Miroslav Lisoň, Gabriel Moskvič

Identifikácia série trestných činov počítačovej kriminality

Anotácia: Otázky súvisiace s identifikáciou série v páchaní trestných činov počítačovej kriminality nie sú v podmienkach Slovenskej republiky aktuálne zodpovedané (výstupy z rešerše odbornej literatúry). V tomto kontexte sa autori rozhodli systémovo skúmať, hodnotiť a predložiť odbornej verejnosti náčrt možného postupu policajno-bezpečnostných orgánov (ďalej len „*PBO*“) pri realizácii tejto formy poznávania. Pri napĺňaní tejto ambície využívajú poznanie, ktoré je čiastočne spracované pri plnení výskumných úloh súvisiacich so spracovaním dizertačnej práce, v ktorej sú riešené otázky súvisiace s vyšetrovaním trestných činov počítačovej kriminality.

Kľúčové slová: počítačová kriminalita, kyberkriminalita, znaky počítačovej kriminality, skutkové podstaty trestných činov počítačovej kriminality, séria trestných činov, identifikácia, objektová identifikácia, identifikácia systémov, postup pri realizácii identifikácie.

Úvod

Výstupy z identifikácie série trestných činov počítačovej kriminality sú významné pre prijímanie a realizáciu opatrení na úseku ich vyšetrovania, predchádzania a zamedzovania (*nielen trestných činov počítačovej kriminality*). Osobitne sa to odráža, ak túto činnosť PBO realizujú v štruktúre kriminálno-policajného poznania.[1]

Spravodajská činnosť, operatívno-pátracia činnosť a policajné vyšetrovanie sú súčasťou štruktúry policajného konania. V policajnej praxi pri poznávaní určitých trestných činov tieto špeciálne činnosti tvoria realizačný systém. Pre potreby policajnej praxe a teórie je vhodné, ak sa tento systém skúma, vysvetľuje a projektuje ako jednotný model, ktorý je vhodné označiť termínom kriminálno-policajné poznanie (ďalej len *„KPP“*). Spravodajská činnosť, operatívno-pátracia činnosť a vyšetrovanie vykazujú charakter techník (*súbor činností, pracovných spôsobov a špecifických prostriedkov určených na stále dokonalejšie využívanie prírodných síl a zdrojov*), ktoré sú v súlade s identifikovanou potrebou (*účelovo*) realizované pri dosahovaní stanovených cieľov. Tieto činnosti pri plnení stanovených úloh predstavujú variantné spôsoby postupov v štruktúre tohto modelového systému.[2] Charakteristickou črtou *KPP* je, že zisťovanie, skúmanie, hodnotenie a vysvetľovane určených javov (*získavanie objektívnych relevantných faktov*) PBO realizujú špecifickými formami (*funkčný prejav procesov – používanie prostriedkov v metódach*), rešpektujúc realizačné prostredie (*udalosť + situácia*). Pri ich realizácii predstavuje kriminalita kategóriu (*jav, objekt poznávania*), ktorej ontologické a gnozeologické vlastnosti určujú kvalifikované znaky skutkových podstát páchaných a spáchaných trestných činov (podľa *platného a účinného Trestného zákona*).

PBO pri plnení zákonom delegovaných úloh, ktoré predovšetkým súvisia s poznávaním kriminálnych aktivít (*ich fragmentov, prvkov*), cieľavedome a systematicky využívajú formy identifikácie. V danom prípade nemusí ísť o *kriminalistickú identifikáciu*, ale o postup, pri ktorom sú dominantne aplikované metódy a používané prostriedky *KPP* (*napríklad spravodajskej činnosti (ďalej len „SČ“), operatívno-pátracej činnosti (ďalej len „OPČ“) - mimo trestného konania, integrované v trestnom konaní a pod.).* Prax potvrdzuje, že využitím metód a prostriedkov *KPP* (*SČ, OPČ a vyšetrovaním*) je možné nielen spracovať identifikačné charakteristiky objektov, ktoré sa využívajú nielen pri rozhodovaní o napĺňaní

[1] Predkladané poznanie vo forme vedeckej štúdie je spracované v procese aplikovaného výskumu, ktorý je realizovaný pre potreby dizertačnej práce *„Špecifiká vyšetrovania trestných činov počítačovej kriminality v podmienkach Slovenskej republiky.“* Projekt výskumu pre potreby dizertačnej práce bol úspešne obhájený v roku 2025.

[2] LISOŇ, M., A. VAŠKO a kol. *Teória kriminálno-policajného poznania*, s. 49 a násl.

účelu trestného konania, ale aj pri samotnom vyhotovovaní dôkazov. K uvedenému je vhodné dodať, že práve tieto skutočnosti sú typické pre trestné činy páchané v sérii. Obsahom týchto postupov je poznávať a charakterizovať vzťahy, ktoré existovali, resp. existujú, medzi rôznymi druhmi prejavu trestných činov, s cieľom individualizovať ich a využiť pri objektívnom charakterizovaní série.

V súčasnej dobe PBO, najmä v procesoch účelového poznávania trestných činov a vzťahov medzi nimi, realizujú dve formy identifikácie. Ak majú minimálne dva objekty reálne k dispozícii, realizujú *identifikáciu objektov (objektová identifikácia).* V prípadoch, ak je identifikačné skúmanie realizované len izolovanou analýzou jedného z nich, pretože druhý nie je pre jeho potreby k dispozícii, realizujú tzv. *identifikáciu systému.*

1 Počítačová (*kybernetická*) kriminalita

Spolu s nárastom využívania počítačových zariadení zaznamenávame aj vývoj trestnej činnosti, ktorá s týmito zariadeniami priamo súvisí. V počiatočných štádiách mal tento druh kriminality skôr lokálny charakter, avšak s rozšírením prístupu na internet, prehlbovaním globalizácie a prepojením jednotlivých častí sveta začal naberať výrazne širšie a globálnejšie rozmery. Postupne sa jednotlivé formy protiprávneho konania začali vzájomne kombinovať, čím sa vytvárali nové a sofistikovanejšie metódy dosahovania protiprávneho stavu.

V počiatkoch počítačovej kriminality išlo predovšetkým o formy sabotáže či priemyselnej špionáže, ktoré vyžadovali fyzický prístup k zariadeniam. S príchodom možností sieťového prepojenia počítačových systémov však došlo k zásadnej zmene – *kybernetická kriminalita* sa začala rýchlo prispôsobovať technologickému vývoju a operatívne reagovať na nové podmienky. Tento vývoj, trvajúci už niekoľko desaťročí, postupne prenikol do všetkých oblastí spoločenského života.

V súčasnosti, keď dochádza k masívnej digitalizácii, integrácii operačných systémov do dopravných prostriedkov, automatizovaných vozidiel, ale aj k budovaniu konceptu inteligentných miest (*tzv. smart cities*) a prepojeniu mestskej infraštruktúry, vzniká nový priestor pre páchanie kybernetickej trestnej činnosti. Ide o závažnú bezpečnostnú výzvu, ktorá si vyžaduje systematické a multidisciplinárne riešenia.

Postupný vývoj od *offline zariadení* cez *ethernetové LAN* siete až po plnohodnotné internetové pripojenie zároveň prispel k precizovaniu a štandardizácii odbornej terminológie používanej pri tejto forme kriminality. Kriminalitu možno vo všeobecnosti definovať ako súhrn pripravovaných, páchaných a spáchaných trestných činov, ktoré majú negatívny dopad na spoločnosť.[3]

Vo všeobecnosti možno kriminalitu chápať ako súbor konaní, ktoré sú v rozpore s ustanoveniami Trestného zákona, prípadne ako činnosť napĺňajúcu znaky skutkovej podstaty niektorého z trestných činov v ňom upravených. Otázkou však ostáva, ako definovať kriminalitu páchanú prostredníctvom informačno-komunikačných technológií (ďalej len *„IKT“*) a do akej miery sa jej špecifiká odlišujú od tradičných foriem trestnej činnosti.

Pri terminologickom vymedzení protiprávneho konania realizovaného pomocou *IKT* sa stretávame s rozličnými označeniami, ktoré sú používané v teoretickej, akademickej, právnej, ale aj policajno-bezpečnostnej praxi. Pomerne často sa vyskytujú názory, že jednotlivé termíny, ako „*počítačová kriminalita*“, „*internetová kriminalita*“ či „*kybernetická kriminalita*“, sú vzájomne zameniteľné a môžu byť chápané ako synonymá. Podľa nášho názoru je však precízne terminologické rozlíšenie tejto trestnej činnosti mimoriadne dôležité a malo by byť predmetom samostatného odborného záujmu. Najčastejšie používanými označeniami pre kriminalitu súvisiacu s *IKT* sú výrazy ako počítačová, internetová a kybernetická kriminalita. Na prvý pohľad môže vzniknúť dojem, že ide o totožné označenia,

[3] LISOŇ, M. *Operatívno-pátracia činnosť (Všeobecná časť)*, s.15.

no pri podrobnejšej analýze možno zistiť, že každý z uvedených pojmov má svoje špecifiká. V nasledujúcej časti sa preto zameriame na ich bližšie objasnenie a vymedzenie.

Počítačová kriminalita predstavuje kategóriu trestnej činnosti, pri ktorej je *počítač, prípadne iné počítačové alebo komunikačné zariadenie*, použité ako nástroj, cieľ alebo prostriedok páchania protiprávneho konania.[4] Ide o trestné činy, v rámci ktorých je *počítač* buď primárnym objektom útoku (*napr. poškodzovanie softvéru*), nástrojom na vykonanie skutku (*napr. podvod cez e-mail*) alebo vystupuje ako vedľajší prvok v širšom reťazci trestnej činnosti.

