Odhalování a kontrola počítačové kriminality

Detection and Monitoring of Cybercrime

Bc. Václav Pechlát

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Václav Pechlát**
Osobní číslo:	**A11378**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Odhalování a kontrola počítačové kriminality**

Zásady pro vypracování:

1. **Zpracujete rešerši literatury, která se vztahuje k odhalování a kontrole počítačové kriminality.**
2. **V rámci východiskové hypotézy vymezte fenomenologické a etiologické otázky spojené s odhalováním a kontrolou počítačové kriminality, včetně souvisejících právních aspektů, viktimologie a historických souvislostí.**
3. **Analyzujte současnou dynamiku počítačové kriminality, vymezte rozdělení tohoto fenoménu včetně všeobecných postupů při vyšetřování počítačové kriminality.**
4. **Analyzujte kontrolní a preventivní postupy včetně institucionálního zakotvení příslušných institucí, které se těmto aktivitám věnují, případně mají věnovat [bezpečnostní politika státu]. Specifikujte názorovou hladinu dospělé populace k aktuálním otázkám počítačové kriminality.**
5. **V rámci tvůrčí části diplomové práce proveďte výzkum ke zvolené problematice, výstupy výzkumu a analytické části statisticky vyhodnoťte a pomocí statistických metod zpracujte do grafů a tabulek [včetně sociálních a ekonomických dopadů].**
6. **Tvůrčí část diplomové práce zaměřte na syntézu – vycházejte ze specifikace analytických závěrů a výstupů; prezentujte vlastní pohled na danou problematiku, pokuste se navrhnout a doporučit vlastní opatření.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **CHMELÍK, J. Vyšetřování trestné činnosti mládeže a páchané na mládeži v teorii a praxi. Praha: MV ČR, Sekce personální práce a vzdělávání, 1995.**
2. **JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.**
3. **NAKONEČNÝ, Milan. Motivace lidského chování. 1.vyd. Praha: Academia, 1997, 270 s. ISBN 80-200-0592-7.**
4. **TOMÁŠEK, Jan. Úvod do kriminologie: jak studovat zločin. Vyd. 1. Praha: Grada, 2010, 214 s. ISBN 978-80-247-2982-4.**
5. **Trestní zákoník a trestní řád: průvodce trestněprávními předpisy a judikaturou. Praha: Linde, 2010, 2 sv. (xviii, 1317, xviii, 1184 s.). ISBN 978-80-7201-808-6.**
6. **Úplné znění zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád). Vyd. 6. Praha: Armex, 2011, 291 s. ISBN 978-80-87451-04-5x.**
7. **VEČERKA, Kazimír. Prevence kriminality v teorii a praxi. Vyd. 1. Praha: Institut pro kriminologii a sociální prevenci, 1996, 202 s. ISBN 80-86008-24-x.**
8. **ZOUBKOVÁ, Ivana. Kontrola kriminality mládeže. 1. vyd. Dobrá Voda u Pelhřimova: Aleš Čeněk, 2002, 231 p. ISBN 80-864-7308-2.**

Vedoucí diplomové práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce se zabývá řešením problematiky počítačové kriminality a urychlením jejího prověřování a vyšetřování. V rámci tohoto se zabývá návrhem národní databáze IP adres a způsobu jejího vedení, zabezpečení, naplňování a vytěžování. Dále si tato práce klade za cíl být metodickou pomůckou pro orgány činné v trestním řízení, které se s prověřováním počítačové kriminality setkávají poprvé a neznají základní pojmy, vztahy a principy této problematiky.

Klíčová slova:

Počítačová kriminalita, hacker, právo, vyšetřování, doporučené postupy, prověřování, kriminologie, databáze IP adres, metodika, trestní řízení, neodůvodněné průtahy trestního řízení, počítačové podvody

ABSTRACT

This Diploma thesis has been addressed the problem of computer crime and speeding up its examination and investigation. It has dealt with the national database of IP addresses and the method of its management, security, fulfillment and exploitation. Further, this work has aimed to be a methodological tool for law enforcement proceedings with the screening of cybercrime which meeting for the first time and do not know the basic concepts, relationships and principles of this issue.

Keywords:

Computer crime, hacker, law, investigation, best practices, auditing, criminology, databases, IP addresses, methodology, criminal procedure, criminal procedure unjustified delays, computer fraud.

Poděkování

Na tomto místě bych chtěl poděkovat zejména svému vedoucímu diplomové práce PhDr. Mgr. Stanislavu Zelinkovi, za jeho podporu a mnoho cenných rad při vedení této mojí diplomové práce. Dále bych rád poděkoval svým kolegům za spolupráci při výzkumu prováděném v rámci této práce. Poděkování také náleží mojí přítelkyni Bc. Janě Halíčkové za velkou morální podporu při studiu.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

V práci policejního orgánu nastávají, kromě jiných, i takové situace, které mohou být vnímány jako neodůvodněné průtahy v trestním řízení. Tento termín nemá nikde v žádné normě svou definici, která by jej upravovala, a na jejímž základě by bylo možno takovou situaci jako neodůvodněný průtah v trestním řízení označit. Jedná se, jak již samotný název napovídá, o otázku rychlosti trestního řízení. Tento pojem se stále častěji vyskytuje v záznamech o prověrce spisu ze strany státních zástupců a to zejména v oblasti počítačové kriminality. Nutno uvést, že ne vždy oprávněně.

Již v Listině základních práv a svobod a také v Úmluvě o ochraně lidských práv a svobod je uvedeno, že základem každého demokratického státu je právo na spravedlivý proces. Tedy na proces, který splňuje všechna zákonná ustanovení, pravidla a kritéria. Jedním z takových kritérií je i projednání věci v přiměřené lhůtě. Rychlost trestního řízení se pak projevuje i v hodnocení kvality a efektivity práce policejního orgánu a dalších orgánů činných v trestním řízení a tato rychlost bývá ze strany veřejnosti nejčastěji kritizována.

Zákon vymezuje pro postup orgánů činných v trestním řízení určité lhůty, které je nutno dodržet, avšak tyto lhůty lze v odůvodněných případech prodlužovat. Délka trestního řízení se posuzuje vždy dle konkrétní věci a povahy případu.

Policisté, kteří vedou trestní řízení, jsou posuzováni podle jejich aktivity a správnosti svých postupů. Mnohdy musejí čelit kritice jak ze strany dozorujících státních zástupců, tak i poškozené strany a musejí si přiměřeně zdůvodnit a obhájit svůj postup a vyvrátit tak domněnku o jejich neaktivitě či špatných postupech.

Proto důležitým cílem této práce tedy je, navrhnout takové opatření, které by vedlo k podstatnému zkrácení doby trestního řízení, a zásadním způsobem usnadnilo orgánům činným v trestním řízení jejich úkoly, které jsou s prověřováním a vyšetřováním spojené. Toto opatření navrhované jako „De Lege Ferenda“ by mělo být zapracovatelné do legislativních norem České republiky.

Dalším, cílem, který by měl být touto prací dosažen je provedení výzkumu v oblasti znalostí a schopností policistů v České republice správně přijímat a efektivně a rychle řešit a vyšetřovat trestné činy v oblasti počítačové kriminality. Tento výzkum bude realizován

deduktivní metodou provedenou formou dotazníkového šetření. V návaznosti na tento výzkum si pak práce klade za cíl navrhnout opatření, které by tento zjištěný stav, v případě ověření pracovních hypotéz, řešilo a to zejména návrhem metod zvyšování vědomostní báze policistů v oboru počítačové kriminality, s jejími jednotlivými druhy, s některými základními pojmy z této oblasti.

Dalším cílem této práce je provést analýzu současného stavu preventivních opatření v oblasti počítačové kriminality a případně se pokusit zlepšit stávající, či definovat nová opatření, která by vedla ke zvýšení a zlepšení preventivních opatření.

I. TEORETICKÁ ČÁST

1 VYMEZENÍ POJMŮ

V této kapitole jsou vymezeny, vysvětleny a definovány základní pojmy z výpočetní a informační terminologie. Bez přesného vymezení těchto pojmů by mohly být některé pasáže této práce nepřesné a to by vedlo k nesprávné situovanosti do oblasti počítačové kriminality, kde se tyto pojmy běžně užívají a znalost jejich významu je nezbytná pro správný postup při následném prověřování a vyšetřování kybernetické trestné činnosti.

1.1 Fenomenologie

Spam – Nevyžádaná pošta. V tomto případě se nejedná až tak úplně o kriminální činnost. Do e-mailové schránky přichází i pošta, většinou reklamní.

Crack – prolomení ochrany. Většinou používáno u programů, které jsou placené a chráněné nějakým druhem ochrany.

Sniff – „čmuchání“. Jedná se o proces, při kterém se sleduje provoz dat na síti, odchytávají se pakety a ty se pak shromažďují a jejich filtrací může správný sniffer získat informace jako jsou například uživatelské jméno a heslo

Hacking – postup obcházení a překonávání bezpečnostních překážek nějakého počítačového systému, za účelem získání nelegálního přístupu k tomuto systému.

Phishing – někdy též česky překládáno jako rybaření. Spočívá právě na principu rybaření, kdy útočník rozešle hromadně e-mailové zprávy na pokud možno co nejvíce e-mailových schránek s podvrženou zprávou, ve které požaduje zaslání citlivých informací (nejlepším příkladem je Česká spořitelna, kdy útočník vydávající se právě za ČS rozeslal e-mailové zprávy s požadavkem na potvrzení uživatelského jména a hesla)

Počítačové viry – počítačové programy, které jsou schopny replikovat sama sebe a způsobovat v počítači, případně počítačovém systému nějaké škody. Jsou schopny se šířit i po počítačové síti z počítače nebo systému do dalšího PC nebo systému.

Krádež identity – jednání, kdy útočník si zjistí informace o své oběti a za tuto se pak vydává.

Cyberstalking – používání internetu (a v současné době i mobilních telefonů) k pronásledování a sledování oběti útočníkem (nečastění zhrzený milenec)

DOS – Denial-of-service – znepřístupnění služby – útok na server, většinou internetové stránky, za účelem způsobení jejich nedostupnosti. Provádí se velmi rychlým opakovaným dotazem na takové stránky, většinou z více počítačů naráz, čímž dojde k zahlcení serveru, který nestíhá odpovídat.

Hacker – člověk, který dokáže svými znalostmi prolomit počítačovou ochranu systému

Cracker – dokáže díky svým znalostem odstranit ochranu programu tak, aby jej mohl používat kdokoli, aniž by si jej musel koupit.

Uživatelské jméno – přezdívka, skutečné jméno nebo nějaké slovo, které uživatel – člověk – používá k přihlašování se do nějakého zabezpečeného i nezabezpečeného systému, kdy tímto slovem je pak označován.

