na Slovensku a pod.).
17. Identifikácia, či na zaistenej výpočtovej technike (resp. hardvérovom vybavení) mohol byť spustený konkrétny typ softvéru, ktorý umožnil spáchanie trestného činu.
18. Kontrola počítačového systému a identifikácia, či sa v rámci tohto systému nachádza alebo nenachádza škodlivý softvér, prostredníctvom ktorého by mohla osoba ovládať iný počítačový systém, získať prístupové kódy k platobným kartám, prístupové heslá a pod.
19. Vyjadrenie znalca k zaisteniu počítačového systému v kontexte externej intervencie (prieniku) do systému. Identifikácia, či zaistený počítačový systém javil prípadné známky po takomto prieniku, aké mohol mať tento prienik následky, s akým cieľom bolo do informačného systému preniknuté a pod.
20. Uvedenie ďalších skutočností, ktoré môžu mať vzťah k vyšetrovaniu prípadu, ak ich je dôležité ich zo strany znalca špecifikovať[79].

K posudku znalca sa štandardne pripájajú aj vybrané dáta, ktoré boli pri domovej prehliadke zaistené. Údaje, ktoré znalec alebo vyšetrovateľ zaistil, štandardne zostávajú v elektronickej podobe, pričom sú uložené na pamäťovom médiu.

Záver

V odbornom článku som sa zaoberal odhaľovaním a dokazovaním počítačovej kriminality v legislatívnych podmienka SR. Pracoval som s hypotézou, že vývoj bezpečnosti v kybernetickom priestore úzko koreluje s vývojom kriminality páchanej v tomto priestore, čomu je nevyhnutné dynamicky prispôsobovať aj smerovanie odhaľovania a dokazovania počítačovej kriminality.

Vzhľadom na výrazný progres v oblasti kybernetiky, robotizácie či digitalizácie spoločnosti je možné aj v budúcnosti očakávať revidovanie legislatívnych dokumentov platných v súčasnosti a tiež vytváranie nových legislatívnych aktov regulujúcich prostredie a chrániacich bezpečnosť používateľov siete, softvéru, informačných a komunikačných prostriedkov.

[79] Vlastné poznanie, zvyčajne uvedené v unesení o pribratí znalca zadaním na znalca aby uviedol iné zistenia dôležité pre posúdenie veci

Literatúra

GOEL, Sanjay a kol. *Digital Forensis and Cyber Crime*. New York: Springer, 2010, s. 184.

HOSP, Julian. *Kryptomeny*. Bratislava: Tatran, 2021, s. 39 – 40.

KOLOUCH, Jan. 2016. *Cybercrime*. Praha: CZ.NIC, 2016, s. 516.

MOKRÁ, Jana. Methodology of detection and investigation of the crime of human trafficking. In: *Projustice* [online]. 2023. [cit. 3. februára 2026]. Dostupné na internete: https://www.projustice.sk/trestne-pravo/metodika-odhalenia-a-vysetrovanie-trestneho-cinu-obchodovania-s-ludmi

PORADA, Viktor a STRAUS, Jiří. *Kriminalistické stopy. Teorie, metodologie, praxe*. Plzeň: Aleš Čeněk, 2012, s. 512.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2022, s. 640.

STRAUS, Jiří a kol. *Kriminalistická metodika*. Plzeň: Aleš Čeněk, 2008, s. 320.

ŠAMKO, Peter. *Daňové podvodné konania a ich dokazovanie*. Bratislava: Wolters Kluwer, 2015

ŠÁNDOR, Michal. 2018. Praktické spôsoby zaisťovania počítačových údajov v trestnom konaní. In: *Poradca policajta*. [online]. 2018. [cit. 3. februára 2026]. Dostupné na internete: https://poradcapolicajta.sk/prakticke-sposoby-zaistovania-pocitacovych-udajov-v-trestnom-konani/

ZÁHORA, Jozef. Zaisťovanie digitálnych dôkazov v cezhraničných situáciách. In: *Časopis pro právní vědu a praxi*, 2019, roč. 27, č. 1.

ZÁHORA, Jozef, Ivan ŠIMOVČEK, Peter POLÁK a kol. 2025. *Zákon č. 301/2005 Z. z. Trestný poriadok. Komentár*. Bratislava: ASPI, 2025, s. 1205.

Zákon č. 301/2005 Z. z. Trestný poriadok.

Dohovor o počítačovej kriminalite. [online]. [cit. 3. februára 2026]. Dostupné na internete: https://rm.coe.int/16802fa420.

Nález Ústavného súdu SR II. ÚS 386/2014.

Nález Ústavného súdu SR II. ÚS 78/2019.

Nález Ústavného súdu SR II. ÚS 53/2010.

Zákon č. 452/2021 Z. z. o elektronických komunikáciách.

Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1114 z 31. mája 2023 o trhoch s kryptoaktívami a o zmene nariadení (EÚ) č. 1093/2010 a (EÚ) č. 1095/2010 a smerníc 2013/36/EÚ a (EÚ) 2019/1937.

NÁRODNÁ BANKA SLOVENSKA. In: *Čo sú kryptoaktíva?* [online]. 2025. [cit. 3. februára 2026]. Dostupné na internete: https://nbs.sk/dohlad-nad-financnym-trhom/fintech/financne-technologie/co-su-kryptoaktiva/

Keywords: cyber atack, computer crime, digital trace, investigation, cryptoactiva

Summary

The article is organized into one thematic chapter and six subchapters. The main topic of the article is the detection and evidence of computer crime in the conditions of the

legislation of the Slovak Republic. In the first subchapter, I discuss approaches to the investigation of criminal offenses. In the following chapters, I present individual institutes of criminal law that can be used in the investigation of computer crime offenses. I discuss in detail individual institutes of criminal law such as home search and seizure of traces, securing digital traces, seizing computer equipment, seizure of computer data, seizing crypto assets. In the last subchapter, I elaborated on the evidence of computer crime. To achieve the goal of the article and verify the hypothesis, the methods of description, analysis, synthesis and deduction are used.

JUDr. Martin Bicko, Paneurópska vysoká škola,
Fakulta práva
Katedra trestného práva
Advokátska kancelária JUDr. Martin Bicko,
advokát s.r.o.
e-mail: bicko@advokatbicko.sk

Recenzent: plk. doc. JUDr. Veronika Marková, PhD.