Pod *týmto* pojmom by sme mali rozumieť najmä správanie, ktoré je zamerané na výpočtovú techniku a ktoré je neoprávnené a protiprávne. Na prvý pohľad sa počítačová kriminalita nemusí zásadne odlišovať od tradičných foriem páchania trestných činov, hlavným prvkom je tu však využitie počítača alebo jemu podobného zariadenia v niektorom štádiu trestného konania. Počítačová kriminalita teda nepredstavuje nové druhy trestných činov, ale skôr nové metódy a technológie na páchanie existujúcich skutkov. Cieľom páchateľov býva najčastejšie narušenie, poškodenie alebo zneužitie informačnej infraštruktúry jednotlivcov, organizácií či štátnych orgánov, a to práve prostredníctvom zneužitia zraniteľností technických systémov. Z terminologického hľadiska je pod pojmom „*počítač*“ v tomto kontexte potrebné chápať elektronické, magnetické, optické alebo iné zariadenie určené na spracovanie alebo prenos údajov, ktoré je schopné vykonávať logické, aritmetické alebo pamäťové operácie.[5]

Na rozdiel od počítačovej kriminality, ktorá je úzko spojená s fyzickým, hmotným zariadením a jeho využitím pri páchaní trestnej činnosti, sa pojem internetová kriminalita zameriava predovšetkým na trestnú činnosť realizovanú prostredníctvom internetového pripojenia. V tomto prípade je internet chápaný ako primárne médium, prostredníctvom ktorého dochádza k uskutočneniu protiprávneho konania. Ide napríklad o prípady *šírenia detskej pornografie, internetových podvodov, phishingu, cyberstalkingu, online vydierania (tzv. cyberextortion), porušovania autorských práv prostredníctvom „warezu“ atď.*

Internetovú kriminalitu môžeme chápať ako trestnú činnosť, ktorá využíva internet ako hlavný kanál na distribúciu nezákonného obsahu, získavanie neoprávneného prístupu alebo ako prostriedok sociálneho inžinierstva. V mnohých prípadoch ide o rozšírené formy už existujúcich trestných činov, ktorých páchanie je vďaka internetu efektívnejšie, anonymnejšie a často znemožňuje aj identifikáciu a autentifikáciu páchateľov. Dôležitým znakom je to, že internet ako hlavná zložka podporuje páchanie tejto trestnej činnosti bez fyzickej prítomnosti páchateľa, čo značne komplikuje jeho odhalenie.

Najširším a v súčasnosti najaktuálnejším pojmom zo spomenutých označení je kybernetická kriminalita. Z terminologického hľadiska ide o koncept, ktorý zahŕňa nielen počítačovú a internetovú kriminalitu, ale aj ďalšie formy protiprávneho konania súvisiace s využívaním moderných technológií, automatizovaných systémov, umelej inteligencie či internetu vecí (IoT)[6]. *Kybernetická kriminalita* sa týka každej protiprávnej činnosti, ktorá je páchaná v kybernetickom priestore. *Kybernetický priestor* predstavuje komplexné prostredie, v ktorom sa uskutočňujú aktivity spojené s internetom, počítačmi a sieťami. V medzinárodnej technickej norme *ISO/IEC 27032:2012* je kybernetický priestor definovaný ako: *„komplexné prostredie, ktoré je výsledkom interakcie ľudí, softvéru a služieb na internete, podporovaný celosvetovo distribuovanými fyzickými informačnými a komunikačnými technológiami,*

[4] POLČÁK, R a kol. *Právo informačních technologií*, s. 541.
[5] FUNTA, R. *Komentár k Dohovoru Rady Európy o počítačovej kriminalite,* s. 22.
[6] Pod pojmom „*internet vecí*“ sa rozumejú každodenné veci, objekty a zariadenia, ktoré sú pripojené k internetu (*napr. inteligentné hodinky, okuliare, chladničky*). Základom je pripojenie k internetu prostredníctvom senzorov na zaznamenávanie, spracovanie, ukladanie a prenos dát.

zariadeniami a prepojenými sieťami"[7] V Slovenskej právnej úprave je kybernetický priestor upravený v § 3 písm. c) *zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti* (ďalej len „*ZoKB*"), kde sa uvádza, že ide o *„globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi"*[8].

Na základe všetkých uvedených definícií možno konštatovať, že kybernetický priestor predstavuje nehmotné, virtuálne prostredie bez fyzického umiestnenia a hraníc, ktoré je však priamo naviazané na fyzickú infraštruktúru (napr. servery, diskové úložiská, sieťové prvky a pod.). Charakteristické znaky kybernetického priestoru zahŕňajú jeho decentralizáciu, globálnosť, otvorenosť, informačné bohatstvo, interaktivitu a schopnosť ovplyvňovať verejnú mienku prostredníctvom používateľov. Hlavnými stavebnými prvkami tohto priestoru sú technológie a nimi sprostredkované služby, ktoré formujú digitálnu spoločnosť.

Z uvedeného vyplýva, že počítačová kriminalita predstavuje najužší pojem, viazaný predovšetkým na použitie výpočtovej techniky ako nástroja alebo cieľa trestnej činnosti. Internetová kriminalita predstavuje špecifickú *subkategóriu* sústredenú na zneužívanie internetového priestoru. Naproti tomu kybernetická kriminalita predstavuje zastrešujúci pojem, ktorý reflektuje najnovšie technologické trendy a zahŕňa aj nové hrozby a formy útokov v kybernetickom priestore.

Počítačová alebo kybernetická kriminalita sa vyznačuje viacerými znakmi, ktorými sa odlišuje od iných druhov kriminality. Ako sme už uviedli v predchádzajúcej časti, základom počítačovej kriminality je spáchaná trestná činnosť prostredníctvom počítačových zariadení, resp. IKT v kybernetickom priestore. Ďalším z meritórnych znakov tejto trestnej činnosti je *potreba špecifických vedomostí*, zručností a technických znalostí. Nie je, samozrejme, nevyhnutné, aby v každom z prípadov (*napr. pri podvodoch či šírení detskej pornografie*) mal páchateľ vysoký stupeň odborných znalostí z oblasti IKT. V mnohých prípadoch však technologická gramotnosť predstavuje zásadný predpoklad pre úspešné dokonanie skutku, najmä ak ide o sofistikované formy kybernetických útokov.

V spojitosti s odbornými znalosťami je zásadný aj *prístup páchateľov* k samotnej protiprávnej činnosti. Pokiaľ páchatelia nevyužívajú techniky ako *hacking* alebo nasadzovanie škodlivého softvéru (*napr. malware, trójske kone, ransomware atď.*), často využívajú formy tzv. sociálneho inžinierstva, teda súbor manipulatívnych psychologických techník zameraných na získanie dôverných informácií od obete prostredníctvom ľsti, klamstiev alebo presviedčania.

V odbornej literatúre sa môžeme stretnúť aj s ďalším delením počítačovej kriminality, ktoré ju kategorizujú podľa miery závislosti od IKT na tri základné skupiny: *cyber-dependent*, *cyber-enabled* a *computer-supported* kriminalitu.

Cyber-dependent kriminalita predstavuje trestnú činnosť, ktorá je páchaná výlučne prostredníctvom počítačových zariadení alebo počítačových sietí. Ide o užšiu kategóriu kybernetickej kriminality, pri ktorej sú cieľom útoku samotné technológie. Typickými príkladmi je napr. *hacking, šírenie malvéru, útoky typu či DoS alebo DDoS.*

Cyber-enabled kriminalita zahŕňa tradičné trestné činy, ktorých rozsah a dopad je vďaka využitiu IKT výrazne rozšírený. V tomto prípade ide napr. o šírenie detskej pornografie prostredníctvom internetu alebo porušovanie autorských práv cez tzv. *warezové stránky* alebo *torrenty*. Tieto činy by mohli byť spáchané aj bez použitia IKT, no technológie výrazne zvyšujú ich efektivitu a dosah.

Computer-supported kriminalita označuje situácie, kedy sú počítačové zariadenia alebo iné súvisiace technológie využívané pri páchaní trestných činov len príležitostne.

---

[7] ISO/IEC 27032:2012 – Introduction [online]. 2025. [cit.3. marca 2025]. Dostupné na internete: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:en>.

[8] *§3 písm. c) zákon č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.*

Ide o trestné činy, ktorých skutkovú podstatu možno naplniť aj klasickým spôsobom, no IKT tomu značne napomáhajú a uľahčujú ich páchanie. Sem patria rôzne druhy podvodov, legalizácia výnosov z trestnej činnosti či obchodovanie s drogami. Hoci táto kategória nemusí spadať priamo pod kybernetickú kriminalitu, v priebehu vyšetrovania možno využívať digitálne dôkazy, ako sú e-maily, lokalizačné údaje alebo IP adresy, ktoré napomáhajú identifikácii páchateľa.[9]

Niet pochýb o tom, že rozširovanie využívania počítačových zariadení a IKT zásadným spôsobom zasahuje do všetkých oblastí života používateľov. Exponenciálny nárast digitalizácie priniesol nielen výhody, ale zároveň aj nové formy trestnej činnosti, ktoré by bez existencie týchto technológií nebolo možné páchať. Klasifikácia druhov počítačovej kriminality prešla dlhodobým vývojom, čo sa prejavuje aj na spôsobe kategorizácie jej jednotlivých foriem a metód.

V tomto kontexte možno hovoriť o rozsiahlom využívaní *sociálneho inžinierstva*, ktoré predstavuje sofistikovaný nástroj podvodov a manipulácie používateľov s cieľom získať prístup k citlivým údajom. Najčastejšie formy tejto techniky zahŕňajú *zneužitie SMS správ, e-mailovej komunikácie, phishingových odkazov, pharmingových stránok atď.*

Odborné technické znalosti páchateľov vedú k vytváraniu a distribúcii rôznych druhov škodlivého softvéru (*malvéru*), ako sú *trójske kone, botnety, ransomware* a ďalšie. Tieto nástroje umožňujú útočníkom preniknúť do systémov obetí, získať kontrolu nad zariadeniami alebo spôsobiť ich úplnú nefunkčnosť. Osobitnou kategóriou sú útoky na informačné a operačné systémy, ktoré majú za cieľ ich vyradenie z prevádzky. Ide o tzv. DoS *(Denial of Service)* alebo DDoS *(Distributed Denial of Service)* útoky, ktoré zahlcujú cieľové systémy množstvom požiadaviek a tým znemožňujú ich funkčnosť.

Počítačové technológie zároveň uľahčujú páchanie širokého spektra trestnej činnosti, čím zásadne menia charakter a formy jej realizácie. Medzi najčastejšie trestné činy, ktoré sú podporované využívaním IKT, patrí najmä *porušovanie autorských práv,* ku ktorému dochádza prostredníctvom tzv. *warezových stránok, peer-to-peer (P2P) sietí* alebo *trackerových serverov*, ktoré umožňujú masové poskytovanie (zdieľanie) a sťahovanie nelegálneho obsahu.