Heslo – slovo, sousloví, množina čísel, písmen a speciálních znaků, která se používají k přihlášení se do zabezpečeného systému. Heslo se nikde nezobrazuje, ani není nikde v databázi uloženo ve svém nezakódovaném tvaru. Většinou se ukládá v šifrované podobě a to pouze jako HASH hesla.

HASH – transformační funkce, do které vstupuje heslo – řetězec písmen, číslic, speciálních znaků v určitém pořadí, a libovolné délky, a vystupuje z ní řetězec znaků o určité konkrétní délce. Jedná se o jednosměrnou silně bezkolizní funkci, což znamená, že HASH výsledku nelze zpětně zjistit nějakým výpočtem, zdrojový text, a ani není možno najít jakýkoli jiný text, který by po vypočítání HASH vydal stejný výsledek, jakým je HASH jiného textu.

Sociální inženýrství – to pojem, který pod sebe shrnuje nejrůznější metody, které využívají a zneužívají lidský faktor (lidskou neznalost a hloupost, či jen pomalejší úsudek) pro spáchání počítačové kriminality

1.2 Technické pojmy

Router (Směrovač) – síťové zařízení, které přeposílá data (datagramy) k jejich cíli.

Server – označení počítače, který v síti poskytuje nějaké speciální služby (www stránky, databáze, úložný prostor atd.) Nemusí se vždy jednat pouze o počítač. Funkci serveru může vykonávat i samotný program v počítači (např. Apach – pro web)

Access point (přístupový bod) – zařízení, které je součástí bezdrátové sítě, které umožňuje připojení dalších počítačů a jiných zařízení k síti bezdrátově.

NAT – jedna z funkcí routeru v síti, (Network Address Translation), která mění IP adresy paketů, které jím procházejí na jiné. Nejčastější použití je v síti, kdy router má svou veřejnou IP adresu a pomocí funkce NAT 1:1 směřuje data do příslušných počítačů tak, že vnější (veřejné) IP adresy odpovídají vnitřním IP adresám (např.: 74.68.152.1 = 192.168.1.45). NAT 1:N je taková funkce, která z jedné veřejné IP adresy směřuje data do vnitřní sítě a podle portů přiděluje této veřejné IP adrese IP adresu vnitřní sítě. (Např.: 74.79.54.142:534 = 192.168.1.4, 74.79.54.142:534 = 192.168.1.5 … atd.)

IP adresa – číslo, které jednoznačně určuje (identifikuje) síťové zařízení (rozhraní) v počítačové síti. V dnešní době jsou již dvě verze IPv4 (př.: 192.168.1.1) a IPv6 (př.: 2002:791:1b01:18:220:33ee:Bed9:bb5)

Gate (Brána) – zařízení, sloužící jako uzel v počítačové síti, který spojuje jednu síť s druhou, kdy na každé síti je jiný protokol. Funguje podobně jako router, respektive musí umět plnit jeho funkci. (Příklad brány: GSM brána, SMS brána, VoIP brána… atd.)

Hlavička e-mailové adresy – část e-mailové zprávy, která se běžně uživatelům nezobrazuje, ale která obsahuje poměrně důležité informace pro e-mailové klienty – programy ve kterých se zprávy zobrazují a e-mailové servery – servery, přes které takové zprávy procházejí. E-mailová hlavička obsahuje kromě dalších, informace odkud byla odeslána, zda byla zkontrolována nějakým antivirem, přes který e-mailový server prošla, komu je určena a hlavně z jaké IP adresy byla odeslána. Díky takové informaci lze zjistit z přijaté e-mailové zprávy, z jakého počítače byla odeslána.

Anonymizační síť – počítačová síť na internetu, kterou tvoří velké množství počítačů dobrovolníků, kteří se do této sítě vědomě připojili, kdy na svém počítači spustí program,

který čeká, až bude ze sítě osloven jiným, stejně fungujícím počítačem a pak přes svou IP adresu přepošle data, která předtím přijal. Tak se může stát, že pokud někdo použije takovou anonymizační síť například k odeslání e-mailové zprávy, v hlavičce najdeme IP adresu například z Jižní Ameriky nebo Thajska. Nejznámější je např.: TOR, I2P a podobně.

Peer-to-peer – takto se označuje speciální druh počítačové sítě, která slouží zejména pro výměnu dat mezi jednotlivými počítači. Počítač A se dotáže serveru na určitý soubor (film, zvuk, text apod.) Server najde počítač B, který uvedený soubor má uložen na HDD a sdělí počítači A adresu počítače B. Ten pak kontaktuje počítač A s požadavkem na odeslání předmětného souboru a tak dojde k přenosu.

LAN (lokální bezdrátová síť) – používá se pouze v domácnostech, malých společnostech. Jedná se o malou soukromou síť, která k internetu připojena vůbec není, nebo je k internetu připojena přes zabezpečený router nebo bránu.

Wi-Fi připojení – jakýsi standard pro LAN, který vychází ze specifikace IEEE 802.11, jednoduše řečeno se tak označuje bezdrátové připojení počítačů k síti.

1.3 Počítačová kriminalita

O fenoménu počítačové kriminality již bylo napsáno poměrně mnoho knih, publikací a odborných článků a to z toho důvodu, že se tato oblast kriminality poměrně rychlým tempem rozvíjí a zasahuje již nejen do velkých společností, ale i do domovů obyčejných lidí.

Pojem počítačová kriminalita byl asi poprvé definován a vymezen v práci V. Sokola a T. Vlčka – Počítačové právo z roku 1995. Nejstručnější je asi definice:

„*Počítačová kriminalita je jakýkoli čin směřující k narušení nebo zneužití počítače, nebo počítačového systému a informací v něm obsažených*“ (Jirovský 2007, s. 91)

V minulosti nebyla tato problematika příliš sledována a mnoho se o ní nehovořilo, neboť jen malá komunita byla schopna ji pochopit a reagovat na ni.

U Policie České republiky bylo ještě v nedávné minulosti velmi nízké povědomí o této specialitě kriminality. Pokud se v minulosti s počítačovou kriminalitou, nebo „kybernetickou kriminalitou“ (Cyber Crime), jak se o ní hovoří v zahraničních pramenech, některý z vyšetřovatelů setkal, nedokázal ji vůbec rozpoznat a už vůbec ani netušil, jak takový druh kriminality vyšetřovat. Později, s masivním rozšířením osobních počítačů i mezi laickou veřejnost, začala stoupat i počítačová gramotnost obyvatelstva a tím samozřejmě i státních složek. Ty si jen pomalu začaly uvědomovat vznik nového druhu kriminality a postupně, i když velice nepružně, začaly chápat, že se bude třeba s tímto novým fenoménem vypořádat. Policie a soudy zprvu počítačovou kriminality řešily a vyšetřovaly stejně jako obecnou kriminalitu. Vzhledem k absenci základních ustanovení trestního zákona nebylo možno posoudit kriminalitu jako počítačovou, ale bylo na ni třeba aplikovat jiná ustanovení trestního zákona, které jednání spáchané prostřednictvím počítače, či internetu alespoň analogicky vystihovalo. Například Šíření dětské pornografie a její výroba se vyšetřovala a posuzovala jako Týrání svěřené osoby, Pohlavní zneužívání, nebo Ohrožování mravní výchovy dítěte.

Teprve s příchodem novely Trestního zákoníku č. 40/2009 Sb. bylo do právního systému České republiky zavedeno i několik skutkových podstat, které přímo tento druh kriminality specifikují. Nový zákoník vychází, co se pojmů týče, z Úmluvy o počítačové kriminalitě, schválené Výborem ministrů Rady Evropy dne 8. 11. 2001, kterou Česká republika podepsala v roce 2005. Ta obsahuje soupis kriminálních jednání, která by měly smluvní strany, v rámci svých zákonů a svého práva postihovat. Jde zejména o:

- Zásah do počítačového systému
- Podvod související s počítači
- Trestné činy, které se týkají a souvisejí s dětskou pornografií
- Trestné činy v oblasti porušování autorského práva
- Falšování údajů ve spojitosti s počítači
- Zásah do dat (na nosiči informací, v počítači)
- Protiprávní přístup do počítače, či počítačového systému

- Protiprávní zachycení informací
- Zneužití zařízení

Díky tomu se ČR dočkala takových skutkových podstat, jako jsou §230 – Neoprávněný přístup k počítačovému systému a nosiči informací, §231 – Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, dále byly upraveny a doplněny i některé stávající skutkové podstaty, jako například §180 – Porušení tajemství dopravovaných zpráv, kterou upravuje právě uvedený §230 v prvním odstavci, nebo §192 – Výroba a jiné nakládání s dětskou pornografií, kde v prvých dvou odstavcích je již zmíněno i dílo počítačové a elektronické, stejné jako šíření elektronickou a počítačovou sítí.

Obdobných inovací se dočkaly i jiné právní normy, např. zákon Autorský, který stanovuje co je to Sdělování díla veřejnosti, kdy v tomto ustanovení se již hovoří i o počítačové síti a elektronické podobě díla.

S nástupem uvedených legislativních inovací, si začala policie osvojovat nové postupy prověřování a vyšetřování, a zejména zajišťování stop v této oblasti. S rychlým rozvojem techniky pak vznikla potřeba řešit tuto činnost stále častěji, a to i na základních útvarech policie, které disponují jen velmi malým procentem odborníků, nebo policistů znalých funkce a principů počítačových sítí. Mnozí policisté v současné době nemají základní znalosti nutné ke správnému přijetí trestního oznámení od oběti tohoto druhu kriminality.

1.4 Trestný čin

Trestný čin se z kriminologického hlediska ztotožňuje s definicí trestného činu z hlediska trestněprávního. Existuje však i sociálně-kriminologické hledisko, které trestný čin definuje jako čin, který je společensky škodlivý, asociální, nebo jednání, které má určitý patologicko-kriminální charakter a porušuje zásadním způsobem pravidla a zájmy chráněné společností.

Podle trestního řádu je trestným činem: „*protiprávní čin, který trestní zákon označuje za trestný a který vykazuje znaky uvedené v takovém zákoně*[1]“. Souhrn takových znaků se nazývá skutková podstata trestného činu. Je to souhrn objektivních a subjektivních znaků, který určuje jednotlivé druhy trestných činů, a odlišuje je od sebe navzájem. Skutková podstata je vlastně odrazem skutku a je charakterizována čtyřmi skupinami znaků:

- **objekt** – okruh společenských vztahů, případně zájmů, které jsou takovým činem dotčeny, a na jejichž ochraně má společnost zájem,
- **objektivní stránka** – určení způsobu, jakým byl trestný čin spáchán a jeho následků. Zahrnuje v sobě jak obligatorní (povinné) znaky, jako jsou jednání, následek a příčinný vztah mezi nimi, tak i znaky fakultativní (nepovinné) jako je doba, po kterou byl čin páchán, čas a místo spáchání,
- **subjekt** – osoba fyzická, jenž je v době spáchání činu starší 15-ti let a je příčetná. U některých skutkových podstat je vyžadována speciální vlastnost, způsobilost, či postavení (policista, veřejný činitel atd.) subjektu. Zde se pak hovoří o takzvaném subjektu speciálním.
- **subjektivní stránka** – vnitřní psychický vztah pachatele ke spáchanému skutku. Jedná se o takzvané zavinění. Toto může být buď nedbalostní, nebo úmyslné.

