Paneurópske právnické listy
ISSN: 2644-450X (online)

Ročník/Volume: **1**
Číslo/Number: **1**
Rok/Year: **2018**

Vybrané kriminalistické osobitosti počítačovej kriminality
Selected criminalistic peculiarities of cybercrime

Mgr. Dávid Lučivjanský
Paneurópska vysoká škola, Fakulta práva, Ústav verejného práva

Anotácia

Odborný článok sa zaoberá počítačovou kriminalitou so zreteľom na dokazovanie. Venuje sa špecifikám vyšetrovania, objasnenia počítačových deliktov a ich konkrétnym problémom. Článok má 7 strán a pozostáva z 5 tématických častí.

Annotation

Scholarly article deals about cyber crime with focus on evidence. It addresses the specifics of investigation, clarifying cyber crimes and their specific problems. The article has 7 pages and contains 5 thematic parts.

Kľúčové slová

počítačová kriminalita, dôkazy, vyšetrovanie, páchateľ počítačovej kriminality

Key words

cybercrime, evidence, investigation, cyber criminals

I. Úvod

S kontinuálnym vývojom moderných informačných a komunikačných technológií je spájaná aj narastajúca trestná činnosť v tomto odvetví, s ktorou súvisí jej stále veľmi náročné odhaľovanie. Pri objasňovaní trestnej činnosti je na základe zaistených stôp možná individuálna identifikácia páchateľa. Takéto stopy sú zväčša zaistené na mieste činu, čo je pre orgány činné v trestnom konaní indikátorom vedúcim ku konkrétnym osobám.

Naopak, vyšetrovaniu počítačovej kriminality táto výhoda chýba, pretože stopy v kyberpriestore vedú ku koncovému zariadeniu, z ktorého bolo porušenie urobené a teda nie priamo ku konkrétnej osobe. Na základe týchto skutočností prichádza do úvahy rad nepriamych dôkazov, ktoré by takúto skutočnosť potvrdili či vyvrátili. Možno tak konštatovať, že stopy v kyberpriestore nie sú priamo oprávnené k individuálnej identifikácii osoby páchateľa.

II.

1. Ochrana verejného záujmu ako (opomínaná) procesná zásada/procesný princíp (?)

Počítačovú kriminalitu považujeme za kriminalitu páchanú predovšetkým skryto. Aj keď trestné činy súvisiace s počítačmi, respektíve internetom, majú často charakter trvajúcich alebo pokračujúcich

deliktov, dochádza k tomu, že počítačová kriminalita je málokedy odhalená a páchateľ je zriedkakedy vôbec trestne stíhaný či dokonca odsúdený. Na základe dostupných štatistík Ministerstva vnútra môžeme tvrdiť, že objasnenosť trestných činov počítačovej kriminality je veľmi malá.[1]

Je možné domnievať sa, že jedným z hlavných dôvodov, prečo dochádza k tak vysokej latencii pri trestných činoch počítačovej kriminality, je veľmi rýchly časový sled udalostí, ktoré prebiehajú v rámci páchania a odhaľovania počítačovej kriminality. Ak je páchateľ predčasne upozornený o potenciálnom záujme policajných orgánov o jeho nekalú činnosť, môže prakticky okamžite konať vo svoj prospech a tým pádom včas zničiť kriminalistické stopy.

Podľa viacerých zdrojov literatúry sú výsledky operatívno-pátracej činnosti typickým a najmä základným zdrojom informácií o trestnej činnosti v prípade počítačovej kriminality. Takéto tvrdenie je možné spochybniť, keďže viac ako polovica páchanej trestnej činnosti pochádza z trestných oznámení. Tieto podnety na rozdiel od vlastných poznatkov policajného orgánov bývajú často motivované individuálnymi záujmami poškodeného na náhrade škody spôsobenej trestným činom (napríklad krádež citlivých informácií alebo peňazí prostredníctvom internetbankingu). V prípadoch trestných oznámení je potrebné taktiež prihliadať na motív oznamovateľa. Je to predovšetkým z dôvodu zamedzenia neopodstatnených alebo nepravdivých oznámení.[2]

Jedným z ďalších podnetov k vyšetrovaniu sú oznámenia inšpekčných, kontrolných a revíznych orgánov jednotlivých inštitúcií. Takéto oznámenia by mali byť ťažiskom oznamovania počítačovej trestnej činnosti. Prax však ukazuje, že obete takýchto trestných činov z rôznych dôvodov nemajú záujem o zaoberanie sa počítačovými deliktmi orgánmi činnými v trestnom konaní. Môže za to napríklad páchanie iných trestných činov, ktoré by mohli byť vyšetrovacou činnosťou orgánov činných v trestnom konaní odhalené, ochrana dobrého mena alebo z iných subjektívnych dôvodov.