Závažným problémom je aj výroba, uchovávanie a šírenie detskej pornografie, ktoré je uľahčené anonymitou digitálneho prostredia a možnosťou šifrovanej komunikácie. Rovnako tak je častým javom aj podpora toxikománie a nelegálny predaj omamných a psychotropných látok prostredníctvom *dark webových* anonymných platforiem (*napr. Pandora, Silk Road 2.0, Evolutin, AlphaBoy* atď.). V neposlednom rade vážnu hrozbu predstavuje aj *legalizácia príjmov z trestnej činnosti* prostredníctvom kryptomien a anonymných digitálnych peňaženiek, ktoré sťažujú sledovanie finančných tokov.

S počítačovou kriminalitou sa často spája pojem „*hacker*“, ktorý slúži ako spoločný menovateľ pre rôzne subjekty pôsobiace v kybernetickom prostredí. V súčasnosti má tento termín prevažne negatívnu konotáciu a je spájaný s nezákonnými aktivitami. Je však dôležité poznamenať, že nie každý hacker je nevyhnutne osobou usilujúcou o spôsobenie škody. Existujú aj skupiny jednotlivcov, ktoré sa zameriavajú na identifikáciu zraniteľností s cieľom zvyšovať úroveň bezpečnosti a predchádzať potenciálnym rizikám. Títo jednotlivci využívajú svoje odborné znalosti na bezpečnostné, obranné a etické účely.

V súčasnosti sa v kybernetickej terminológii štandardne používajú tri základné označenia pre hackerov: *Black Hats (zlomyseľní hackeri), White Hats (etickí hackeri)* a *Gray Hats (neetickí hackeri)*[10]. Toto delenie odráža motiváciu, zameranie a ciele jednotlivých skupín. S postupujúcim vývojom technológií sa objavili aj ďalšie subkategórie hackerov,

[9] POLČÁK, R a kol. *Právo informačních technologií,* s. 542.
[10] KOLOUCH, J. *CyberCrime*, s. 273.

ktoré pôsobia v kybernetickom priestore a predstavujú rozšírené spektrum aktérov s rôznorodými záujmami a úrovňou etiky.

Black hat (zlomyseľný hacker) – keď sa spomenie výraz hacker, zvyčajne si predstavíme jedinca, ktorý chce škodiť, ničiť a ubližovať. Predstavíme si skupinu osôb, ktorá útočí, znefunkčňuje webové stránky a spôsobuje chaos. Tento obraz je spojený s hackermi známymi ako *black hats* alebo aj „*malicious hackers*“ (*zlomyseľní hackeri*). Ide o najpočetnejšiu skupinu týchto subjektov, ktoré stoja za väčšinou kybernetických útokov. Ich činnosť kvalifikujeme ako nezákonnú, primárne motivovanú snahou o vlastný prospech na úkor práv a záujmov poškodených. Môžu spôsobiť vážne finančné škody jednotlivcom aj organizáciám krádežou citlivých alebo osobných údajov, únikom dát, kompromitáciou počítačových systémov alebo zmenou kritických sietí.[11]

Táto skupina hackerov využíva rôzne formy počítačovej trestnej činnosti, ako sú *phishing, DoS a DDoS útoky, podvodné e-maily a sociálne inžinierstvo*. Mnohí získavajú svoje „*príležitosti*“ prostredníctvom fór a iných spojení prostredníctvom *dark webu*.[12] Istá časť si sama vyrába a sprostredkováva (*samozrejme za poplatok*) rôznu škálu škodlivých softvérov (napr. rôzne druhy *malvérov, vírusov a ransomvérov atď.)*. Iní preferujú pracovať prostredníctvom *franšíz* alebo na základe *lízingových zmlúv*, podobne ako v legálnom podnikateľskom svete. V dnešnom internetovom prostredí nie je distribúcia *škodlivého softvéru* zložitá, čo prináša množstvo príležitostí nielen na finančné zisky. Mnohé hackerské útoky sú rýchle a automatizované a nezahŕňajú priamy kontakt s človekom. V týchto prípadoch sa útočné roboty pohybujú po internete a vyhľadávajú nechránené počítače, do ktorých by mohli preniknúť. *Hackerské útoky* predstavujú globálny problém, čo negatívne ovplyvňuje ich obmedzenie a zastavenie. Je výzvou pre zákonodarcov, aby vytvorili legislatívne predpoklady na rýchle zadržanie takýchto páchateľov. Rovnako to je výzvou pre orgány činné v trestnom konaní, pretože takéto osoby zanechávajú veľmi málo stôp a často ich konanie prechádza cez viaceré jurisdikcie čím naberá medzinárodný charakter. Európska únia sa snaží tieto problémy čoraz aktívnejšie riešiť, páchatelia v kybernetickom prostredí sú však vždy o niekoľko krokov vpred. Aj keď sa podarí identifikovať hackerskú skupinu, často ide o operáciu s viacerými uzlami v rôznych krajinách, čo skupine umožňuje fungovať nepretržite. [13]

White hat (etický hacker) – ide o skupinu hackerov pracujúcich s cieľom pomáhať, odstraňovať hrozby, chrániť systémy, dáta a samotných používateľov. Využívajú svoje schopnosti a znalosti na vyhľadávanie zraniteľných miest v počítačových systémoch a sieťach. Výrazným rozdielom pri tomto druhu hackera je to, že má oprávnenie vniknúť do systému, pretože jeho cieľom je odhaliť bezpečnostné riziká skôr, ako to urobí niekto iný (*napr. hacker zo skupiny black hat*). Často sú najímaní vládou alebo rôznymi spoločnosťami, aby identifikovali slabé miesta v bezpečnostných systémoch organizácií a pomohli zabrániť vonkajším útokom alebo narušeniu údajov.[14] Vytvárajú aj simulované nástrahy a útoky na ich počítačové systémy, kde títo hackeri demonštrujú, ako by skutočný kybernetický útok mohol vyzerať a aké škody by hypoteticky mohol spôsobiť s daným zabezpečením. Tieto informácie sa následne využívajú na aktualizácie softvéru, zlepšenie bezpečnosti a odstránenie

---

[11] 14 Types of Hackers to Watch Out For [online]. 2025. [cit. 13. marca 2025]. Dostupné na internete: <https://www.pandasecurity.com/en/mediacenter/14-types-of-hackers-to-watch-out-for/>.

[12] Časť internetu, ktorá je prístupná len cez špeciálne softvéry, napr. Tor a často sa využíva na anonymnú komunikáciu a nelegálne aktivity.

[13] What is a Black-Hat hacker? [online]. 2025. [cit. 7. marca 2025]. Dostupné na internete: <https://www.kaspersky.com/resource-center/threats/black-hat-hacker>.

[14] 14 Types of Hackers to Watch Out For [online]. 2025. [cit. 10. marca 2025]. Dostupné na internete: <https://www.pandasecurity.com/en/mediacenter/14-types-of-hackers-to-watch-out-for/>.

zraniteľnosti.[15] Táto skupina *hackerov* nielen odhaľuje slabé miesta, ale bojuje aj proti *black hat hackerom*. Ich spôsob práce so spracovaním údajov, uniknutými dátami a odhaľovanie slabých miest sú vždy v medziach hackerskej etiky. Jednoducho povedané, ich cieľom je pomáhať, nie škodiť.

G*ray hat* (neetický hacker) – predstavuje tú časť hackerskej skupiny, ktorá objavuje spôsoby, ako preniknúť do počítačových sietí a systémov, ale na rozdiel od *black hats* bez zlého úmyslu. Ich pozícia je v nejednoznačnej etickej oblasti medzi skupinami *hackerov white hat* a *black hat*, z čoho vyplýva aj ich farebné označenie. Prekračujú hranice medzi *etickým* a *neetickým hackingom* tým, že porušujú zákony alebo používajú neetické techniky. Napriek tomu ich cieľom je dosiahnuť etický výsledok.[16] Snažia sa využiť svoje vedomosti a zručnosti na vyhľadávanie bezpečnostne zraniteľných miest v sieťach a systémoch bez povolenia alebo na základe vopred uzavretého zmluvného či pracovnoprávneho vzťahu ako v prípade *white hat*.

2 Možný postup PBO pri identifikovaní série trestných činov počítačovej kriminality

Na základe analýzy káuz (*vyšetrovacie spisy, ktoré boli úspešne ukončené súdnym rozhodnutím*) k uvedenému dodávame, že pre potreby identifikácie série trestných činov počítačovej kriminality PBO skúmajú minimálne procesuálny funkčný prejav u dvoch trestných činov, ktorých kvantita a kvalita je priamo determinovaná realizovanými aktivitami pri:

1. Formulovaní identifikačného problému – formulácii identifikačnej otázky.
2. Akceptácii delegovaných kompetencií vo vzťahu k realizácii identifikácie – prevzatí zodpovednosti za realizáciu identifikácie.
3. Analýze objektov identifikácie – ustanovení, konštruktívnom skúmaní, hodnotení a vysvetľovaní.
4. Používaní prostriedkov v metódach identifikácie (*operácií a techník*) identifikácie.
5. Spracovaní informačných výstupov a ich využívaní – akceptovaní výstupov z foriem identifikácie.[17]

Podstatou procesov tzv. objektovej identifikácie je práca s informáciami. Túto prácu realizujú kompetentní príslušníci PBO, ktorí si uvedomujú, že komplikovanosť gnozeologického prístupu v týchto procesoch spôsobujú najmä:

- ✓ Špecifická zložitosť a značná variabilnosť poznávaného javu (*subjektom trestného činu je človek, poznávanie rozličných vlastností ľudí, najmä psychických, teda javových, ktoré sa vymykajú bezprostrednému pozorovaniu a meraniu*).
- ✓ Retrospektívne vyhľadávanie (*odhaľovanie*), skúmanie a hodnotenie informácií o trestnom čine (*objekty identifikácie nie sú dostupné priamemu a systematickému pozorovaniu akcie a reakcie, výnimkou môže byť aplikácia kompetencií, ktoré vyplývajú z právnej, organizačno-riadiacej a taktickej „SČ“ a „OPČ“*).
- ✓ To, že skúmanie a hodnotenie systému trestného činu je vykonávané na základe subjektívne sprostredkovaných hodnôt jeho prvkov a interakcií, najmä vzťahov človeka ako subjektu (*aj potenciálneho*) trestného činu k inému človeku (*poškodený, obeť*), resp. k spoločenstvu, spoločnosti.
- ✓ Konkrétne prostredie, v ktorom sa zisťujú, skúmajú a hodnotia informácie o trestnom čine (*sociálne prostredie*).