Trestní odpovědnost pachatele a s ní spojené trestněprávní důsledky, je pak možno uplatňovat pouze v případech, které jsou škodlivé pro společnost, a ve kterých nepostačuje uplatnění odpovědnosti podle jiného právního předpisu.

[1] Ust. §13 trestního zákoníku

1.5 Pachatel z pohledu kriminologie

Pojem pachatel se z kriminologického hlediska neomezuje jen na osobu, která se dopustila trestného činu, který je definován v zákoně, ale chápe pod tímto pojmem i osoby, které by pachatelem trestného činu být mohly, avšak z důvodu nedostatku věku, případně duševní poruchy nejsou za své činy trestně odpovědny. Pod označení pachatel patří i skupiny, případně jednotlivci, jejichž chování je sociálně patologické.[2] Psychologické poznatky o takových pachatelích jsou využívány i v jiných oblastech než je trestní právo. Využívají se zejména v kriminalistice, penologii, anebo soudní psychiatrii a podobně.

Osobnost pachatele je pak z pohledu kriminologie chápána jako organický celek života člověka vztažený k podmínkám společenského života takové osoby.

Původně se pachatelé dělili pouze podle toho, zda spáchali nějaký kriminální čin. Později však bylo přistoupeno k zohlednění i dalších různých faktorů, jako například podmínky za jakých došlo ke spáchání kriminálního činu, úloha, nebo role oběti a samozřejmě i vliv ostatních společenských podmínek. Teorie osobnosti pachatele je velmi široká. Při členění jsou aplikovány různé snahy o rozčlenění takových osob dle souboru znaků, případně kritérií do skupin, které se následně blíže charakterizují, nejčastěji podle následujících kritérií:

- Sociologická charakteristika
- Biologická charakteristika
- Psychologická charakteristika

Do biologické charakteristiky je možno zařadit, krom jiného zejména genetickou výbavu jedince, neboť v ní jsou zakódovány a vlastnosti jako je vzhled, dispozice k nemocem a podobně.

Do sociální a psychologické charakteristiky patří zejména různé faktory a to jak sociální, tak i faktory prostředí, ve kterém se jedinec vyvíjí a ve kterém žije. Tyto pak

[2] Jedná se zejména o prostitutky, drogově závislé osoby, extrémistické skupiny a jednotlivce, alkoholiky nebo gamblery

ovlivňují změny v chování jedince. Velmi výrazným a důležitými faktory v současné době jsou i informovanost jedince a jeho vzdělanost.

Takové rozdělení pachatelů je však pouze vědecké. V reálném světě je vliv na jedince, který se stává pachatelem kriminálního činu, ovlivněn kombinací všech výše uvedených faktorů.

Speciálním typem pachatele je pak z kriminologického hlediska pachatel – recidivista. Z pohledu kriminologie je recidivistou jedinec, který se dopustil kriminálního jednání a po jeho spáchání se jej dopustil znovu, bez ohledu na to, zda za tento čin byl odsouzen. Z pohledu trestně – právního je recidivistou jedinec, který spáchal trestný čin dle definice v zákoně a za tento čin byl pravomocně odsouzen a dopustí se jej opakovaně. Z pohledu penologického se jedná o pachatele, který již za spáchání trestného činu byl nejméně dvakrát odsouzen k výkonu trestu odnětí svobody.

Z kriminalistického (trestně-právního) hlediska je pachatel trestného činu definován v ust. §22 jako: „*ten, kdo svým jednáním naplnil znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, je-li trestná*[3].“

Typologie pachatele počítačové kriminality

Osobou pachatele počítačové kriminality, dle výše uvedeného, může být:

- **běžný uživatel** - umí používat alespoň základní funkce některých počítačových aplikací,
- **pokročilý uživatel** - má alespoň základní povědomí o funkci počítače a funkci počítačové sítě, zná a umí používat větší množství počítačových aplikací
- **zkušený uživatel** - je dobře obeznámen se základními i pokročilejšími funkcemi v oboru IT, má pokročilejší znalosti o principech fungování počítačových systémů a sítí a tyto dokáže patřičně využít, a používá základní principy sociálního inženýrství

[3] Ust. §22 trestního zákoníku

- **odborník v oboru IP** - pachatel sofistikované počítačové kriminality - je většinou nadprůměrně intelektuálně vybavený jedinec s velmi kreativním myšlením, který může být zaměstnaný v oblasti IT, má téměř neomezený přístup k informacím prostřednictvím internetu.

S narůstajícím trendem vybavení běžných domácností osobními počítači připojenými k internetu se pachateli stávají i mladí lidé – vysokoškoláci, nezřídka středoškoláci, ale i studenti základních škol, kteří díky velmi rozšířenému přístupu k internetu a tím k téměř všem informacím jsou mnohdy počítačově gramotnější, než současná průměrná dospělá generace.

Dlouholetých zkušenosti s vyšetřováním tohoto druhu kriminality naznačují, že podněty, které vedou takové pachatele k páchání trestné činnosti v oblasti internetu a počítačů, jsou ovlivněny zejména věkem pachatele.

- **Nejmladší pachatelé** se dopustí takové trestné činnosti proto, že zkoumají nové možnosti, které se před nimi ve světě IT otevírají. Vzhledem k velmi snadné dostupnosti různých nástrojů, umístěných na běžně přístupných webových stránkách, které se specializují na tvorbu viru pouhou variabilitou nastavení jeho vlastností a následných činností (payload), kdy vir je pak automaticky vytvořen, je to pro takové mladé pachatele většinou jen zábava udělat někomu něco naschvál. Tito pachatelé, vzhledem ke svému duševnímu vývoji, ještě plně nechápou důsledky své činnosti. Nemají dosud utvořený pevný žebříček hodnot, a proto celé své jednání považují pouze za neškodnou zábavu. Nedospělý jedinec ve vývojovém stádiu dítěte je většinou tím nejzákeřnějším a nejbrutálnějším pachatelem.

  Je znám případ, kdy dítě – žák základní školy – pomocí webové aplikace vytvořilo virus tak dokonalý, že nejlepším odborníkům trvalo velmi dlouho, než se jim podařilo jej dešifrovat a odstranit.

- **Mladí pachatelé** - navštěvující střední školy. Jejich pohnutka k páchání této trestné činnosti je vidina legrace z toho, co způsobí své oběti, ale na rozdíl od svých mladších „kolegů“ jsou lákáni i možností získat svým jednáním nějaký prospěch. Např. získání správných odpovědí na test z učitelova počítače, nebo naopak smazání špatných výsledků a podobně. Tito lidé již začínají chápat, jaké by jejich

jednání mohlo mít důsledky, ale vzhledem k stádiu dospívání si tyto následky nechtějí připustit a uvědomí si je až je většinou pozdě. Z jejich řad se nejčastěji rekrutují pachatelé kyberšikany[4]. Pomocí sociálních sítí šíří o svých obětech nepravdy, nebo nějaká citlivá data ve snaze svou oběť zdiskreditovat a tím si z ní udělat legraci, aby tak získali ve svém okolí uznání. Nutno dodat, že oběti takového druhu kriminality, pokud jejich okolí včas nezasáhne, končí většinou s velkými psychologickými problémy, nebo i sebevraždou.

Příklad.: StarWars Kid[5]- Mladík z USA natočil ve školním studiu video, na kterém předváděl pohyby z bojového umění s tyčí. Toto video si natočil pro sebe, aby si vyzkoušel, jak se zachází s nastavením přístrojů ve studiu. Jeho spolužáci se ale k videu dostali a umístili je na YouTube. Během několika málo dní se toto video stalo nejsledovanějším a mladík, díky své obézní postavě, předvádějící bojové umění se stal terčem posměchu téměř celého světa. Vznikaly k tomuto videu i různé předělávky, kdy mu místo dřevěné tyče byly digitálně vytvořeny laserové meče z trilogie StarWars. Mladík se psychicky zhroutil a pokusil se i o sebevraždu.

Dalším faktorem, který podněcuje mladé lidi k páchání počítačové kriminality, je neúspěšnost takového jedince v okolí svého reálného světa. Takový jedinec se pak snaží být úspěšný alespoň ve virtuálním světě, tedy na různých sociálních sítích. Tím se dostáváme opět většinou ke kyberšikaně. Fyzicky slabý jedinec, který se nedokáže ubránit silnějšímu, o něm vytvoří nějaký hanlivý, posměšný dokument, který pak rozšíří s patřičným komentářem na internetu a tím jej ve virtuálním světě porazí, což se pak promítne i do světa reálného.

- **Pachatelé středního věku** – vysokoškoláci, páchají počítačovou trestnou činnost, aby předvedli svému okolí, jak brilantně zvládají počítačovou techniku. Toto je ovlivněno zejména filmy z Hollywoodské produkce, kde všichni hackeři a jim podobní lidé jsou glorifikováni jako lidé s neomezenými možnostmi a jako „borci“. Tito pachatelé jsou ještě částečně ovlivněni faktory mladších kolegů, ale vzhledem

[4] O tomto problému velice dobře pojednává článek: http://www.lupa.cz/clanky/kde-konci-legrace-a-zacina-kybersikana/
[5] Případ podrobně popsán i na: http://cs.wikipedia.org/wiki/Kyberšikana

k jejich ustalujícímu se žebříčku hodnot, začínají své jednání více přizpůsobovat uspokojení svých potřeb, nejčastěji získávání jinak drahých počítačových her, filmů, hudby a programů. V této skupině lidí dochází k nejčastějšímu neoprávněnému šíření filmů a her a programů – tedy porušování autorských práv. Někteří jedinci z této kategorie začínají svou činnost zaměřovat na získání nejlépe finančních prostředků, aby si tak přilepšili na svých studiích, ale nejen tam. Ti nejzkušenější pak po dokončení studia, pokud jej vůbec dokončí, si začínají vydělávat právě tímto druhem činnosti, tedy pácháním trestné činnosti v oblasti kriminality.