Pracovnou náplňou týchto inšpekčných, kontrolných a revíznych orgánov je sledovanie nezrovnalostí vo finančných a peňažných ústavoch. Ak tieto orgány odhalia určitú nezrovnalosť a uznajú, že nejde o administratívnu chybu, môžu podať podnet na vyšetrovanie, ktorý je však potrebné preveriť, doplniť a spresniť.

Dôležitým je predovšetkým spôsob, akým je konkrétny podnet k vyšetrovaniu počítačovej kriminality daný. Externé podnety je potrebné preverovať, na rozdiel od informácií získaných operatívno-pátracou činnosťou policajných orgánov. Presnosť, pravdivosť a úplnosť externých podnetov nemusí byť absolútna. Včasnosť zaistenie kriminalistických stôp je kľúčová a ovplyvňuje počiatočnú vyšetrovaciu situáciu a úspech celého vyšetrovania.[3]

2. Počiatočné vyšetrovacie situácie

Počiatočnou vyšetrovacou situáciou rozumieme stav, v ktorom sa nachádza vyšetrovanie v momente získania prvotných informácií o čine. Tento stav má zásadný význam pre úspech vyšetrovania, pretože ten závisí na jej zvládnutí. Počiatočná vyšetrovacia situácia je determinovaná tým, z akého zdroja pochádzajú prvotné informácie o spáchanom delikte.

Medzi počiatočné vyšetrovacie situácie počítačovej kriminality zaraďujeme napríklad, ak:

a) Zistené skutočnosti nasvedčujú tomu, že sa stal skutok, v ktorom možno badať skutkovú podstatu určitého trestného činu, no nedá sa vysloviť jednoznačný záver o totožnosti páchateľa a spôsobe spáchania trestného činu.

Takáto vyšetrovacia situácia je priaznivá najmenej. Vyšetrovateľ sa najprv zameriava na zistenie informácií o možnom spôsobe spáchania trestného činu a informácií, vďaka ktorým by bolo možné odhaliť totožnosť páchateľa.

Elementárnou úlohou je pribrať znalca z odboru výpočtovej techniky a po konzultácii s ním zaistiť materiály k počítačovej expertíze. V prípade, že sa pred zaistením s počítačovým systémom alebo s nosičmi informácií manipulovalo, je nutné požadovať vysvetlenie kto, prečo a akým spôsobom s nimi manipuloval.

Za tejto počiatočnej situácie, najmä pokiaľ je poškodenou osobou väčšia právnická osoba, je potrebné zachovať dôvernosť informácií zo strany poškodenej inštitúcie. V takýchto prípadoch existuje predpoklad, že páchateľ by mohol pochádzať práve z radov zamestnancov a rozšírenie informácie o vykonávanom vyšetrovaní by ho mohlo upozorniť a prebiehajúce vyšetrovanie by sa mohol pokúšať mariť.

b) Zistené skutočnosti nasvedčujú tomu, že sa stal skutok, ktorý vykazuje všetky znaky trestného činu, a objasňujú spôsob spáchania trestného činu. Nemožno však vysloviť záver o totožnosti páchateľa.

V týchto prípadoch sa vyšetrovateľ zameriava predovšetkým na získanie informácií ohľadom totožnosti páchateľa. Ak je známy spôsob vykonania trestného činu, značne to môže zúžiť okruh potencionálnych páchateľov. Je vhodné opäť pribrať znalca z odboru výpočtovej techniky. Jeho analýza spôsobu spáchania trestného činu môže niektoré osoby vylúčiť z okruhu potencionálnych páchateľov. Vylúčené tak môžu byť napríklad osoby pochádzajúce zvnútra poškodenej spoločnosti (zamestnanci) alebo zvonku; osoby, ktoré nemajú prístup k určitým súborom; osoby zvnútra poškodenej spoločnosti, ktoré nemajú prístup k programovému vybaveniu pracoviska.

c) Zistené skutočnosti nasvedčujú tomu, že sa stal skutok, ktorý vykazuje všetky znaky trestného činu a na ich základe je možné určiť pravdepodobného páchateľa. Nemožno však vysloviť záver o spôsobe spáchania trestného činu.