---

[15] What is ethical hacking? [online]. 2025. [cit. 10. marca 2025]. Dostupné na internete: <https://www.ibm.com/topics/ethical-hacking>.

[16] White hat, black hat, grey hat hackers: What's the difference? [online]. 2025. [cit. 10. marca 2025]. Dostupné na internete: <https://www.malwarebytes.com/blog/news/2021/06/white-hat-black-hat-grey-hat-hackers-whats-the-difference>.

[17] JANÍČEK, P. a R. RAK. Systémové pojetí identifikace. In: PORADA, V. a kol. *Kriminalistika*, s. 105 –106.

- ✓ Latencia príčin, podmienok vzniku, existencie a zániku objektov identifikácie (*genéza ich existencie*).
- ✓ Aktivity subjektov trestného činu (*sú súčasťou spoločnosti*, najmä realizácie identifikácie) a pod.

Aj napriek tomu presadzujú gnozeologický optimizmus, že páchané a spáchané trestné činy sú plne poznateľné. Platnosť uvedenej konštatácie je evidentná najmä za predpokladu, že pri účelovej realizácii identifikácie využívajú adekvátne, praxou a teoretickou explanáciou overené zdôvodnené postupy a prostriedky.

1. Formulovanie identifikačného problém (identifikačná otázka)

Realizácia foriem identifikácie musí byť zdôvodnená, a to nielen definovaním identifikačnej úlohy, ale aj z hľadiska právnych a personálnych kompetencií, ktoré umožňujú realizovať túto činnosť v rámci existujúcej a vytváranej informačnej bázy ((*v súlade s presne formulovaným (definovaným) identifikačným problémom*)). Ten musí korešpondovať so sledovanými cieľmi v súvislosti so zabezpečovaním neodvratnosti trestného postihu za spáchaný trestný čin.

Praktické skúsenosti z aplikácie identifikácie série trestných činov počítačovej kriminality potvrdzujú, že je vhodné, ak PBO výstižne definujú problémy, ktoré súvisia s určovaním identity poznávaných objektov (*trestné činy*) a prípadné situácie, ktoré môžu spôsobiť určité konflikty pri jej realizovaní. Určia svoju identifikačnú pozíciu, ako aj význam pre stanovenie hlavnej a čiastkových (*priebežných*) identifikačných úloh. PBO pri formulovaní identifikačného problému zhodnotia, aký môže mať kriminálno-policajná situácia vplyv na organizačné a materiálne aspekty aplikácie foriem identifikácie. Cieľom tohto hodnotenia je eliminovať nepriaznivé vplyvy, ktoré môžu pôsobiť nielen v samotnom ich priebehu, ale hlavne na identifikačné výstupy, a to až do takej miery, že by sa nemohli v ďalšom poznávaní a dokazovaní použiť.

Niet sporu v tom, že formulovanie otázky pre potreby identifikácie je účelová a cieľavedomá činnosť, ktorá sa obligatórne spája s trestným právom. Je tomu tak preto, lebo trestné právo zabezpečuje ochranu štátom chránených záujmov a chráni rozvoj štátu pred javmi a útokmi proti spoločenskému vývoju, proti základným hodnotám demokratickej spoločnosti. Represívne pôsobí na konkrétneho páchateľa a preventívne pôsobí na možného páchateľa trestného činu. Na dosiahnutie svojho účelu používa hrozbu trestom, ukladanie trestu, výkon trestu a ochranné opatrenia.

PBO sú pri formulovaní otázky pre potreby identifikácie série povinné v prvom rade: poznávať formy trestnej činnosti (*odrážané v štádiách trestného činu a trestnej súčinnosti*). V tomto kontexte musia akceptovať, že *trestné nie je iba dokonané konanie, ale aj jednotlivé jeho štádiá – príprava a pokus. Príprava* je úmyselné vytváranie podmienok na spáchanie určitého trestného činu (*organizovanie činu – zadovažovanie prostriedkov a nástrojov na jeho spáchanie, spolčenie, štruktúrovanie, návod alebo pomoc*). *Pokus* bezprostredne smeruje k dokonaniu trestného činu – *páchateľ mal v úmysle spáchať trestný čin, no nedokonal ho*.[18]

O trestnej súčinnosti hovoríme, ak trestný čin spoločným konaním spáchali viacerí páchatelia (*spolupáchatelia*). Títo sú zodpovední tak, ako keby trestný čin spáchali samostatne (*každá osoba sama*). Osobitnou formou súčinnosti je účastníctvo na trestnom čine (*organizátor, navádzač, pomocník, účastník trestného činu sa nepodieľa na naplnení všetkých*

[18] Príprava a pokus sú trestné podľa trestnej sadzby pre trestný čin, ku ktorému smerovali (*ak zákon v prípade prípravy neustanovuje inak*). Ich trestnosť zaniká dobrovoľným upustením od ďalšieho konania a odstránením nebezpečenstva, včasným oznámením prokurátorovi alebo bezpečnostnému orgánu. *Trestný čin je pre spoločnosť nebezpečný čin, ktorý naplnil znaky svojej skutkovej podstaty.*

znakov príslušnej skutkovej podstaty), ďalej *podnecovanie a schvaľovanie trestného činu, nadržovanie páchateľovi, neprekazenie a neoznámenie trestného činu, pohŕdanie súdom, krivá výpoveď*.[19]

Kontinuálne (*v druhom rade*) je nutné rešpektovať, že identifikáciou môžu dospieť k záveru, že touto špecifickou komparáciou foriem trestnej činnosti ide o recidívu, súbeh trestných činov, pokračovací trestný čin, resp. trestný čin spáchaný opakovane. Recidívou sa v trestnom práve rozumie prípad, ak ten istý páchateľ znovu spácha trestný čin po tom, ako ho súd právoplatne odsúdil za iný predchádzajúci trestný čin.

Podľa trestnoprávnej teórie o súbeh trestných činov ide vtedy, ak ten istý páchateľ spácha dva alebo viac trestných činov pred tým, ako bol za niektorý z nich odsúdený súdom prvého stupňa a pokiaľ nezanikla trestnosť niektorého z nich.

Za pokračovací trestný čin sa považuje, ak páchateľ pokračoval v páchaní toho istého trestného činu. Trestnosť všetkých čiastkových útokov sa posudzuje ako jeden trestný čin, ak všetky čiastkové útoky toho istého páchateľa spája objektívna súvislosť v čase, spôsobe ich páchania a v predmete útoku, ako aj subjektívna súvislosť, najmä jednotiaci zámer páchateľa spáchať uvedený trestný čin; to neplatí vo vzťahu k čiastkovým útokom spáchaným mimo územia Slovenskej republiky (*ustanovenie § 122 TZ*).

Trestný čin je spáchaný opakovane, ak páchateľ postupne spáchal viac rovnakých trestných činov opakovanými samostatnými činmi, medzi ktorými nie je žiadna objektívna alebo subjektívna súvislosť, pričom trestnosť každého z nich sa posudzuje samostatne. V policajno-bezpečnostnej praxi sú štyri a viac opakovane spáchané trestné činy označované termínom trestné činy páchané v sérii (*aj sériová trestná činnosť*). Pritom kvantifikácia počtu trestných činov je spájaná so samotným účelom ich poznávania (*identifikácia páchateľa, prostriedkov, prostredia – situácie, udalosti, v neposlednom rade časového sledu*).

Objektívna a subjektívna súvislosť trestného činu sú dva rôzne aspekty, ktoré sa posudzujú pri posudzovaní trestnosti činu. Objektívna súvislosť sa týka zjavnej súvislosti medzi jednotlivými trestnými činom, zatiaľ čo subjektívna súvislosť sa týka páchateľovho vedomia a úmyslu. Objektívna súvislosť sa týka toho, či medzi jednotlivými trestnými činmi existuje zjavný vzťah. Napríklad, ak ide o pokračovací trestný čin, kde sa páchateľ opakuje v páchaní toho istého trestného činu. V takom prípade sa všetky čiastkové útoky posudzujú ako jeden trestný čin,

Subjektívna súvislosť sa týka páchateľovho vedomia a úmyslu. Napríklad, ak osoba spáchala viaceré trestné činy, ktoré sú spojené tým, že ich páchateľ spáchal s tým istým úmyslom alebo v rámci jedného komplexu, môže sa to považovať za viacčinný súbeh trestných činov.[20] *Napríklad, ak niekto spácha viaceré trestné činy počítačovej kriminality v priebehu jedného dňa, pričom tieto konania boli spáchané s tým istým úmyslom - obohatiť sa - môže sa to posudzovať ako jeden trestný čin. Tu ide o súbeh objektívnej a subjektívnej súvislosti, pretože tieto sú zjavne spojené (objektívna súvislosť) a boli spáchané s tým istým úmyslom (subjektívna súvislosť).*

Rešpektujúc uvedené vo vzťahu k potrebám identifikácie série trestných činov počítačovej kriminality, PBO hľadajú odpovede na otázku:

Odhalené trestné činy (počítačovej kriminality) sú páchané opakovane v sérii?

Uvedomujeme si, že nami formulovaná otázka je lakonická, jej zodpovedanie však súvisí s identifikáciou znakov skutkových podstát trestných činov (*odhaľovanie,*

[19] IVOR, J. a kol. *Trestné právo hmotné 1. Všeobecná časť.*

[20] *Objektívna súvislosť*: vzťah medzi trestnými činmi, ktorý je zjavný z ich povahy a okolností.
Subjektívna súvislosť: vzťah medzi trestnými činmi, ktorý je založený na vedomí a úmysle páchateľa.

objasňovanie), ako aj ich vzájomnou komparáciou. Zjednodušene povedané, pri hľadaní odpovede na ňu je nutné pracovať s mnohými ďalšími otázkami.