Příklad: Student jedné nejmenované VŠ během svých studií získal znalosti v oblasti IT a zaměřil se na průzkum virů, červů a mallware. Díky jeho neutuchajícímu zájmu a přísunu informací nabyl takových vědomostí, že vytvořil počítačového červa, který nijak svou činností nenarušoval běh žádného počítačového systému a pouze se šířil z počítače do počítače. Tento červ měl v sobě zaimplementovánu funkci, aby se jednou za čas podíval na určité místo na internetu, kde měl povely pro svou činnost. Poté nějaké době šíření těchto červů mladík spustil DOS útok na server jedné nejmenované velké společnosti, které na serveru běžel internetový obchod a servis a server na několik dní zablokoval. Společnost přišla o zisky ve výši několika milionů dolarů. Tímto mladík ukázal celému světu, co dokáže, kdy samozřejmě se k tomuto útoku přihlásil pouze v uzavřeném prostředí hackerů, kde nabídl svou síť na prodej. Vydělal na ní velké jmění.

Zde výčet kategorií pachatelů dle věku končí. Ostatní pachatelé starší se již zaměřují na získávání finančních prostředků. Specialitou v počítačové kriminalitě je průmyslová špionáž, nebo mezinárodní špionáž. V této oblasti působí většinou jen špičkoví odborníci v oboru, kteří svou činnost provádějí zejména v utajení. Nezanechávají po sobě téměř žádné stopy. Nezřídka se rekrutují z řad hackerů.

Hackeři tvoří speciální skupinu pachatelů počítačové kriminality. Lze je kategorizovat dle následujících kritérií:

- **Wannabes** – takto jsou označováni především začínající hackeři, kteří se teprve učí a zkoušejí si testovat získané znalosti a postupy jiných zkušenějších. Leckdy jsou to lidé, kteří nemají žádné znalosti v tomto oboru a jen testují postupy, které nalezli na internetu.

- **White hats** – to jsou odborníci, kteří provádějí své útoky za účelem zjištění slabin systému, sítě nebo nějaké síťové služby a to s vědomím, anebo přímo na objednávku nějaké společnosti, která chce zjistit tzv.:"díry" – slabá místa ochrany svých systémů, případně svých produktů.

- **Black hats** – tito hackeři zaměřují své útoky na již běžící a fungující síťové služby a systémy, a to za účelem získání nějakého prospěchu. Ať již finančního, či jiného (např. získání určitého software, chráněného proti bezplatnému užívání). Proto se této skupině hackerů někdy říká Crackeři.

- **Grey hats** – poslední skupina hackerů. Tito lidé nejsou nijak vyhranění. Pohybují se na hranici mezi White hats a Black hats, jak již název naznačuje. Jedná se o lidi, kteří se mohli dopustit nějakého trestného činu svým útokem na nějaký chráněný systém a po svém dopadení přešli na „druhou" stranu a stali se kupříkladu právě testovacími techniky pro ověřování funkčnosti systémů. Nebo opačně se může jednat o odborníky, kteří pracují na legální bázi a poté, co si plně uvědomí své možnosti a vyskytne se před nimi příležitost, spáchají díky svým schopnostem trestný čin.

Další specialitou počítačové trestné činnosti je kyberstalking. Stalking je činnost, kterou páchají většinou zhrzení milenci a to ať muži, tak i ženy. Právní normy České republiky jej definují jako Nebezpečné pronásledování[6]. Po rozchodu neustále sledují svého bývalého partnera, obtěžují jej zasíláním e-mailů nebo SMS zpráv, patří k tomu i neustálé prozvánění telefonu a i fyzické sledování. Kyberstalking je speciální druh stalkingu, kdy dochází k zasílání nevhodných e-mailových zpráv, a nejen e-mailových, ale i SMS, nebo prostřednictvím sociálních sítí, Facebook, MySpace, Badoo, Yono a dalších, ale samozřejmě i pomocí různých IM komunikačních prostředků jako jsou např. ICQ, Skype, MSN Messenger atd. Zasílané zprávy mají různé povahy a to jak prosící, kdy odvržený partner neúměrně dlouho a neúměrným způsobem žádá a prosí o obnovení vztahu. Pak

[6] Ust. §354 trestního zákoníku

takové jednání může přejít do zpráv výhrůžné povahy, nejprve jen výhrůžkami vlastního sebepoškození v případě neobnovení vztahu, které později přecházejí do fáze již nebezpečných výhrůžných zpráv, které svou povahou dokážou v oběti – adresátovi - vzbudit důvodnou obavu o svůj život.

Do této oblasti počítačové kriminality patří i sledování provozu na počítači. Například jeden z páru je přespříliš žárlivý a tak nainstaluje do počítače, který používá jeho protějšek program, který není nijak viditelný, ani zjistitelný, který má za činnost to, že v pravidelných intervalech snímá obrazovku počítače a stav stisknutých kláves, které zaznamenává a následně odesílá do jiného počítače tomu partnerovi, který tento program nainstaloval a ten tak sleduje vše, co jeho protějšek na počítači dělá. Takovým programem je např.: SPY007.

1.6 Oběť počítačové kriminality - typologie

Pojem oběť trestného činu, tak, jak je chápan z pohledu viktimologie, definují ve svém článku PhDr. Alena Marešová a PhDr. Milada Martinková takto: „*Oběť je zpravidla chápána, jako konkrétní fyzická osoba, která byla trestným činem usmrcena, nebo zraněna, nebo ohrožena na životě a zdraví, nebo jí byla způsobena škoda na majetku nebo škoda morální, byla omezena na svobodě nebo jiných právech, a to nezávisle na tom, zda jí bylo následně zvláštním procesním rozhodnutím přiznáno poškození poškozeného.*“ (Marešová 2009, s. 1)

Analogicky tedy obětí trestného činu z oblasti počítačové kriminality může být prakticky kterákoli osoba, která používá k některé ze svých činností počítač připojený k internetu a je jí způsobena škoda na majetku či morální, byla omezena na svobodě nebo jiných právech a to prostřednictvím počítače a internetu. Obětí počítačové kriminality může být však i právnická osoba a dokonce i stát.

Oběť z pohledu Viktimologie (vědy o obětech) je chápána pouze jako fyzická osoba, která je potenciální obětí pachatele (viktimnost), stane se obětí pachatele (proces viktimizace) a následně se stane obětí nevhodného chování svého okolí (sekundární viktimizace).

Oběti lze z viktimologického hlediska kategorizovat na dvě základní skupiny.

- Oběti, které si samy svým jednáním a chováním zapříčinili, že se obětí staly (ať tím, že patří do slabé sociální skupiny – bezdomovci, prostitutky, drogově závislí atd., nebo tím, že například chodí vyzývavě oblečeni, vystavují na odiv svůj velký majetek a podobně)

- Oběti, které si svým chováním a jednáním nezavinily, že se obětí staly. (například tím, že patří k určité pozitivně vnímané a hodnocené skupině jako je policie, hasiči, společensky a kulturně známé osobnosti a podobně)

V oblasti počítačové kriminality je pak možno oběti dělit následovně:

- Častými obětmi, jsou zejména lidé, kteří nejsou, nebo jsou jen málo počítačově gramotní a nemají povědomí o procesních úkonech, právních předpisech a normách anebo postupech firem. Nejčastější trestná činnost je v tomto případě Phishing, případně podvod.

  Příklad: Nejmarkantnějším příkladem z poslední doby je takzvaný „Policejní virus“. Je to jednoduchý vir, který se do uživatelova počítače dostane prostřednictvím různých internetových stránek. Z počátku byl umístěn především na erotických a porno stránkách. Po infikování počítače se vir spustí a v okně internetového prohlížeče zobrazí text a obrázek, které společně uvádějí poškozeného – uživatele napadeného PC – v omyl tím, že mu tvrdí, že Policie ČR spolu s ústavem autorského práva zablokovala jeho počítač z důvodu používání nelegálního software. Dále jej informuje, že pro další používání počítače je nutné jej odblokovat, což je možno provést tím, že poškozený zašle na účet provozovaný společností UCash, částku 2000,- Kč a pak mu přijde na jeho e-mail kód, pomocí kterého tento počítač odblokuje.

  Výše popsaná oběť se pak domnívá, že policie je oprávněna takovýmto způsobem narušovat soukromí občanů a blokovat celý jejich počítač, a proto zaplatí požadovaný poplatek.

- Do další kategorie obětí patří osoby, které díky svému zaměstnání, či pozici ve firmě přicházejí do styku s cennými, někdy i citlivými údaji, daty a informacemi.

Mohou to být zejména správci sítí ve firmách, manažeři a sekretářky a podobně. Související trestná činnost v tomto případě je Phishing a Pharming.

- Obětí se nově může stát i právnická osoba. Zejména se to týká velkých průmyslových společností, kdy cílem útočníka – pachatele – je získat utajované výrobní postupy (průmyslová špionáž), nebo naopak zničit některá důležitá data, případně databáze (konkurenční boj)

- Poměrně častými obětmi jsou osoby, které o sobě na sociálních sítích (FaceBook, Twitter, Badoo, ICQ, www.lide.cz a dalších) uvedou veškeré osobní údaje a informace, bez rozmyslu popisují každou věc, kterou právě dělají a sdělují veřejně, kde se právě nacházejí, neboť ze svého chování nedokáží, vzhledem k nedostatečným zkušenostem a vědomostem, vyvodit možné následky. Tito se stávají nejčastěji obětmi krádeží identity a kybernetické šikany, jak je popisována výše. Největší množinu této skupiny tvoří děti.

- Samostatnou skupinu obětí pak tvoří osoby, které jsou prostřednictvím počítačů a internetu pronásledovány zhrzenými partnery po rozchodu, případně děti, pronásledované neznámým deviantem (kyberstalking).

- Majoritní podíl však v České republice tvoří oběti podvodu spáchaného prostřednictvím internetu. Takové oběti, ve snaze nakoupit co možná nejlevněji, se pak nechávají zlákat podvodnými inzeráty nabízejícími drahé předměty za nápadně nízkou cenu, kdy po zaplacení předem požadovaný předmět neobdrží.

2 ODHALOVÁNÍ A KONTROLA POČÍTAČOVÉ KRIMINALITY

Zatímco odhalováním počítačové kriminality se v současné době již orgány činné v trestním řízení a k nim přidružené státní orgány zabývají, na kontrolu počítačové kriminality nejsou dostupné prostředky a síly. Tato činnost je tak odsouvána na okraj zájmu státních orgánů.

Podle některých názorů vedení policie je důležité, aby bylo prováděno zejména objasňování a odhalování pachatelů již spáchané trestné činnosti. Podle jiných názorů je kontrola počítačové kriminality mimo zájem policie a orgánů činných v trestním řízení, neboť se jedná zejména o orgány represivní. Kontrolou počítačové kriminality by se dle tohoto názoru měla zabývat preventivní, či preventivně-kontrolní složka státního aparátu.