Vyšetrovateľ po tom, čo zaistí objekty za účelom vykonania počítačovej expertízy, stanoví v spolupráci so znalcami kriminalistickú verziu na objasnenie spôsobu spáchania trestného činu. Vyšetrovateľ následne obstaráva dôkazy, ktoré potvrdzujú alebo vyvracajú jednotlivé kriminalistické verzie. Účasť znalcov je za tejto situácie opäť nevyhnutná, a to vzhľadom k tomu, že objasnenie spôsobu spáchania trestného činu vyžaduje nevyhnutne odborné znalosti.

Veľmi dôležitým úkonom je v tejto fáze výsluch obvineného. Najmä ak obvinený spolupracuje, je jeho výsluch významným zdrojom informácií. Výsluch obvineného treba konfrontovať so znalcami, prípadne inými expertmi, najmä čo sa týka technických detailov. Je však potrebné mať na mysli, že v tejto situácii ide väčšinou už o rozvinutú etapu vyšetrovaní, kedy je potrebné obstarávať dôkazy preukazujúce naplnenie všetkých znakov skutkovej podstaty trestného činu.

d) Zistené skutočnosti nasvedčujú tomu, že sa stal skutok, ktorý vykazuje všetky znaky trestného činu a na ich základe je možné určiť pravdepodobného páchateľa a zároveň objasňujú spôsob spáchania trestného činu. [4]

Táto východisková vyšetrovacia situácia je najpriaznivejšia. Vyšetrovateľ má možnosť po vyhodnotení nazhromaždených materiálov oznámiť obvinenie určitej osobe a svoju ďalšiu činnosť zamerať na sprocesnenie doteraz získaných informácií, zabezpečenie objektov potrebných pre expertízu a ich následnému nariadeniu.

3. Charakteristické stopy počítačovej kriminality

Pri odhaľovaní a objasňovaní kriminality musia orgány činné v trestnom konaní, najmä policajný orgán, určitým spôsobom získať informácie a poznanie o jave, ktorý sa odohral v minulosti. Trestný čin je možné z kriminalistického hľadiska chápať ako proces určitého priestorovo určeného a časovo ohraničeného pohybu hmoty. Správanie páchateľa sa určitým spôsobom odráža v materiálnom svete. Za kriminalistickú stopu je teda možné považovať podľa odbornej literatúry *„každú zmenu v materiálnom prostredí alebo vo vedomí človeka, ktorá príčinne, lokálne alebo časovo súvisí s vyšetrovanou udalosťou, obsahuje kriminalistickú alebo trestnoprávne relevantnú informáciu a je zistiteľná a zaistiteľná; informácie z nej sú využiteľné pomocou prístupných kriminalistických, prírodovedných a technických metód, prostriedkov a postupov.“* [5]

Základné delenie kriminalistických stôp je na stopy pamäťové a stopy materiálne. Zásadný rozdiel je v prostredí, kde tieto stopy vznikajú. Pamäťová stopa vzniká vďaka ľudským zmyslom sprostredkovane v pamäti človeka, zatiaľ čo stopy materiálne sa vyskytujú v rôznych podobách v prírode, a to ako na objektoch živých, tak neživých. V prípade počítačovej kriminality je zabezpečovaná celá rada stôp materiálnych aj pamäťových, avšak typická je zvláštna kategória materiálnych stôp nazývaná stopy počítačové alebo stopy digitálne.

4. Špecifiká počiatočných úkonov a krokov k objasneniu počítačovej kriminality

V počiatočnej etape trestného konania je nutné ešte pred tým, než policajný orgán pristúpi k dokazovaniu, vykonať úkony, ktoré sú zásadné pre úspech celého vyšetrovania. Nevyhnutnosť týchto úkonov je determinovaná extrémnou dynamikou prostredia informačných technológií. Úplne zásadné je zabránenie výmazu dát, obnovenie vymazaných dát a informácií a v prípade úmyselného zavíreniu počítača zabránenie šírenia vírusu.