2. Akceptácia delegovaných kompetencií vo vzťahu k realizácii identifikácie

PBO po definovaní identifikačného problému vykonávajú analýzu a hodnotenie vlastných predpokladov aplikácie foriem identifikácie (*Prezídium PZ, Národná centrála osobitných druhov kriminality, odbor počítačovej kriminality, oddelenie objasňovania a odborných činností, oddelenie odhaľovania*).[21] Ide o zhodnotenie informačného zázemia nevyhnutného na aplikáciu a zdôvodnenie nárokov na ich odbornú, psychickú a fyzickú úroveň a samotnú dispozíciu kompetencií a pod. V tomto realizačnom štádiu foriem identifikácie PBO hodnotia:

- ✓ impulzy odhaľovania a objasňovania, z ktorých môžu vymedziť identitu potrieb týchto špecifických PBČ,
- ✓ dispozíciu právom regulovaných kompetencií,
- ✓ možnosti súvisiace s prevzatím zodpovednosti za realizáciu identifikácie v termínových a priestorových dimenziách,
- ✓ personálne predpoklady aplikácie formy identifikácie, určenie subjektov pre realizáciu konkrétnych činností,
- ✓ definovanie potreby koordinácie, vymedzenie potreby a určenie spôsobov kooperácie s občanom, predbežné opatrenia z hľadiska prípadného krytia skutočného záujmu a cieľov aplikácie formy identifikácie smerom k verejnosti a obyvateľom, záujmovým objektom a subjektom,
- ✓ v prípade potreby zabezpečenie bezpečnosti účastníkov aplikácie tejto metódy a takisto nezúčastnených osôb,
- ✓ materiálno-technické zabezpečenie aplikácie formy identifikácie,
- ✓ predpokladaný informačný výstup a prípravu na zmenu situácie po jeho prezentácii.

Výsledky výskumu naznačujú, že pre riešenie identifikačného problému v účelovo realizovaných procesoch odhaľovania a objasňovania je vhodné zriadiť tím z PBO a do riešenia identifikačnej úlohy prizvať odborníkov z iných vedných odborov a profesií (*mimorezortných*). Osobitne je to dôležité pre účinnú a efektívnu aplikáciu identifikácie systémov.

Účelom realizácie tejto etapy je, nadväzne na formulovaný identifikačný problém, vyvodiť taktické zámery aplikácie foriem identifikácie. Na základe taktických zámerov (*podľa zložitosti predpokladaného postupu*) je nevyhnutné rozhodnúť o potrebe vypracovania písomného *plánu vykonania formy identifikácie.* Tým končí vecná, t. j. obsahová časť prípravy na ich aplikáciu. Po nej nasleduje organizačno-materiálna časť prípravy, ktorá vychádza z predchádzajúcich taktických zámerov. Jej podstata je však v tom, že plní funkciu ich konkrétneho zabezpečenia, a to po organizačnej a materiálnej stránke.

Takto konkretizované personálne a organizačno-materiálne opatrenia sa vyjadria (*celkom konkrétne*) v pláne aplikácie formy identifikácie, ak bolo o jeho spracovaní v rámci taktických zámerov rozhodnuté.

---

[21] Príslušníci národnej centrály osobitných druhov kriminality Prezídia Policajného zboru, jedného z centrálnych útvarov služby kriminálnej polície, vykonávajú finančné vyšetrovanie, objasňujú, dokumentujú a vyšetrujú trestné činy legalizácie výnosu z trestnej činnosti, nelegálneho zaobchádzania s nebezpečnými materiálmi, prekurzormi a výbušninami, trestné činy environmentálnej kriminality, počítačovej kriminality so zameraním na oblasť detskej pornografie a ďalšej závažnej trestnej činnosti páchanej prostredníctvom počítačového systému, sietí alebo počítačových dát a pôsobia na úseku pátrania a cieľového pátrania po páchateľoch najzávažnejšej trestnej činnosti.

3. *Analýza objektov identifikácie*

Zmeny v prostredí, ktoré sú vyvolané pri páchaní trestných činov, je možné identifikovať podľa konkrétnych príznakov, resp. ich súborov, pretože ich existenciu podmieňuje celý rad známych princípov, resp. zákonitostí (*napríklad teória odrazu, teória systému, ...*). Z uvedeného poznania vyplýva záver, že nie je možné, aby existovala kriminálna aktivita (*trestný čin*), počas ktorej by neboli medzi jednotlivými objektmi vzájomne odovzdávané informácie vzťahujúce sa práve k nim. To znamená, aby nedošlo k zmene v prostredí, v ktorom sú realizované kriminálne aktivity v jednotlivých etapách páchania trestného činu.[22]

Objektmi foriem identifikácie série trestných činov počítačovej kriminality sú znaky ich skutkových podstát. Predmetom tohto špecifického poznávania je samotná intencionálna činnosť (*aktivity*) vykonávaná používaním počítačov, prípadne inými počítačovými alebo komunikačnými zariadeniami pri dosahovaní kriminálnych cieľov. PBO ich identifikačnú funkciu určujú formulovaním problému, konkrétne definovaním úlohy, ktorú sa rozhodli plniť. Z praktického poznania vyplýva, že realizáciu identifikácie ovplyvňuje celý rad faktorov. Osobitnú pozíciu medzi nimi zastáva úroveň poznania skutkových podstát trestných činov a ich možná dispozícia pre potreby aplikácie metód identifikácie.

Tak, ako sme uviedli, trestná činnosť počítačovej kriminality predstavuje heterogénny jav, ktorý zasahuje do širokého spektra trestných činov upravených v osobitnej časti Trestného zákona. Nejde len o skutky, pri ktorých je počítačové zariadenie priamym objektom alebo cieľom útoku, ale aj o činy, kedy sa počítač využíva ako nástroj alebo nosič informácií a dát, prostredníctvom ktorých sa napĺňajú znaky rôznych trestných činov. Protiprávna činnosť páchateľov v tejto oblasti má potenciál zasiahnuť do širokej škály základných ľudských práv a slobôd. V ďalšej časti stručne charakterizujeme vybrané trestné činy, ktoré reflektujú zásahy do počítačových zariadení a ich systémov, ktoré môžu byť objektmi identifikácie.

§ 247 - Neoprávnený prístup do počítačového systému

Ustanovenie § 247 Trestného zákona upravuje skutkovú podstatu trestného činu neoprávneného prístupu do počítačového systému, ktorého podstatou je prekonanie bezpečnostného opatrenia a následné získanie neoprávneného prístupu do počítačového systému alebo jeho časti.[23] Predmetom právnej ochrany v tomto prípade je počítačový systém ako celok a jeho jednotlivé časti vrátane technického a softvérového vybavenia. Objektívnu stránku trestného činu napĺňa konanie páchateľa, ktorý vedome a bez oprávnenia prekoná bezpečnostné opatrenie systému – napríklad heslo, šifrovací mechanizmus alebo hardvérovú ochranu – čím získa neoprávnený prístup. Na naplnenie základnej skutkovej podstaty nie je potrebné, aby konanie spôsobilo škodu; jej vznik však môže predstavovať kvalifikačný znak umožňujúci uloženie prísnejšieho trestu. Subjektom tohto trestného činu môže byť akákoľvek trestne zodpovedná fyzická alebo právnická osoba. Pokiaľ ide o subjektívnu stránku, tento trestný čin si vyžaduje úmyselné zavinenie – z dôvodu odbornej povahy zásahu a typického sofistikovaného postupu páchateľa je vylúčené jeho spáchanie z nedbanlivosti.

§ 247a - Neoprávnený zásah do počítačového systému

Ustanovenie § 247a Trestného zákona upravuje skutkovú podstatu trestného činu neoprávneného zásahu do počítačového systému, ktorého podstatou je obmedzenie alebo

---

[22] PORADA, V. a J STRAUS. Kriminalistická stopa. In: *Kriminalistika* [online]. Praha: MV ČR, 1999, roč. 32., č. 3, s. 187. [cit. 7. marca 2025]. Dostupné na internete: <http://www.mvcr.cz/soubor/1999-zip.aspx>

[23] *§ 247 zákona č. 300/2005 Z. z., Trestný zákon.*

prerušenie fungovania počítačového systému alebo jeho časti neoprávnenou manipuláciou s počítačovými údajmi alebo zásahom do technického alebo softvérového vybavenia systému.[24] Predmetom ochrany je počítačový systém a jeho funkčnosť, a to v plnom rozsahu vrátane podpory riadneho chodu systému. Objektívna stránka je založená na spôsobe narušenia alebo prerušenia funkcie prostredníctvom neoprávneného zásahu. Pri tomto trestnom čine môže ísť o kumulatívne prepojenie napríklad s trestným činom neoprávneného prístupu do počítačového systému. Subjektom tohto trestného činu môže byť akákoľvek trestne zodpovedná fyzická alebo právnická osoba. Pokiaľ ide o subjektívnu stránku, tento trestný čin si vyžaduje úmyselné zavinenie.

§ 247b - Neoprávnený zásah do počítačového údaja

Ustanovenie § 247b Trestného zákona upravuje skutkovú podstatu trestného činu neoprávneného zásahu do počítačového údaja, ktorého podstatou je úmyselné poškodenie, vymazanie, pozmenenie, potlačenie alebo zneprístupnenie počítačových údajov alebo zhoršenie ich kvality.[25] Predmetom ochrany je dôvernosť, integrita a dostupnosť informácii s odkazom na technickú normu ISO/IEC TS 27000:2018. Skutková podstata je naplnená akýmkoľvek zásahom, ktorý vedie k poškodeniu údajov, či už ide o zníženie ich kvality, úplné zničenie alebo zneprístupnenie. Subjektom tohto trestného činu môže byť akákoľvek trestne zodpovedná fyzická alebo právnická osoba. Pokiaľ ide o subjektívnu stránku, tento trestný čin si vyžaduje úmyselné zavinenie.

§ 247c - Neoprávnené zachytávanie počítačových údajov

Ustanovenie § 247c Trestného zákona upravuje skutkovú podstatu trestného činu neoprávneného zachytávania počítačových údajov, pri ktorom dochádza k neoprávnenému zachytávaniu počítačových údajov, napríklad prostredníctvom technických prostriedkov počas neverejného prenosu údajov alebo zachytávaním elektromagnetických emisií.[26] Predmetom ochrany je súkromie pri elektronickej dátovej komunikácii. Podobne ako pri ostatných skutkoch z tejto kategórie, ani tu sa nevyžaduje spôsobenie škody, no pri značnej škode možno uplatniť vyššiu trestnú sadzbu.