Vzhledem k současné finanční situaci státu, jsou necitlivě snižovány stavy státních složek, které se touto problematikou zabývají, neboť na jejich provoz a činnost není dostatek prostředků. To je dáno zejména tím, že množství spáchaných trestných činů, které je nutno objasnit je vysoké a proto byly téměř veškeré prostředky a síly přesunuty do této oblasti činnosti. V současné době u policie existuje pouze jedno oddělení, které se zabývá kontrolou a vyhledáváním počítačové trestné činnosti. Toto oddělení spadá pod policejní prezidium.

Samostatné oddělení, které se zabývá pouze objasňováním počítačové kriminality, vzniklo díky nezměrnému úsilí některých policistů, na Krajském ředitelství policie Jihomoravského kraje. Zde působí odborníci v oboru počítačových technologií. Toto oddělení se stalo vzorem i pro Zlínský kraj, kde takové oddělení také vzniklo, ale právě v důsledku zmíněných finančních problémů se celé oddělení skládá z jednoho pracovníka.

S nárůstem počítačů v domácnostech a velmi výrazným nárůstem počítačové gramotnosti obyvatelstva však dochází i poměrně rychlému nárůstu počítačové kriminality. Z tohoto důvodu se budou muset vedoucí složky policie začít zabývat otázkou zvýšení počtu takových speciálních oddělení.

Kontrolou a prevencí v oblasti počítačové kriminality se tedy začaly, v negativní reakci státních složek na tuto problematiku, zabývat nově vzniklá občanská sdružení, o nichž je pojednáváno v kapitole 5.

3 VYŠETŘOVACÍ POSTUPY

3.1 Trestní řízení

Trestní řád[7] upravuje proces trestního řízení. Stanovuje podmínky, za kterých lze trestní řízení provádět. Určuje postupy, jakými se pro účely trestního řízení zajišťují důkazy, a vyjmenovává prostředky, kterými lze důkazy důležité pro trestní řízení opatřit.

Trestní řízení má šest fází.

1) **Zjištění skutečností nasvědčujících tomu, že byl spáchán trestný čin**

   O skutečnosti, že byl spáchán trestný čin, se orgány činné v trestním řízení dozvídají různými způsoby:

- Výsledek vlastní činnosti
- Zprávy podané jinými státními orgány
- Trestní oznámení na známého či neznámého pachatele ze strany občanů či firem

Trestní oznámení je povinen přijmout každý policejní útvar ČR nebo Státní zastupitelství.

2) **Fáze prověřování**

   Orgány činné v trestním řízení (policie pod dohledem státního zástupce) prověřuje oznámené skutečnosti, zda skutečně nasvědčují tomu, že byl spáchán konkrétní trestný čin a zda jej spáchal konkrétní pachatel.

   V této fázi se neprovádějí důkazy. Tyto se pouze vyhledávají a zajišťují. Provádět důkaz v této fázi trestního řízení lze pouze ve výjimečném případě, kdy věc nesnese odkladu (neopakovatelný úkon).

[7] Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád)

3) Fáze vyšetřování

Pokud všechny zjištěné skutečnosti nasvědčují tomu, že trestný čin spáchán byl a že je zjištěno konkrétní osoba pachatele nebo pachatelů, je zahájeno trestní stíhání[8].

Výše zjištěnému pachateli je sděleno, že je trestně stíhán a pro jaký trestný čin. Probíhá vyhledávání důkazů důležitých pro trestní řízení, které jsou důležité pro objasnění všech důležitých skutečností, k osobě pachatele a následků trestného činu.

Po skončení vyšetřování je obviněnému umožněno, aby si prostudoval trestní spis a případně navrhl další provedení důkazů.

4) Podání obžaloby

Jakmile jsou shromážděny důkazy, dostatečně prokazující skutečnosti, které jsou důležité pro posouzení viny a trestu, podá státní zástupce obžalobu.

5) Přezkoumání obžaloby soudem

V této fázi přezkoumá předseda senátu spisový materiál, zda obsahuje všechny skutečnosti a důkazy o nich, a zda lze na jejich základě postavit obviněného před soud.

6) Hlavní líčení

V této fázi, je obžalovaný předvolán před soud, předkládají se důkazy o všech zjištěných skutečnostech, jsou slyšeni svědci, obviněný i poškození. Po provedení všech nezbytných úkonů (závěrečné řeči státního zástupce a obhájce obviněného, posledního slova obviněného) se soud odebere k poradě a po ní vynese rozsudek.

Podle některých právních názorů však touto poslední fází trestní řízení nekončí. Následuje ještě fáze Výkon trestu a následně fáze Zařazení zpět do společnosti.

3.2 Přijetí oznámení

Do první fáze trestního řízení patří i přijetí trestního oznámení. Při přijímání trestního oznámení je třeba si nejprve oznamovatele řádně vyslechnout. Není potřeba ihned sepisovat Protokol o trestním oznámení. Důležité je pochopit, v čem tkví podstata toho, co se nám snaží oznamovatel sdělit, neboť ve většině případů ani sám oznamovatel nezná správné termíny, ale někde je zaslechl, a aby sám nevypadal úplně nevzdělaně, snaží se tyto odposlechnuté výrazy používat, avšak na nesprávných místech a označuje jimi nesprávné skutečnosti. Velice vhodné je, aby policista takovému oznamovateli dal najevo, že ani on neví, o čem je řeč a požádal ho, aby mu celou věc vysvětlil jako pro úplného laika.

Poté nastane čas začít celou výpověď sepisovat a to ať formou Protokolu o trestním oznámení, nebo formou Úředního záznamu o podaném vysvětlení.

Po sepsání oznámení výše uvedeného, je vhodné celou věc řádně prokonzultovat s policisty, kteří se vyšetřováním tohoto druhu kriminality zabývají již delší dobu.[9] Je to důležité zejména z toho důvodu, že každý případ je originální a ne vždy se může zajišťování důkazů a stop řídit stejnými pravidly. Tito zkušení policisté mohou poradit s provedením prvotních úkonů, jako jsou právě zajištění důkazů v elektronické podobě, zabránění smazání podstatných elektronických stop a jejich následné uchování a zadokumentování pro následné trestní řízení.

[8] §160/1 tr. řádu
[9] např. pro Jihomoravský kraj je to Skupina Informační Kriminality při Krajském ředitelství policie Jihomoravského kraje

3.3 Prvotní úkony

Prvotním úkonem se rozumí taková činnost, která směřuje k zajištění stopy a jejímu uchování. Může jí být zejména:

- zajištění e-mailové komunikace
- zajištění hlavičky e-mailu
- zajištění obsahu webové stránky v takové podobě, jaká je v době trestního oznámení
- zajištění přijatých SMS zpráv z mobilního telefonu

Zajištění takových stop není nijak složité. Pro účely trestního řízení postačí, když policista například současný stav webové stránky nafotí fotoaparátem, při jejím zobrazení na monitoru a pak o tom sepíše úřední záznam. V tomto úředním záznamu je pak nutno uvést, kdy (rok, měsíc, den, hodina, minuta) a kde (na oddělení, na monitoru služebního počítače připojeného k internetu) byla taková fotografie pořízena. Zejména je důležité uvést, že fotografie byla pořízena za přítomnosti oznamovatele, případně dalších osob.

Zajištění hlavičky e-mailu je možno provést rovněž výše popsaným způsobem. Vhodnější je však takovou hlavičku vytisknout a k tomuto výtisku pak opět pořídit úřední záznam o způsobu domě a místu jeho pořízení a samozřejmě nesmí chybět přítomnost oznamovatele.

Stejně jako v případě zajišťování současného stavu web stránek je možno postupovat i při zajišťování SMS zpráv.

Zajišťování obsahů harddisků, případně konfigurací počítačů a podobně je dobré konzultovat s odborníky, anebo je k takovému zajištění přizvat.

3.4 Lhůty v trestním řízení

Zákon vymezuje pro postup orgánů činných v trestním řízení určité lhůty, které je nutno dodržet, avšak tyto lhůty lze v odůvodněných případech prodlužovat. Neexistuje tedy žádná lhůta, nebo doba trvání trestního řízení, která by byla nepřekročitelná. Délka trestního řízení se posuzuje vždy dle konkrétní věci a povahy případu. Podle judikatury Evropského soudu pro lidská práva platí, že množství práce, nedostatek personálu a špatná organizace, či přetíženost soudů nemohou být důvodem, který by opravňoval soudy k nepřiměřenému zvyšování délky řízení.[10]

Základní délky lhůt jsou stanoveny v ustanovení §159 odst. 1 trestního řádu. K těmto lhůtám je však třeba přistupovat i z pohledu ustanovení §2 odst. 5 trestního řádu, který uvádí, že orgány činné v trestním řízení postupují vždy podle svých oprávnění a povinností a zejména za součinnosti stran tak, aby byl zjištěn skutkový stav věci v takovém rozsahu, který je nutný pro následné rozhodnutí takového orgánu. Z toho plyne, že rychlost řízení není závislá pouze na aktivitě orgánů činných v trestním řízení, ale i na aktivitě dalších stran. Na základě ustanovení §157 odst. 1 trestního řádu je konkrétně policejnímu orgánu ukládáno, aby svou činnost a aktivitu organizoval takovým způsobem, aby přispěl k včasnosti a důvodnosti trestního řízení. Nutno však dodat, že zde musejí být brány v úvahu kriminalisticko-technické požadavky, zvláště pak požadavky na vyhledání a zajištění stop. A právě zde je spatřován největší problém v souvislosti s počítačovou kriminalitou.

[10] Rozsudek ESLP ve věci De Micheli v. Itálie ze dne 26. 2. 1993, publikace pod A-257D.

3.5 Nejčastější druhy trestné činnosti v oblasti internetu prověřované a vyšetřované policií

Roztřídění do níže uvedených kategorií je dáno závažností kriminality a je stanoveno v závislosti na nejčastěji prověřovaných trestných činech.

A) V oblasti držení, šíření a výroby dětské pornografie prostřednictvím internetu a elektronických komunikačních kanálů

B) Oblast nebezpečného vyhrožování a pronásledování prostřednictvím internetu a elektronických kanálů.

C) Oblast specifických trestných činů souvisejících s podstatou existence Internetu a elektronických komunikačních kanálů.