V prvotnej fáze vyšetrovania je tiež nutné vyžiadať od príslušných orgánov zbavenie mlčanlivosti osôb, ktoré by mohli mať trestnoprávne relevantné informácie. S predpokladom kvalifikovaného páchateľa je nutné postupovať rýchlo, ale na druhej strane veľmi obozretne. Vo väčšine prípadov je nutné postupovať v spolupráci s počítačovými expertmi. Už pri samotnom plánovaní procesu priebehu počiatočných vyšetrovacích úkonov je mnohokrát nevyhnutné konzultovať ich s expertmi. V súvislosti s počítačovou kriminalitou je veľmi dôležité poznamenať, že neodborná manipulácia so stopami môže mať za následok zničenie relevantných dôkazov a tým aj zmarenie celého vyšetrovania.

Zásadnými počiatočnými úkonmi pri vyšetrovaní počítačovej kriminality je predovšetkým:
a) obhliadka miesta činu

b) domová prehliadka
c) zaisťovacie úkony pre počítačovú expertízu a vyhľadávanie počítačových stôp a dôkazov

a) Obhliadka miesta činu

Pri ohliadke miesta činu je potrebné policajnému orgánu uvedomiť si, na akých miestach sa môžu technické počítačové stopy nachádzať. Miestom, na ktoré by mala byť upriamená pozornosť primárne, je samozrejme samotný počítač a jeho periférne zariadenia, teda najmä monitory, klávesnice, tlačiarne. Ďalej sú bežnými technickými stopami nosiče digitálnych informácií. Okrem tradičných nosičov digitálnych informácií, ako sú CD, DVD disky, flash disky sa môžu trestnoprávne relevantné informácie nachádzať aj na úplne nezvyklých miestach, ako čierna skrinka, palubný počítač či riadiaca jednotka motorového vozidla. Odborná literatúra uvádza, že ľahko prehliadnuteľnými zdrojmi informácií môžu byť aj ďalšie digitálne zariadenia, ktoré nie sú tak nápadné, napríklad modifikácia operačného systému hernej konzoly, ktorá bola využívaná ako počítač.

Okrem tradičných miest, ako poznámkové bloky, korešpondencia alebo odpadkový kôš sa môžu relevantné informácie nachádzať taktiež v mobilných telefónoch, faxoch, telefónnych odkazovačoch, diktafónoch a pod.

Ohliadku miesta činu je vhodné konzultovať s expertmi na výpočtovú techniku, prípadne ich priamo prizvať k tomuto úkonu. Ich odborné znalosti pomôžu vymedziť rozsah objektov skúmania, ich zabezpečenie a dokumentáciu. To vyplýva aj z dikcie ustanovenia § 154 ods. 1 Trestného poriadku, ktorý uvádza, že obhliadky sa môže zúčastniť osoba, ktorá vykonáva odbornú činnosť, alebo pribratý znalec.

b) Domová prehliadka

Tento zaisťovací inštitút je upravený v § 99 a nasl. Trestného poriadku. Slúži cielenému vyhľadávaniu (nielen) počítačových stop. Práve počas vykonávania domovej prehliadky dochádza najčastejšie k zaisťovaniu stôp.

Domová prehliadka predstavuje značný zásah do ústavne garantovaného práva na súkromie, plynúceho z článku 12 Charty. Jej realizácia je preto možná iba zo zákonom stanovených dôvodov a za prísnych podmienok. *„Domovú prehliadku možno vykonať, ak je dôvodné podozrenie, že v byte alebo v inom priestore slúžiacom na bývanie alebo v priestoroch k nim patriacim je vec dôležitá pre trestné konanie alebo že sa tam skrýva osoba podozrivá zo spáchania trestného činu, alebo je potrebné vykonať zaistenie hnuteľných vecí na uspokojenie nároku poškodeného na náhradu škody.“* [6] Ak sa počas domovej prehliadky nájdu veci dôležité pre trestné konanie, je policajný orgán oprávnený ich zabezpečiť. Avšak v prípade počítačovej techniky je situácia veľmi špecifická. Zaistením počítačovej techniky môže dôjsť k zaisteniu aj údajov ďalších, na ktoré sa môže vzťahovať povinnosť mlčanlivosti. V tomto zmysle má zabezpečovanie vecí pri vyšetrovaní počítačovej kriminality voľnejšie podmienky a policajný orgán je oprávnený zabezpečiť aj tieto informácie.