§ 247d - Výroba a držba prístupového zariadenia, hesla alebo iných údajov

Ustanovenie § 247d Trestného zákona upravuje skutkovú podstatu trestného činu spojeného s výrobou a držbou prístupového zariadenia. Predstavuje trestný čin ktorý môžeme označiť ako predčasne dokonaným. Upravuje situáciu, keď páchateľ v úmysle spáchať niektorý z predchádzajúcich trestných činov vyrobí, dovezie, obstará, predá alebo sprístupní zariadenie (vrátane softvéru) určené na neoprávnený prístup, alebo získa a sprístupní heslo, prístupový kód alebo iné údaje umožňujúce neoprávnený vstup do systému.[27]

Samozrejme, uvedomujeme si, že tento zoznam trestných činov počítačovej kriminality je neúplný.[28] Medzi kľúčové charakteristiky tejto trestnej činnosti patrí vysoká latencia, vysoká miera anonymity a potreba špecifických technických znalostí a schopností zo

---

[24] *§ 247a zákona č. 300/2005 Z. z., Trestný zákon.*
[25] *§ 247b zákona č. 300/2005 Z. z., Trestný zákon.*
[26] *§ 247c zákona č. 300/2005 Z. z., Trestný zákon.*
[27] *§ 247d zákona č. 300/2005 Z. z., Trestný zákon.*
[28] Objektmi identifikácie série môžu byť ďalšie skutkové podstaty trestných činov: „*§ 174 – Šírenie toxikománie, § 221 – Podvod, § 226 - Neoprávnené obohatenie, § 282 - Porušovanie priemyselných práv, § 283 – Porušovanie autorského práva, § 360b – Nebezpečné elektronické obťažovanie, § 368 – Výroba detskej pornografie, § 369 – Rozširovanie detskej pornografie, § 370 – Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení, § 374 – Neoprávnené nakladanie s osobnými údajmi, § 422b – Rozširovanie extrémistického materiálu.“*

strany páchateľov. Tieto schopnosti sa často prejavujú vo vysokej miere sofistikovanosti pri páchaní protiprávnej činnosti.

Prax potvrdzuje, že pri riešení identifikačných úloh sú PBO povinné analýzou charakterizovať identifikačné objekty požadovaným počtom vlastností, ktoré umožňujú jednoznačne určiť ich identitu. Pritom sú povinné vyhodnocovať tieto vlastností z hľadiska ich stálosti (*trvanlivosti*), pretože využiteľnosť premenných vlastností objektov (*v čase a priestore*) pre potreby identifikácie je dočasná a pod. V tomto smere je vhodné uviesť, že pri aplikácii foriem identifikácie medzi pomerom stálych a premenných identifikačných vlastností musí existovať určitá vyváženosť. Napríklad, ak majú PBO pri identifikácii nedostatok stálych identifikačných vlastností, túto absenciu vypĺňajú skúmaním a vyhodnocovaním premenných vlastností. Aj táto možnosť pomerne výrazne vymedzuje špeciálnosť aplikácie foriem identifikácie série trestných činov počítačovej kriminality. K uvedenému je vhodné dodať, že redundancia informácií pre potreby identifikácie výrazne negatívne ovplyvňuje jej efektivitu. Táto skutočnosť je evidentná, tak pri určovaní identity subjektov, ako aj činností spájaných s používaním počítača.

Ak identifikačným objektom je počítač, PBO:

- ✓ určujú jeho aplikačnú funkciu (*záujmový, resp. preverovaný objekt*),
- ✓ modelom vytvoria jeho systémovú identitu (*akceptujúc alternatívy*),
- ✓ stanovia možnosti jeho dispozície (*miestna, časová, vlastnícke vzťahy, právna regulácia činnosti súvisiace so zabezpečením vec, a pod*.),
- ✓ rozhodnú o aplikácii metód identifikácie (*s vymedzením zodpovednosti*) a pod.

PBO pre potreby aplikácie foriem identifikácie pri vypracovaní informačných charakteristík objektov využívajú najmä kriminalistické, kriminologické metódy, metódy forenzných vedných disciplín a osobitne metódy PBČ (*napríklad OPČ, SČ – osobné vyhľadávanie, operatívne vyťažovanie, operatívnu prehliadku, operatívne pozorovanie, operatívne zisťovanie a šetrenie a iné).* V súlade a rozsahu zákona sú pri tejto činnosti oprávnené využívať prostriedky OPČ a ITP. V prípade, že nedisponujú potrebným poznaním o objektoch identifikácie, vyhodnocujú dostupné informačné siete, ktorých vyťažením môže tento identifikačný handicap odstrániť.

V konkrétnej syntéze uvádzanú realitu PBO akceptujú. Uvedomujú si, že komplikovanosť gnozeologického prístupu v procesoch identifikácie série trestných činov počítačovej kriminality spôsobujú najmä:

- ✓ Špecifická zložitosť a značná variabilnosť ich znakov *(subjektom trestného činu je človek, ..., poznávanie rozličných vlastností ľudí, najmä psychických, teda javových, ktoré sa vymykajú bezprostrednému pozorovaniu a meraniu, analogicky uvedené je možné uviesť aj vo vzťahu k používaniu počítača a pod.).*
- ✓ Ich retrospektívne poznávanie – pomerne frekventované vlastnosti objektov identifikácie nie sú dostupné priamemu a systematickému pozorovaniu *(výnimkou môže byť aplikácia kompetencií, ktoré vyplývajú z právnej, organizačno-riadiacej a taktickej regulácie OPČ, resp. SČ).*
- ✓ Odhaľovanie, skúmanie, hodnotenie a vysvetľovanie ich prejavov realizujú na základe subjektívne sprostredkovaných hodnôt a interakcií, najmä vzťahov subjektu k poškodeným (*obetiam*), ako aj k PC.
- ✓ Odhaľovanie, skúmanie, hodnotenie a vysvetľovanie kriminálnych aktivít prebieha v konkrétnom prostredí *(sociálnom).*
- ✓ Latencia príčin, podmienok vzniku, existencie a zániku znakov kriminálneho konania *(genéza ich existencie).*
- ✓ Aktivity subjektov trestných činov*, ktorí sú súčasťou spoločnosti, v ktorej je páchaný trestný čin.*
- ✓ Odbornosť PBO a ich prístupy k plneniu špeciálnych identifikačných úloh.

- ✓ Koordinácia v rámci plnenia úloh orgánov policajno-bezpečnostných zložiek, znalcami, konzultantmi a v neposlednom rade s poškodenými (*obmedzené možnosti*) a pod.

Aj napriek týmto skutočnostiam presadzujú gnozeologický optimizmus, že páchané a spáchané trestné činy sú plne poznateľné. Z empirického poznania vyplýva, že pre zabezpečenie metodického prístupu pri analýze trestného činu je vhodné, ak PBO využívajú *vypracované modelové typové kriminálne charakteristiky trestného činu.* Dá sa povedať, že ide v podstate o najbohatší a najaktuálnejší metodicky informačný obsah spracovaný pre účely identifikácie série trestných činov počítačovej kriminality. Z hľadiska týchto potrieb kriminálnu charakteristiku trestného činu (*systémový model*) predovšetkým tvoria:

- ✓ typické formy páchania trestnej činnosti (*skutková podstata, štádia, trestná súčinnosť*),
- ✓ typické situácie v čase páchania trestného činu,
- ✓ typické vlastností potenciálneho páchateľa (*pohlavie, vek, vzťah k miestu udalosti, intelektuálna vyspelosť, odbornosť, kriminálna minulosť(skúsenosť), a pod*.),
- ✓ účel kriminálneho konania a sledované ciele páchateľov,
- ✓ motivácia a motívy páchania daného druhu trestných činov,
- ✓ typické spôsoby správania sa potenciálneho páchateľa (*pred, v priebehu a po spáchaní trestných činov*),
- ✓ povaha a osobitosti správania sa poškodených (*pred, v priebehu a po spáchaní trestných činov*) – osobitne vo vzťahu k používaniu PC, ITK a pod.,
- ✓ typické reálne, analytické a transferové (*apriórne*) informácie,
- ✓ osobitosti impulzov (*podnetov a indikátorov*) pre realizáciu identifikácie série,
- ✓ typické kriminálno-policajné (*napríklad operatívne*) situácie,
- ✓ osobitosti tvorby a previerky operatívno-pátracích verzií, plánovania a organizácie identifikácie,
- ✓ osobitosti typických počiatočných a následných opatrení a úkonov v procese identifikácie,
- ✓ typické dôkazy, vykonávanie dokazovania,
- ✓ metódy a prostriedky identifikácie a pod.

Zhromažďovanie faktov a informácií o prvkoch tohto systémového modelu, ich nepretržitá aktualizácia, spracovanie a transfery vytvárajú určitú sumu východiskových informácií o tzv. *predpolí* identifikácie série daného druhu trestných činov (*kriminality*). Zabezpečovanie tohto *„informačného manažmentu“* pre reálne potreby tohto špecifického poznávania sú povinní vykonávať PBO na jednotlivých stupňoch riadenia a účelovo zriadené koordinačné centrum. [29]

V súlade s našim poznaním predstavuje kriminálna charakteristika významný poznávací prostriedok, ktorý odporúčame využívať pri identifikácii série trestných činov a pod. Napríklad pri myšlienkovom modelovaní vlastností, resp. možných aktivít a vlastností o nezistených subjektov trestného činu, používaného počítača, prostredia, času a pod. Informácie o kriminálnej charakteristike trestného činu majú význam aj pri vytváraní evidenčných a informačných systémov, ktoré sú pre príslušníkov polície dôležitým nástrojom pri plnení stanovených úloh (*aj identifikačných*).