D) Oblast klasických trestných činů využívajících prostředí Internetu a elektronických komunikačních kanálů

Ad A) Oblast držení, šíření a výroby dětské pornografie prostřednictvím internetu a elektronických komunikačních kanálů

Dotčená ustanovení:

- §191 trestního zákoníku – Šíření pornografie
- §192 trestního zákoníku – Výroba a jiné nakládání s dětskou pornografií

Popis trestné činnosti:

Jedná se o trestnou činnost, při jejímž páchání dochází pouze ke komunikaci pachatelů této trestné činnosti prostřednictvím různých komunikačních kanálů, jako je např.: e-mail, Skype, ICQ, různé sociální sítě (Facebook, Badoo, www.lide.cz) a podobně. Pachatelé si vytvoří falešnou identitu a prostřednictvím výše uvedených sociálních sítí kontaktuje jiné podobně zaměřené pachatele. Poté si prostřednictvím těchto komunikačních kanálů spolu

vyměňují materiály obsahující dětskou pornografii v elektronické podobě. Tyto materiály získávají buď na internetu, nebo ji sami pořizují. Nezřídka je zaznamenán případ, kdy zkušený pachatel, který tuto činnost páchá po delší dobu, nutí svou, ne ještě tak zkušenou, protistranu, aby tyto materiály sama sháněla, případně vytvářela, kdy takto může dojít i ke spáchání vedlejší trestné činnosti, jakou je například vydírání.

Úkony prováděné při prověřování, šetření a vyšetřování:

U těchto trestných činů jsou prováděny úkony, jako vyžadování obsahu e-mailových schránek, obsahů internetové komunikace na zmiňovaných kanálech, jsou zajišťovány logy přístupů do e-mailových schránek, případně do uvedených komunikačních kanálů, jsou ustanovovány majitelé IP adres, případně alespoň adres přípojek internetu dle IP adres zjištěných k pachatelům.

Zde byla policie značně znevýhodněna vydáním nálezu Ústavního soudu PI 24/2010 ze dne 22. 3. 2011, týkajícího se zrušení vyhlášky č. 485/2005 Sb. a odstavců 3, 4 § 97 zákona č. 127/2005 Sb., o elektronických komunikacích, kdy tento nález prakticky znemožnil policii vyžadovat výše uvedené nezbytné informace. Teprve nedávno došlo k novelizaci tohoto ustanovení a upřesnění způsobu ukládání a uchovávání takových informací a způsobu a podmínek jejich vyžadování.

Ad B) Oblast nebezpečného vyhrožování a pronásledování prostřednictvím internetu a elektronických kanálů.

Dotčená ustanovení:

- §175 trestního zákoníku – Vydírání
- §272 trestního zákoníku – Obecné ohrožení
- §352 trestního zákoníku – Násilí proti skupině obyvatelů a proti jednotlivci
- §353 trestního zákoníku – Nebezpečné vyhrožování
- §357 trestního zákoníku – Šíření poplašné zprávy

Popis trestné činnosti:

Jedná se o trestnou činnost, která byla zmiňována v kapitole 2, kdy pachatel, v domnění, že je na internetu úplně anonymní, z nejrůznějších pohnutek pronásleduje, případně pouze vyhrožuje své oběti, které totožnost pachatele není vůbec známa, nebo oběť totožnost pachatele jen tuší, anebo oběť přímo zná totožnost pachatele a to hlavně dle textu a způsobu vedení výhrůžek. Pachatel provádí svou činnost tak, že všemi mu známými způsoby se snaží svou identitu zakrýt.

Úkony prováděné při prověřování, šetření a vyšetřování:

U takových trestných činů jsou zejména vyžadovány obsahy e-mailových schránek, obsahy internetové komunikace na různých komunikačních kanálech, z těchto je pak prováděno ustanovování IP adres a dle nich pak místa přípojky, případně i osoby, které je taková IP adresa přidělena. Provádí se i zajišťování výpisu pevných i mobilních telefonů a následně ustanovování jejich majitelů, či používatelů. Na základě toho pak lze nejen určit osobu, ale i místo, odkud je taková trestná činnost páchána. Ve výjimečných případech může dojít i k nasazení odposlechu jak na telefony, tak i na e-mailové schránky, případně na jiné komunikační kanály.

Ad C) Oblast specifických trestných činů souvisejících s podstatou existence Internetu a elektronických komunikačních kanálů.

Dotčená ustanovení:

- **§228** trestního zákoníku – **Poškození cizí věci**
- **§230** trestního zákoníku – **Neoprávněný přístup k počítačovému systému a nosiči informací**
- **§231** trestního zákoníku – **Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat**

- **§232** trestního zákoníku – **Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti**
- **§276** trestního zákoníku – **Poškození a ohrožení provozu obecně prospěšného zařízení**

Popis trestné činnosti:

Jedná se o trestnou činnost páchanou především na samotných základech výpočetní techniky a počítačových sítí a dalších elektronických komunikačních nástrojů. Většinou se jedná o sofistikované útoky na některá zařízení, která jsou zařazena so počítačových systémů. Například útoky na vysílače bezdrátového připojení k síti, prolamování hesel, útoky na webové stránky a podobně. Útočník svou činností nikterak fyzicky nepoškodí takové zařízení, ale pomocí sofistikovaného softwarového útoku například cíleně směřuje tok dat na jeden konkrétní server v úmyslu jej tímto tokem zahltit. Tento útok se nazývá DOS (Denied of Service). Dalším takovým útokem může být rušení signálu bezdrátového připojení a tím znemožnění správné funkce tohoto zařízení, průnik do zabezpečeného systému využitím nedostatečné ochrany takového systému, obejitím ochranných opatření, a v důsledku tohoto pak smazání dat v chráněném systému, pozměnění dat. Může se jednat i o útoky na bankovní systémy. V takových případech zanechává útočník pouze elektronickou stopu a to zejména IP adresu.

Úkony prováděné při prověřování, šetření a vyšetřování:

Při prověřování takových případů je nutno vyžadovat a zjišťovat uživatele IP adresy, či místa přípojky, a v případě, že pachatel použije jiné elektronické nástroje je nutno zjišťovat údaje nutné k identifikaci pachatele. To se děje zejména na základě soudního příkazu ke sdělení Údajů o uskutečněném telekomunikačním provozu. Na základě těchto údajů je pak možno zjistit, případně za použití dalších prostředků dohledat místo páchání trestné činnosti a následně určit konkrétní osobu pachatele.

Ad D) Oblast klasických trestných činů využívajících prostředí Internetu a elektronických komunikačních kanálů

Dotčená ustanovení:

- **§209** trestního zákoníku – **Podvod**
- **§181** trestního zákoníku – **Poškozování cizích práv**
- **§182** trestního zákoníku – **Porušení tajemství dopravované zprávy**

Popis trestné činnosti:

Jedná se o podvodnou trestnou činnost, která normálně spadá do oblasti obecné kriminality, ale k jejímuž spáchání je použito internetu, jiné počítačové sítě a elektronických komunikačních prostředků a kanálů. Jsou to zejména falešné – podvodné inzeráty, ve kterých prodávající nabízí k prodeji zboží, které nevlastní a následně po projevení zájmu ze strany kupujících si nechá poslat peníze předem a zboží samozřejmě nikdy nedodá. Pachatelé používají výhradně elektronické komunikační prostředky, jimiž kryjí svou identitu, tuto mění a využívají i falešné, nebo v poslední době velice oblíbené anonymní účty, na které si peníze nechají zasílat.

Úkony prováděné při prověřování, šetření a vyšetřování:

Při prověřování a následném vyšetřování této trestné činnosti jsou vyžadovány obsahy e-mailových schránek, obsahy internetové, či elektronické komunikace, logy přístupů do takových schránek, nebo komunikačních prostředků, následně pak ustanovování IP adresy, zajišťování výpisů z pevných i mobilních telefonů dle ust. §88a – Údaje o uskutečněném telekomunikačním provozu. Následně stejně jako v předchozích případech dochází na základě takto získaných dat ke zjišťování místa spáchání a ke zjištění totožnosti pachatele.

3.6 Popis jednotlivých postupů a úkonů při prověřování, šetření a vyšetřování

- **Ustanovení IP adresy**

Pokud policejní orgán při prověřování zjistí jako vodítko k dalším informacím IP adresu, je nutno zjistit, kdo (jaká společnost poskytující připojení k internetu) tuto IP adresu spravuje.

Takové zjištění se provádí běžným způsobem a to například dotazem na stránkách www.ripe.net, kdy společnost RIPE eviduje všechny IP adresy Evropského kontinentu. Zde je tedy možno zjistit poskytovatele internetového připojení. Konkrétní zařízení, kterému je IP adresa přidělena však RIPE neeviduje. Tuto informaci je nutno získat od konkrétního provozovatele internetového připojení.

- **Vyžádání dat o uskutečněném telekomunikačním provozu**[11]

Pokud je třeba pro řádné objasnění věci zjistit provozně lokalizační data, musí policejní orgán navrhnout příslušnému Státnímu zastupitelství, který předmětný spis dozoruje, aby od příslušného soudu vyžádalo příkaz ke sdělení dat o uskutečněném telekomunikačním provozu. V tomto návrhu odesílaném policejním orgánem musí být uveden popis skutku, pro který je trestní řízení vedeno, dále zde musí být uvedeny doposud zjištěné skutečnosti a zejména musí být uveden důvod, který opravňuje takové vyžádání informací. Tento důvod musí být podepřen tou skutečností, že jinačím způsobem není možno taková data, či takové informace získat a není jiná možnost, jak věc objasnit. Vyžádat takové informace lze samozřejmě pouze za určitých podmínek a pouze v určitých konkrétních, taxativně vyjmenovaných případech, jak je uvedeno v odstavci 1 tohoto ustanovení.

[11] Provozní data o uskutečněném telekomunikačním provozu jsou údaje o tom, v jaké době (rok, měsíc, den, hodina, minuta a vteřina), jaké zařízení (IP adresa, případně IP + port) komunikovala s jakým jiným zařízením (IP adresa, případně IP + port) na protější straně, kolik dat bylo přeneseno, jak dlouho spojení trvalo a o jaký druh spojení šlo (e-mail, web, ftp atd.)

Ustanovení §88a trestního řádu zní:

„ (1) Je-li třeba pro účely trestního řízení vedeného pro úmyslný trestný čin, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně tři roky, pro trestný čin porušení tajemství dopravovaných zpráv (§ 182 trestního zákoníku), pro trestný čin podvodu (§ 209 trestního zákoníku), pro trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací (§ 230 trestního zákoníku), pro trestný čin opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 trestního zákoníku), pro trestný čin nebezpečného vyhrožování (§ 353 trestního zákoníku), pro trestný čin nebezpečného pronásledování (§ 354 trestního zákoníku), pro trestný čin šíření poplašné zprávy (§ 357 trestního zákoníku), pro trestný čin podněcování k trestnému činu (§ 364 trestního zákoníku), pro trestný čin schvalování trestného činu (§ 365 trestního zákoníku), nebo pro úmyslný trestný čin, k jehož stíhání zavazuje vyhlášená mezinárodní smlouva, kterou je Česká republika vázána, zjistit údaje o telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat a nelze-li sledovaného účelu dosáhnout jinak nebo bylo-li by jinak jeho dosažení podstatně ztížené, nařídí v řízení před soudem jejich vydání soudu předseda senátu a v přípravném řízení nařídí jejich vydání státnímu zástupci nebo policejnímu orgánu soudce na návrh státního zástupce. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn, včetně konkrétního odkazu na vyhlášenou mezinárodní smlouvu v případě, že se vede trestní řízení pro trestný čin, k jehož stíhání tato mezinárodní smlouva zavazuje. Vztahuje-li se žádost ke konkrétnímu uživateli, musí být v příkazu uvedena jeho totožnost, je-li známa. Je-li k objasnění skutečností důležitých pro trestní řízení třeba zjistit údaje o uskutečněném telekomunikačním provozu, které jsou předmětem telekomunikačního tajemství anebo na něž se vztahuje ochrana osobních a zprostředkovacích dat, nařídí předseda senátu a v přípravném řízení soudce, aby je právnické nebo fyzické osoby, které vykonávají telekomunikační činnost, sdělily jemu a v přípravném řízení buď státnímu zástupci, nebo policejnímu orgánu. Příkaz k zjištění údajů o telekomunikačním provozu musí být vydán písemně a odůvodněn.