c) Zaisťovanie digitálnych stôp

Proces zaisťovania digitálnych stôp závisí od faktu, či zaisťujeme stopy technické alebo dátové. V prípade technických stôp je zaistený predovšetkým počítač a jeho periférne zariadenia, ďalej aj rôzne, skôr spomínané, nosiče digitálnych informácií. Na zaistenie dátových stôp je vo väčšine prípadov

potrebné zabezpečiť ich nosiče. Pre zaistenie technických stôp sa v prípade, že k nemu nedochádza pri domovej prehliadke, využíva ustanovenia § 89 a § 91 Trestného poriadku o vydaní, resp. odňatí veci. Pri počítačových trestných činoch je veľmi dôležité ustanovenie § 90 Trestného poriadku, ktoré pojednáva nielen o vydaní počítačového údaju, ale aj o jeho uchovaní. Povinnou osobou pri tomto ustanovení je osoba, ktorá má predmetný údaj v držbe alebo má nad ním kontrolu.[7]

V prípade zaistenia techniky pripadajú do úvahy dva možné spôsoby jej vykonania. Prvým možným postupom je techniku demontovať a previezť na skúmanie do laboratórií. Táto možnosť je ideálna, ale nie je vždy realizovateľná pre niektoré rozmerové alebo váhové disproporcie. Navyše fungovanie takéhoto zariadenia môže byť pre prevádzkovú kontinuitu poškodeného, ktorý je jej vlastníkom, celkom zásadné a následky jej demontovania a prevezenia by pre túto osobu mohli znamenať kolaps, či už informačného systému alebo výrobného procesu. Ak odborník vyhodnotí vyššie uvedený postup ako nevhodný, vykoná na mieste dokumentáciu techniky a na rad prichádza zaisťovanie samotných dát.

Zaisťovanie dát je jednou z najdôležitejších kriminalisticko-technických činností, na ktorej úspešnom zvládnutí závisí nielen výsledok kriminalistickej expertízy, ale aj akceptovateľnosť dôkazov na hlavnom pojednávaní. Ak sú zabezpečované dáta na originálnych nosičoch, je nevyhnutné dbať na to, aby nedošlo k poškodeniu originálov. Ak zaistenie originálu nie je možné, musí byť pri prenose dát na kópii zaistená ich identická postupnosť. Pokiaľ nie je možné zaistiť originálne dáta, je nutné vytvoriť ich presnú kópiu. Pre takúto kópiu sa používa označenie duplikát digitálnej stopy. [8]

5. Problémy pri zaisťovaní digitálnych stôp

Digitálne stopy majú nespornú výhodu v ich časovej trasovateľnosti, ktorá je oproti klasickým kriminalistickým stopám výnimočná. To znamená, že veľká väčšina digitálnych stôp je v prostredí informačných systémov spojená s veľmi presným stanovením času. K väčšine digitálnych stôp je možné priradiť časový údaj ich vzniku. Príkladom môžu byť vytvorené súbory či odoslané e-mailové správy, u ktorých je zrejmý čas vytvorenia.

Problém spojený s časovou trasovateľnosť je však iný. Prenastavenie času na počítači je aj pre priemerného používateľa ľahko dosiahnuteľné. Táto dynamika zmien, ktoré sa môžu vykonávať s digitálnymi stopami, sa prejavuje aj na samotnom obsahu dát. V situácii, kedy by poškodenou bola spoločnosť s viacerými zamestnancami a so zložitým informačným systémom, je potrebné vykonávať ohliadku miesta činu za prevádzky spoločnosti. Ak je v takomto prípade páchateľom osoba z vnútorného prostredia spoločnosti, môže mať dostatok času a priestoru pre manipuláciu alebo znehodnotenie dátových elementov. V prípade takejto situácie je užitočnejšie upriamiť pozornosť aj na tzv. nedigitálne stopy, ako môžu byť záznamy bezpečnostných kamier, záznamy z bankových účtov, výpovede jednotlivých svedkov a iné. Takéto stopy môžu pomôcť zistiť totožnosť páchateľa, prípadne v pokročilom štádiu trestného konania môžu byť použité ako priame aj nepriame dôkazy.[9]