4. Používanie prostriedkov v metódach identifikácie (operácií a techník)

V procese aplikácie foriem identifikácie, pred vlastným identifikačným skúmaním, sú PBO povinné realizovať celý rad opatrení a úkonov. V ich obsahu vyťažujú informačné siete, analyticky spracujú relevantné informácie, na základe ktorých môžu vyhotoviť informačné charakteristiky objektov pre potreby identifikácie. Uvedené sa analogicky akceptuje aj pri

[29] LISOŇ, M., A. VAŠKO a kol. *Teória kriminálno-policajného poznania*, s. 77 a násl.

samotnom identifikačnom skúmaní. Pri skúmaní vzťahu medzi objektmi identifikácie sa využívajú vhodné metódy a prostriedky PBČ. Predovšetkým ich adresným využívaním PBO zvyšujú účinnosť a efektivitu aplikácie foriem identifikácie. PBO v prípade plnenia zadanej identifikačnej úlohy môžu objekt individualizovať podľa iného objektu (*systému rovnorodých vlastností*), resp. súboru objektov. Kritériá identifikačnej zhody predovšetkým určujú individualizovaný vzťah medzi komponentmi kriminálnej charakteristiky trestného činu (*odrážaným a jeho odrazom*). Pri ich vymedzovaní vychádzajú z axióm, ktoré tvoria základný predpoklad pre akceptáciu a objektivizáciu výsledkov identifikácie. Napríklad zohľadňujú možnú úroveň objektivity výstupného identifikačného poznania, ktorú môžu alternatívne dosiahnuť použitým induktívnym, resp. deduktívnym prístupom v systéme tejto práce s informáciami (*predpoklad, dôkaz*). Kritériami zhody (*pri aplikácii operatívnej identifikácie*) zisťujú, hodnotia a fixujú údaje, okolnosti, ktoré je možné využiť pri určovaní identity:

- ✓ kriminálneho konania (*trestné činy*), kritéria zhody – *prvky spôsobu páchania – motív, ciele, účel, prvky charakterizujúce konanie v štádiu prípravy, dokonania, správania sa páchateľa po spáchaní trestného činu, používanie prostriedkov a techník a pod.*,
- ✓ účasti konkrétnych osôb na kriminálnom konaní – páchateľ, poškodený (*v štádiu prípravy, páchania, resp. po odchode z miesta činu*),
- ✓ charakteristiky osobností potenciálnych páchateľov *(podozrivých, rozpracovaných*, *obvinených, obžalovaných, odsúdených, odbornosť, špecializácia, a pod.),*
- ✓ poškodených (*obetí*) trestných činov,
- ✓ času a prostredia páchania trestných činov,
- ✓ vzťahu k už v minulosti odhaleným trestným činom registrovaných v informačných systémoch,
- ✓ povahy a rozsahu spôsobeného následku (*škody, obete*),
- ✓ poľahčujúcich a priťažujúcich okolností,
- ✓ vecí získaných spáchaním trestným činov,
- ✓ počítačov, resp. ITK prostriedkov, ktoré boli použité pri páchaní trestného činu,
- ✓ iných predmetov, objektov, systémov, ktoré vykazujú konkrétnu relevanciu vo vzťahu k páchaným trestným činom,
- ✓ objektov a miest, v ktorých sa nachádzal, resp. nachádza majetok a iné hodnoty získané trestnou činnosťou,
- ✓ faktorov, ktoré umožňujú alebo uľahčujú páchať trestnú činnosť a pod.

Na základe praktických skúseností je možné uviesť, že PBO vlastnosti a parametre objektov identifikácie charakterizujú využitím:

- ✓ reálnych informácií,
- ✓ analytických informácií,
- ✓ apriórnych - transferových informácií,
- ✓ kombinácie reálnych, analytických a transferových informácií. [30]

Z charakteru identifikácie série trestných činov počítačovej kriminality vyplýva, že realizačný rozsah opatrení a úkonov určuje samotná povaha poznávaných objektov a povinná akceptácia delegovaných kompetencií realizujúcimi subjektmi. Z empírie je zrejmé, že PBO sa vykonávaním opatrení snažia pochopiť individuálny a celostný význam relevancie zistených informácií o trestných činoch. Pri popise a interpretácii informácií využívajú svoje odborné predpoklady a skúseností. Z informácií, ktoré majú k dispozícii, získavajú nové poznanie o skúmanom objekte, pričom zohľadňujú predovšetkým:

- ✓ genézu ich pôvodu a existencie,
- ✓ popis a interpretáciu,
- ✓ formuláciu domnienok, ich zdôvodnenie a logické preverenie.

[30] LISOŇ, M., A. VAŠKO a kol.. *Teória kriminálno-policajného poznania*, s. 143.

To potvrdzuje, že realizovanými opatreniami cieľavedome vysvetľujú (*dešifrujú a objektívne interpretujú ich význam*) východiskové poznanie. Z poznania praxe vyplýva, že je vhodné, ak pri tejto činnosti využívajú modelovanie. Poznávaný objekt zamieňajú zjednodušenými modelmi *(zobrazenie objektu vybranou množinou jeho vlastností – vytvárajú mentálny model (myšlienkový).* Pri ich zostavovaní akceptujú zadanie *(úlohu).* Vychádzajú z informačnej potreby, interpretácie *(prečítania a vysvetlenia)* zhromaždených informácií a ich intelektuálneho spracovania. To im umožňuje extrahovať dôležité entity a väzby reprezentujúce zmysel obsahu informácií, ako aj plnenie svojej úlohy pri identifikovaní určitých objektov. Získané a dodané informácie skúmajú a hodnotia v paralelnom režime *(jednotlivé informácie súčasne) a* následne ich zoraďujú do série, v ktorej ich spracovávajú – jednu po druhej *(po slovách).* Z empírie je zrejmé, že pri výkone opatrení je vhodné, ak pri aplikácii metód identifikácie série trestných činov počítačovej kriminality *(mentálnom modelovaní)* používajú grafické schémy, napríklad*:*

- ✓ *vzťahové* – vzťahy medzi prvkami *(osoby – subjekt verzus poškodený /obeť/, organizácia, veci, PC, ITK, miesto, čas a iné),*
- ✓ *komoditné* – (*napr. ilustrujú tok tovarov, peňazí a ďalších komodít, ktoré môžu predstavovať predmet kriminálnych aktivít),*
- ✓ *kauzálne* – znázorňujú súvislosti javu, udalosti *(odhaľujú časové a priestorové vzťahy medzi páchanými trestnými činmi),*
- ✓ *postupové* – znázorňujú priebeh procesov *(genézu),* poradie udalostí, dosiahnutie výsledkov alebo stavov *(potvrdenie predpokladov o realizovaných kriminálnych aktivitách v minulosti, resp. ich prognóza, latencia)),*
- ✓ *sieťové* – umožňujú identifikovať hlavné a zvláštne charakteristiky veľkého množstva rovnakých prejavov v konaní subjektu alebo udalostí *(jeho status, rola v spoločnosti, odbornosť, komunikácia s poškodeným a pod.)* a iné.

Na zabezpečenie prehľadnosti a uľahčenie interpretácie zhromaždených informácií sa využívajú aj ďalšie formy znázornenia:

- ✓ porovnávacie záznamy (*podobnosť, odlišnosť*),
- ✓ frekvenčné analýzy (t*ypické, zvláštne*),
- ✓ časové analýzy (*trend, perióda, časová korelácia*),
- ✓ projekcia do máp (*udalosť, príčina, následok viažuci sa na atribúty miesta výskytu*).

Z uvedeného je zrejmé, že PBO pri plnení stanovených úloh opatreniami – analyticko-syntetickou metódou, popisom a interpretáciou zhromaždených informácií – potvrdzujú už existujúce poznanie, resp. získavajú nové poznanie. Prostredníctvom nich konštruujú systémový model vzťahov medzi skúmanými trestnými činmi (*verbálny, grafický*). V tomto postupe domnienkami vyjadrujú najmä predpokladané charakteristiky týchto vlastností a ich možné vzájomné vzťahy, a to v konkrétnej forme prejavu. Okrem iného si uvedomujú, že predpokladom na dosahovanie pridanej hodnoty (*nové poznanie*) v procesoch identifikácie série trestných činov počítačovej kriminality je predovšetkým štúdium objektov, ich vzťahov a vzájomných účinkov.

5. Spracovanie informačných výstupov z identifikácie série a ich využitie

Informačnými výstupmi z aplikácie foriem identifikácie série trestných činov sú texty – dvojstranné bilaterálne kategórie (*výsledok, efekt*), ktoré majú obsahovú a formálnu stránku. Majú potenciálny (*očakávaný*), resp. aktuálny poznávací charakter. Bez ohľadu na úplnosť je možné uviesť, že PBO aplikáciou foriem identifikácie nachádzajú odpovede na otázky:

- ✓ Aké boli dôvody realizácie procesov identifikácie?
- ✓ Ako boli odhalené a objasnené porovnávané trestné činy (kriminálne aktivity)?
- ✓ Kto, kedy, využitím akých kompetencií realizoval procesy identifikácie?

- ✓ Podľa akých vlastností sú charakterizované trestné činy pre potreby identifikácie série?
- ✓ Aká je právna kvalifikácia trestného činu? (štádium trestného činu)
- ✓ Ktoré subjekty sú zainteresované na realizácii kriminálnych aktivít? trestno-právna súčinnosť)
- ✓ Čo je predmetom záujmu kriminálnych subjektov?
- ✓ Na aký účel boli spáchané trestné činy? (analogicky cieľ, motív)
- ✓ Kde, kedy, ako často sú trestné činy spáchané (páchané)?
- ✓ Akým spôsobom sú kriminálne aktivity realizované? a iné.
- ✓ Pre koho je spracovaný informačný produkt?

Z uvedeného vyplýva, že nimi spracovaný informačný výstup musí vyhovovať určitým formálnym a vecným požiadavkám. V prvom rade pri jeho spracovaní sú PBO povinné rešpektovať právnu reguláciu odhaľovania a objasňovania. Jej imanentnou súčasťou je manipulácia a prístup k informáciám. V neposlednom rade sú povinné tento produkt spracovať presne, v predpísanej podobe (*formálne*) a tak jednoznačne, aby mohol byť chápaný (*interpretovaný*) v tom istom zmysle, ako je prezentovaný, a nie inak.