(2) Státní zástupce nebo policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, a v řízení před soudem předseda senátu soudu prvního stupně po pravomocném skončení věci informuje o nařízeném zjišťování údajů o telekomunikačním provozu osobu

uživatele uvedenou v odstavci 1, pokud je známa. Informace obsahuje označení soudu, který vydal příkaz k zjištění údajů o telekomunikačním provozu, a údaj o období, jehož se tento příkaz týkal. Součástí informace je poučení o právu podat ve lhůtě šesti měsíců ode dne doručení této informace Nejvyššímu soudu návrh na přezkoumání zákonnosti příkazu k zjištění údajů o telekomunikačním provozu. Informaci podá předseda senátu soudu prvního stupně bezodkladně po pravomocném skončení věci, státní zástupce, jehož rozhodnutím byla věc pravomocně skončena, podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí nejvyšším státním zástupcem podle § 174a a policejní orgán, jehož rozhodnutím byla věc pravomocně skončena, podá informaci bezodkladně po uplynutí lhůty pro přezkoumání jeho rozhodnutí státním zástupcem podle § 174 odst. 2 písm. e). Příkazu podle odstavce 1 není třeba, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním provozu vztahovat.

(3) Informaci podle odstavce 2 předseda senátu, státní zástupce nebo policejní orgán nepodá v řízení o zločinu, na který zákon stanoví trest odnětí svobody s horní hranicí trestní sazby nejméně osm let, spáchaném organizovanou skupinou, v řízení o trestném činu spáchaném ve prospěch organizované zločinecké skupiny, v řízení o trestném činu účasti na organizované zločinecké skupině (§ 361 trestního zákoníku), nebo pokud se na spáchání trestného činu podílelo více osob a ve vztahu alespoň k jedné z nich nebylo trestní řízení doposud pravomocně skončeno, nebo pokud je proti osobě, jíž má být informace sdělena, vedeno trestní řízení, anebo pokud by poskytnutím takové informace mohl být zmařen účel tohoto nebo jiného trestního řízení, nebo by mohlo dojít k ohrožení bezpečnosti státu, života, zdraví, práv nebo svobod osob.

(4) Příkazu podle odstavce 1 není třeba, pokud k poskytnutí údajů dá souhlas uživatel telekomunikačního zařízení, ke kterému se mají údaje o uskutečněném telekomunikačním provozu vztahovat.“

Státní zástupce, poté co obdrží od policejního orgánu takový návrh, zváží jeho oprávněnost a poté co konstatuje, že je v souladu s výše uvedeným ustanovením a že je oprávněný, sepíše žádost o vydání příkazu k o uskutečněném telekomunikačnímu provozu a tuto odešle soudu.

Soud následně opět zváží oprávněnost vydání takového příkazu a následně, pokud shledá všechny podmínky splněné, vydá příkaz ke sdělení údajů o uskutečněném telekomunikačním provozu (dále jen příkaz). Tento odešle státnímu zástupci, který jej následně odešle policejnímu orgánu. Takové vydání příkazu od návrhu policejního orgánu až po obdržení příkazu může trvat i několik týdnů. V průměru se tato doba pohybuje kolem dvou až tří týdnů.

V ideálním případě je nutno takový příkaz vyžádat pouze jedenkrát. Ve složitějších případech se musí proces vydání příkazu opakovat. Například v případě, že IP adresa, o níž jsou takovým způsobem údaje vyžadovány, patří do adresního rozsahu společnosti, která ji dále poskytuje jiné menší společnosti, zpravidla lokálnímu poskytovateli internetového připojení. Proto se policejnímu orgánu doporučuje vyžádat si tak zvaný hromadný příkaz, kdy soud vydá příkaz pro všechny společnosti, které se zabývají poskytováním připojení k internetu související s uvedenou IP adresou. Ne všechny soudy však přistoupí na vydání takového příkazu, některé trvají na tom, že vydají pouze příkaz ke konkrétní společnosti a pak je nutno celý proces opakovat.

Následně je třeba takto získaný příkaz, úkony provádějícím policistou, směřovat povinné společnosti, cestou Útvaru zvláštních činností (dále jen ÚZČ), který jediný má oprávnění za takové služby platit, neboť dle zvláštního předpisu platí, že dožadované společnosti mají nárok na proplacení účelně vynaložených nákladů spojených s provedením vypracování odpovědi na dožádání.

- **Vyžádání LOGů přihlašování do e-mailové schránky**

V případě, že je potřeba zajistit LOG soubor – tedy soubor, který obsahuje datum a přesný čas přístupu určitého uživatele k určité službě (například uživatele k e-mailové schránce), je nutno oslovit provozovatele stránek, které takovou službu poskytují a to za využití ustanovení §8 odst. 1 tr. řádu, který říká, že „*státní orgány, právnické a fyzické osoby jsou povinny bez zbytečného odkladu, a nestanoví-li zvláštní předpis jinak, i bez úplaty vyhovovat dožádáním orgánů činných v trestním řízení při plnění jejich úkolů.*“ Tento dotaz je třeba vyžadujícím policistou směřovat cestou Útvaru zvláštních činností (dále jen ÚZČ), který jediný má oprávnění za takové služby platit, neboť dle zvláštního

předpisu platí, že dožadované společnosti mají nárok na proplacení účelně vynaložených nákladů spojených s provedením vypracování odpovědi na dožádání.

- **Vyžádání obsahu e-mailové schránky**

Pokud je třeba pro trestní řízení vyžádat obsah e-mailové schránky, tedy obsah všech přijatých, odeslaných a rozepsaných zpráv, je nutno postupovat odlišně, neboť tímto dotazem již policie zasahuje do soukromí osoby, která e-mailovou schránku používá. Proto je třeba, aby policista navrhl Okresnímu státnímu zástupci (dále jen OSZ), aby vyžádal od příslušného soudu opět příkaz dle ust. §88a, který musí být zdůvodněn stejně jako uvedeno výše.

- **Odposlech e-mailové komunikace**

Pokud je pro účely trestního řízení nezbytně nutné sledovat nové příchozí a odchozí e-mailové zprávy, lze provést i takový úkon, ale zásadně rozlišným způsobem, neboť zde je míra zásahu do osobních svobod osoby omezována takovou měrou, že již nepostačí pouze žádost a soudní příkaz, ale celý tento úkon se děje v režimu „Vyhrazené“ – tedy v prvním stupni utajení.

V takovém případě je nutno, aby policejní orgán v tomto speciálním režimu požádal státního zástupce dle ust. §158d odst. 3 tr. řádu, aby tento vyžádal písemné povolení ke sledování věci – e-mailové schránky od příslušného soudu. Pak opět přes ÚZČ, které má na starosti technickou stránku úkonu, se provede realizace tohoto úkonu, kdy vyžadující policista obdrží každý den kopie odesílaných a přijímaných zpráv ze sledované schránky. Toto samozřejmě nelze provádět neomezeně dlouhou dobu. Trestní řád na tuto činnost stanoví dobu nejvýše šesti měsíců a poté, je-li toho stále třeba, musí požádat o prodloužení o tohoto úkonu, kdy toto musí náležitě zdůvodnit a doložit, že doposud získané údaje jsou pro trestní řízení použitelné. Prodloužit lze o nejvýše 6 měsíců a to i opakovaně.

II. PRAKTICKÁ ČÁST

4 VÝZKUM

Tato část se bude zabývat výzkumem, bude specifikován cíl výzkumu a výběr strategie použité pro výzkum. Dále bude následovat Operacionalizace a následně bude popsána technika sběru dat a specifikován výzkumný vzorek.

4.1 Cíl výzkumu a volba strategie

Pomocí výzkumu bude zjišťováno, zda mají policisté, sloužící u Policie České republiky, povědomí o tom, co je to počítačová kriminalita za účelem zjištění, zda by dokázali správně přijmout trestní oznámení a následně takový druh kriminality vyšetřovat. Základním cílem výzkumu tedy je odpověď na otázku:

„Vědí policisté v České republice, co je to počítačová kriminalita a dokážou správně postupovat při přijímání trestního oznámení a následně při prověřování a vyšetřování tohoto specifického druhu trestné činnosti?“

O výsledcích výzkumu bude informován management policie s cílem poukázat na skutečnost, že vzhledem k významně narůstajícím počtům případů počítačové kriminality, bude u policistů potřeba zvýšit povědomí o tomto druhu trestné činnosti,

Pro tento výzkum byla zvolena kvantitativní strategie, za použití deduktivní metody, která vychází z teorie, nebo obecně formulovaného problému. Byla použita základní metoda strukturovaného rozhovoru formou dotazníkového šetření.

Teoretická hypotéza tedy zní:

Valná většina policistů v České republice má jen mlhavé povědomí o tom, co to je počítačová kriminalita a při setkání se s oznamovatelem takového trestného činu jen velmi vzdáleně tuší, která specifika od takového oznamovatele zjistit, jak správně zajistit důkazy o tomto druhu trestné činnosti a jak správně postupovat při prověřování a následném vyšetřování této specifické trestné činnosti.

Ke zjištění odpovědi na tuto otázku byla zvolena dotazníková metoda, která byla aplikována na poměrném vzorku policistů – policistů zařazených na Službě kriminální policie a vyšetřování – Odbor obecné kriminality, Službě kriminální policie a vyšetřování – Odbor hospodářské kriminality a Obvodních oddělení policie Územního odboru Hodonín.

4.2 Operacionalizace

Pod pojmem informovanost je myšlen především soubor znalostí a vědomostí o počítačové kriminalitě. Informovanost nelze zřejmě empiricky změřit, a proto bylo přistoupeno k jejímu rozložení do souboru pracovních hypotéz. Dále budou uvedeny indikátory, které mají vliv na míru informovanosti policistů a jejich schopnost rozlišit počítačovou kriminalitu od ostatních druhů kriminality. Byly vytvořeny celkem 3 pracovní hypotézy, jejichž platnost bude ověřena na základě výsledků dotazníkového šetření. Již v první otázce je položen dotaz na zařazení respondenta u policie, neboť tento indikátor může mít zásadní vliv na zkoumaný jev.