III. Záver

Počítačová kriminalita, ako aj ostatné protispoločenské činnosti, komplikujú a obmedzujú rozvoj spoločnosti. Narúšajú spoločenský a ľudský potenciál, zhoršujú kvalitu života. Naburávajú dôveru medzi obyvateľstvom a štátom, čím narúšajú demokratické princípy fungovania štátu. Samotné odhaľovanie

počítačovej kriminality je pre jej rýchly vývoj extrémne náročné a vyšetrovacie postupy neraz narazia na mnoho úskalí, s ktorými sa musí popasovať. Je preto nevyhnutné pri vyšetrovaní a dokazovaní trestných činov súvisiacich s počítačom, aby bola poskytnutá orgánom činným v trestnom konaní aktívna kooperácia, a to či už zo strany poškodených alebo zúčastnených osôb, ale aj od záujmových združení, kontrolných, revíznych a inšpekčných orgánov, počítačových expertov a v neposlednom rade aj od orgánov Európskej únie.

Použité informačné zdroje:

ČENTÉŠ, J.: Trestný poriadok: veľký komentár. Žilina: Eurokódex, 2014
METEŇKO, J.: Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality. Bratislava: Akadémia Policajného zboru v Bratislave, 2004
ŠIŠULÁK, S., VAJZER, L.: Vybrané problémy objasňovania trestnej činnosti páchanej prostredníctvom informačno-komunikačných technológií. Bratislava: Akadémia policajného zboru v Bratislave, 2017
MICHAĽOV, L., ROMŽA, S., FERENČÍKOVÁ, S.: Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty : zborník príspevkov z Medzinárodného vedeckého sympózia konaného dňa 28. marca 2014 na Katedre trestného práva Právnickej fakulty Univerzity Pavla Jozefa Šafárika v Košiciach. Košice, 2014
PORADA, V. a kol.: Kriminalistika (teorie, metody, metodologie). Plzeň: Aleš Čenek, s.r.o., 2014
Zdroj: https://www.minv.sk/?statistika-kriminality-v-slovenskej-republike-xml (zo 18.11.2018)

Poznámky pod čiarou

[1] Zdroj: https://www.minv.sk/?statistika-kriminality-v-slovenskej-republike-xml (zo 18.11.2018)

[2] MICHAĽOV, L., ROMŽA, S., FERENČÍKOVÁ, S.: Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty : zborník príspevkov z Medzinárodného vedeckého sympózia konaného dňa 28. marca 2014 na Katedre trestného práva Právnickej fakulty Univerzity Pavla Jozefa Šafárika v Košiciach. Košice, 2014, s. 243

[3] ŠIŠULÁK, S., VAJZER, L.: Vybrané problémy objasňovania trestnej činnosti páchanej prostredníctvom informačno-komunikačných technológií. Bratislava: Akadémia policajného zboru v Bratislave, 2017, s. 139

[4] METEŇKO, J.: Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality. Bratislava: Akadémia Policajného zboru v Bratislave, 2004, str. 333

[5] PORADA, V. a kol.: Kriminalistika (teorie, metody, metodologie). Plzeň: Aleš Čenek, s.r.o., 2014, s. 263

[6] ČENTÉŠ, J.: Trestný poriadok: Veľký komentár. Žilina: Eurokódex, 2014. str. 944

[7] ČENTÉŠ, J.: Trestný poriadok: Veľký komentár. Žilina: Eurokódex, 2014. str. 944

[8] MICHAĽOV, L., ROMŽA, S., FERENČÍKOVÁ, S.: Počítačová kriminalita – juristické, kriminalistické a kriminologické aspekty : zborník príspevkov z Medzinárodného vedeckého sympózia konaného dňa 28. marca 2014 na Katedre trestného práva Právnickej fakulty Univerzity Pavla Jozefa Šafárika v Košiciach. Košice, 2014, str.243

[9] ŠIŠULÁK, S., VAJZER, L.: Vybrané problémy objasňovania trestnej činnosti páchanej prostredníctvom informačno-komunikačných technológií. Bratislava: Akadémia policajného zboru v Bratislave, 2017, str. 139