Aktuálny informačný produkt z foriem identifikácie série je výsledkom opisu trestných činov počítačovej kriminality. V jeho obsahu je určená identita určitých vlastností porovnávaných trestných činov (*kriminálna aktivita, iný proces, subjekt a pod.*), osobitne:

- ✓ Existencia objektov – rešpektujúc trestno-právnu charakteristiku obligatórnych a fakultatívnych znakov skutkových podstát trestných činov.
- ✓ Súdržnosť páchaných a spáchaných trestných činov, ktorá zabezpečuje kompaktnosť kriminálneho konania páchaného v sérii. Napríklad sú riešené otázky: *„či ich páchanie má systémový charakter?“*; *„ako je možné charakterizovať genézu ich existencie?, aké sú väzby medzi ich prvkami (znaky modus operandi)“*; *„či poznávané konanie v sérii nevykazuje tendencie dynamiky?“; „aká je ich kompaktnosť? (technická, technologická, časová, priestorová, viktimológická a pod.)“; „aké sú ich väzby v prostredí páchania?“; „aké sú ich väzby (vzťahy) k policajnému poznaniu?“* a pod.
- ✓ Cieľové správania subjektu trestných činov páchaných v sérii, ktoré sú definované vlastným usporiadaním prvkov, jeho osobnostnými vlastnosťami, ktoré sú determinované vplyvmi prostredia, v ktorom žije a pod. *Na základe poznania tejto determinácie sú určované motívy, účel, ciele spáchania trestného činu a iné znaky spôsobu páchania a spáchania trestného činu (osobitne spájané s poškodenými /obeťami/). Samozrejme, je to optimálna skutočnosť, v praxi totiž realizáciou identifikácie môže dôjsť k zisteniu rozporu s očakávaným správaním subjektu.* Z týchto dôvodov je potrebné (predovšetkým) využívaním verzií poznávať vlastné správanie subjektu rešpektujúc možné alternatívy, ktoré sú konfrontované objektivizovaním platnosti vyslovených domnienok. Pri nezhode je potrebná ich korekcia v súlade s už spomenutými alternatívami. Aj v tomto prípade sú riešené otázky: *„Ide o sériu?“ a pod.*
- ✓ Dynamická stabilita a adaptácia subjektu trestných činov páchaných v sérii, jeho reakcie a schopnosti reagovať na okolnosti, ktoré vznikli, resp. môžu vzniknúť v určitom prostredí (*konkrétnej situácii*). Osobitne sa to odráža pri poznávaní reálnych informácií. *(„Aké faktory pôsobili v čase a mieste páchania porovnávaných trestných činov?“; „Ktoré okolnosti pôsobili za existujúcej situácie?“, „Ktoré vlastnosti charakterizujú extrémnosť pôsobenia na kriminálne konanie subjektu?“ „V akom časovom intervale pôsobili?“; „Ktoré vlastnosti a ako ich ovplyvnili?“; „Aké odrazy mohli spôsobiť?“ atď.).*

- ✓ Zmeny, ktoré súvisia s vývojovom subjektu (*dispozícia kriminálnych skúseností a zručností, kapacitné vlastnosti, finančná disponibilita, používaná počítačová technika...),* osobitne tie, ktoré môžu viesť k posilneniu cieľov *(„s jedlom rastie chuť“),* zmene cieľov, kriminálnej orientácie a pod.
- ✓ Ochrana subjektu a jeho záujmov (*vnútorná, vonkajšia; spoľahlivosť prvkov a väzieb, ktoré zabezpečujú realizáciu trestných činov počítačovej kriminality, pre naplnenie vnútorných a najmä vonkajších cieľov (legálnych a nelegálnych) a pod*.).
- ✓ Organizácia práce a riadenie subjektu (*pácha trestný čin sám v spolupáchateľstve /princípy – spolčenie, zoskupenie/, jeho schopnosť vybrať a presadiť také procesy v systéme, ktoré vedú k splneniu cieľov v potrebnom čase*).
- ✓ Účinnosť a efektívnosť aktivít subjektu (*jeho status, rola v kriminálnom prostredí, prečo je akceptovaný?, prečo dosahuje ciele?, ako a čo využíva? a iné*) a pod.

Z tohto neukončeného zoznamu je možné vymedziť konkrétne kritériá, ktoré je vhodné využiť pri právnom, personálnom a ekonomickom posúdení informačnej hodnoty dosiahnutého identifikačného poznania série trestných činov počítačovej kriminality. Predovšetkým ich akceptáciou je možné hodnotiť osobnú akceptáciu kompetencií (*zodpovednosti*) pri plnení stanovených úloh (*organizácia a riadenie práce PBO*). Tá je základným predpokladom pri dosahovaní stanovených informačných cieľov, a to realizáciou práve týchto špecifických procesov.

Záver

V súlade s požiadavkami policajno-bezpečnostnej praxe (*spoločnosti*) je možné vysloviť záver, že vo vzťahu k páchaným trestným činom počítačovej kriminality je potrebné riešiť rozpory medzi dynamicky sa meniacou bezpečnostnou situáciou a používanými prístupmi pri jej riešení. Uvedené skutočnosti sú odborníkom na bezpečnosť (ale aj pomerne veľkej časti občanov) zrejmé, preto permanentne hľadajú odpovede na otázku: „Ako danú situáciu riešiť? V týchto intenciách si PBO uvedomujú, že pocit a potreba bezpečnosti je základnou spoločenskou potrebou. Rešpektujú, že bez adekvátneho riešenia bezpečnosti aj v kybernetickom priestore nie je možná reálna ekonomická prosperita, zvyšovanie a skvalitňovanie životného štandardu obyvateľov, rozvoj ich slobodných aktivít vo všetkých spoločenských sférach i ochrany ich dôstojnosti. Tieto skutočnosti výrazne ovplyvňujú ich samotnú orientáciu a prístup k plneniu zákonom delegovaných úloh.

Z rámcovo vymedzených úloh, ktoré sú PBO povinné plniť, je zrejmé, že cieľom ich činnosti je predovšetkým zabezpečiť neodvratnosť trestného postihu pre páchateľov trestných činov. Včasnosť, dôslednosť a zákonnosť postihov páchateľov za spáchaný trestný čin majú priamy dopad na dosahovanie účelu odhaľovania. Vo vzťahu k zabezpečovaniu neodvratnosti trestného postihu má osobitný význam aplikácia ustanovení Trestného poriadku. Analogickým výkladom týchto ustanovení je možné dospieť k záveru, že trestno-procesné záruky neodvratnosti trestného postihu začínajú pôsobiť zároveň so vznikom trestno-právneho vzťahu, t.j. vzápätí po spáchaní trestného činu, resp. činu inak trestného.

Z praktického poznania vyplýva, že delegovanie zodpovednosti za účinnú a efektívnu aplikáciu identifikácie série trestných činov počítačovej kriminality má širokospektrálny význam. Ten sa odráža najmä v účinnosti, efektivite, kvalite a v neposlednom rade v možnej kontrole realizovaných aktivít. Osobitne sa to týka činnosti realizovanej pri spracovaní a prezentácii výstupných informačných produktov potrebných na realizáciu prevencie a represie počítačovej kriminality.

Literatúra

FUNTA, Rastislav. *Komentár k Dohovoru Rady Európy o počítačovej kriminalite*. Bratislava: Wolters Kluwer, 2021. ISBN 978-80-571-0365-3.

IVOR, Jaroslav a kol. *Trestné právo hmotné 1: Všeobecná časť*. Bratislava: IURA EDITION, 2010. ISBN 978-80-8078-308-2.

JANÍČEK, Přemysl. a Roman RAK. Systémové pojetí identifikace. In: PORADA, Viktor a kol. *Kriminalistika*. Brno: Cerm Akademické nakladatelství, 2001. ISBN 80-7204-194-0.

KOLOUCH, Jan. *CyberCrime.* Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7.

LISOŇ, Miroslav. *Operatívno-pátracia činnosť (Všeobecná časť).* Bratislava, 2012. ISBN 978-80-8054-540-6.

LISOŇ, Miroslav, Adrián VAŠKO a kol. *Teória kriminálno-policajného poznania*. Bratislava: Wolters Kluwer, 2018. ISBN 978-80-8168-838-6.

POLČÁK, Radim a kol. *Právo informačních technologií*. Praha: Wolters Kluwer ČR, 2018. ISBN 978-80-7598-045-8.

Elektronické publikácie:

PORADA, Viktor a Jiří STRAUS. Kriminalistická stopa. In: *Kriminalistika* [online]. Praha: MV ČR, 1999, roč. 32., č. 3. [7. marca 2025]. Dostupné na internete: http://www.mvcr.cz/soubor/1999-zip.aspx.

14 Types of Hackers to Watch Out For [online]. 2025. [13. marca 2025]. Dostupné na internete: <https://www.pandasecurity.com/en/mediacenter/14-types-of-hackers-to-watch-out-for/>

What is a Black-Hat hacker? [online]. 2025. [7. marca 2025]. Dostupné na internete: https://www.kaspersky.com/resource- center/threats/black-hat-hacker.

What is ethical hacking? [online]. 2025. [10. marca 2025]. Dostupné na internete: https://www.ibm.com/topics/ethical-hacking.

White hat, black hat, grey hat hackers: What's the difference? [online]. 2025. [10. marca 2025]. Dostupné na internete: https://www.malwarebytes.com/blog/news/2021/06/white-hat-black-hat-grey-hat-hackers-whats-the-difference.

Zákony a iné dokumenty

ISO/IEC 27032:2012 – Introduction [online]. 2025. [3. marca 2025]. Dostupné na internete: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:en.

Zákon č. 300/2005 Z. z. Trestný zákon v znení neskorších predpisov.

Zákon č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

Keywords: computer crime, cybercrime, characteristics of computer crime, elements of computer crime offences, series of criminal offences, identification, object identification, systems identification, procedures for conducting identification.

Summary

This paper addresses the need to reconcile the rapidly evolving security environment with current approaches to tackling cybercrime. It highlights that both security professionals and the public perceive cyber threats as a pressing societal issue. Ensuring security in

cyberspace is deemed essential for economic prosperity, quality of life, and the protection of human dignity. The role of law enforcement bodies is emphasized, particularly their duty to ensure the inevitability of criminal liability. The importance of timely, lawful, and thorough prosecution is underscored as a key to effective detection. Criminal procedural safeguards are activated immediately after a crime is committed. The study also stresses the strategic value of identifying serial cybercrime and the importance of high-quality information outputs for preventive and repressive measures.

prof. Ing. Miroslav Lisoň, PhD.
Katedra kriminálnej polície
Akadémia Policajného zboru v Bratislave
e-mail: miroslav.lison@akademiapz.sk

Mgr. Gabriel Moskvič, LL.M.
Katedra kriminálnej polície
Akadémia Policajného zboru v Bratislave
e-mail: gabriel.moskvic@akademiapz.sk

Recenzenti: pplk. Ing. Marian Suja, PhD.
pplk. JUDr. Matej Kostrec, PhD.