Pracovní hypotéza 1:

„Policisté zařazení na Obvodním oddělení policie mají nižší znalosti z oboru počítačové kriminality než policisté zařazení na SKPV.“

Ověřováním pracovní hypotézy č. 1 byla zjišťována schopnost rozlišit počítačovou kriminalitu od jiné v závislosti na pracovním zařazení a na zprostředkování informací ze strany policie jako zaměstnavatele a následného zjišťování, zda takové zprostředkování informací bylo účinné, či zda jej respondenti považují za dostačující.

Otázky dotazníku:

- Na jakém útvaru policie jste zařazen?
- Setkal jste se někdy s pojmem počítačová kriminalita?
- Byl/a jste někdy na školení zaměřeném na oblast počítačové kriminality?
- Pokud jste se školení z oblasti počítačové kriminality zúčastnil, bylo pro Vás přínosné?
- Hacker je?

Pracovní hypotéza 2.

Policisté i přes svou nízkou informovanost, dokáží rozeznat počítačovou kriminalitu od ostatních druhů kriminality.

Ověřováním pracovní hypotézy č. 2 byla zjišťována schopnost policistů všeobecně, rozlišit počítačovou kriminalitu a schopnost tuto správně kvalifikovat.

Otázky dotazníku:

- Počítačová kriminalita znamená:
- Znáte podstatná specifika počítačové kriminality, která je nutno zjišťovat při přijímání trestního oznámení z oblasti počítačové kriminality?
- Jak budete kvalifikovat trestní oznámení: „Někdo mi z mého profilu na FaceBooku stahuje moje veřejně přístupné fotografie a rozesílá je mým známým, i neznámým osobám?“
- Která ustanovení nemůže patřit do oblasti počítačová kriminalita?

Pracovní hypotéza 3

Policisté všeobecně neznají postupy při prověřování a následném vyšetřování počítačové kriminality.

Ověřováním pracovní hypotézy č. 3 byla zjišťována dovednost a znalost policistů všeobecně, jak postupovat při prověřování a vyšetřování počítačové kriminality, jejích specifik a specialit.

Otázky dotazníku:

- Víte koho kontaktovat v případě, že budete přijímat nebo prověřovat oznámení z oblasti počítačové kriminality?
- Které ustanovení trestního řádu upravuje získávání informací o uskutečněném telekomunikačním provozu

- Je nutno žádat soud cestou Okresního státního zastupitelství o vydání příkazu dle ust. §88a tr. řádu v případě, že je potřeba zajistit od poskytovatele internetového připojení, smlouvu o poskytování internetu osobě, které byla v určitém časovém období přidělena určitá IP adresa?

- Smí policista vyžádat informace o uživateli konkrétní IP adresy a jeho připojení na konkrétní stránky v přesně určeném čase od poskytovatele internetového připojení žádostí dle ust. §8/1 tr. řádu?

4.3 Technika sběru dat

Jak výše uvedeno, byla zvolena kvantitativní strategie výzkumu, která, jak uvádí Disman: „Není nic jiného než testování hypotéz.“ (Disman, 2011, s. 76), a proto byla zvolena deduktivní metoda, která vychází z teorie, nebo obecně formulovaného problému. Základní metodou, která byla použita je strukturovaný rozhovor formou dotazníkového šetření, neboť ten nejlépe naplňuje požadavky měření, kvůli čemuž je mu v této strategii dávána přednost před polostrukturovaným a nebo nestrukturovaným rozhovorem. Sběr dat byl tedy veden formou dotazníkového šetření. Dotazník je anonymní a vychází z operacionalizace. Obsahuje polootevřené otázky a uzavřené otázky. V tomto případě se jedná o jednorázové výběrové šetření, neboť se provádí v jednom časovém okamžiku. Pomocí získaných dat bude následně zjišťována pravdivost jednotlivých hypotéz.

4.4 Výzkumný vzorek

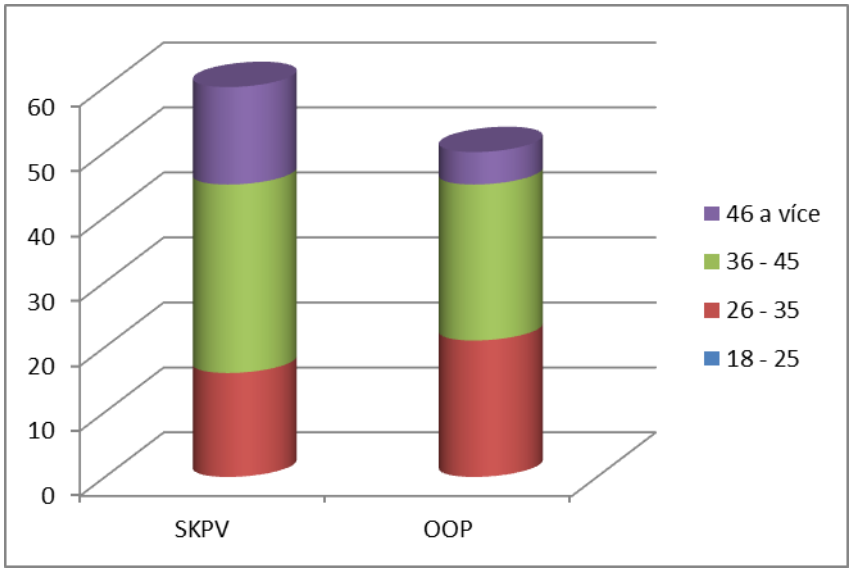
Základní množinou osob pro tento výzkum je okruh policistů, u kterých je předpoklad, že pro ně bude výzkum platný. Jedná se, jak již bylo výše uvedeno o vzorek policistů sloužících na Územním odboru Hodonín, zařazených na Obvodních odděleních, Odděleních kriminální policie obecné i hospodářské, neboť právě tito policisté přicházejí nejčastěji do kontaktu s osobami podávajícími trestní oznámení v oblasti počítačové kriminality a neboť tito policisté následně tuto trestnou činnost prověřují a vyšetřují.

4.5 Výsledky výzkumu

Na základě shromážděných dat za pomoci výše popsaných metod bylo zjištěno, že z celkového počtu 150 dotazovaných policistů nakonec dotazník odevzdalo pouze 110. Policisté zařazení na Obvodních odděleních odevzdali méně dotazníků než policisté zařazení na SKPV. Celkem tedy odpovědělo 50 policistů zařazených na OOP a 60 policistů zařazených na SKPV.

Tabulka 1 - Věkové rozložení dotazovaných podle zařazení

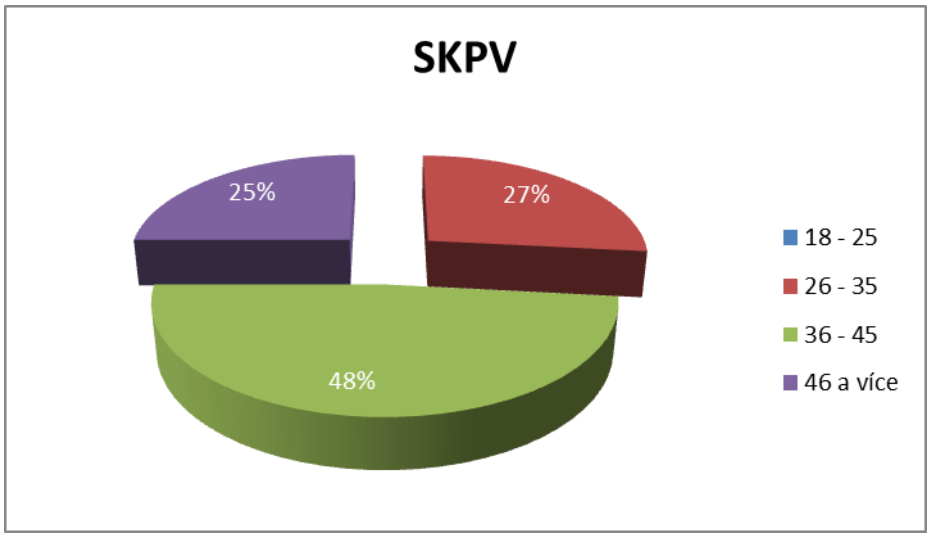
Zařazení	18 - 25	26 - 35	36 - 45	46 a více
SKPV	0	16	29	15
OOP	0	21	24	5



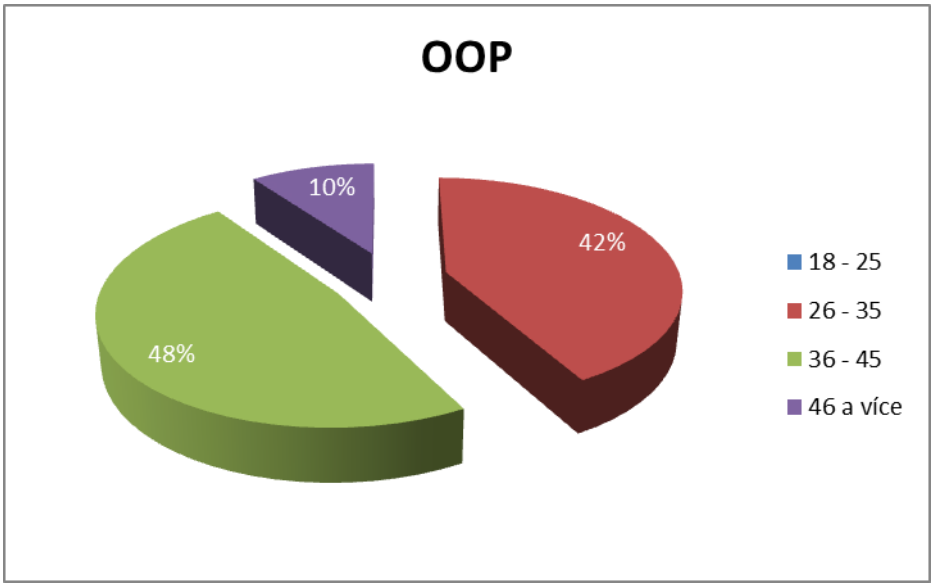
Obrázek 1 – Věkové zastoupení policistů dle zařazení na jednotlivých odděleních

Na Tabulce 1 a Obrázku 1 je vidět, jaké je zastoupení policistů Územního odboru Hodonín dle věku. Na obou dvou součástech policie, tedy jak na oddělení Služby

kriminální policie a vyšetřování, tak i na obvodních odděleních převládá věková skupina 36 – 45 let.



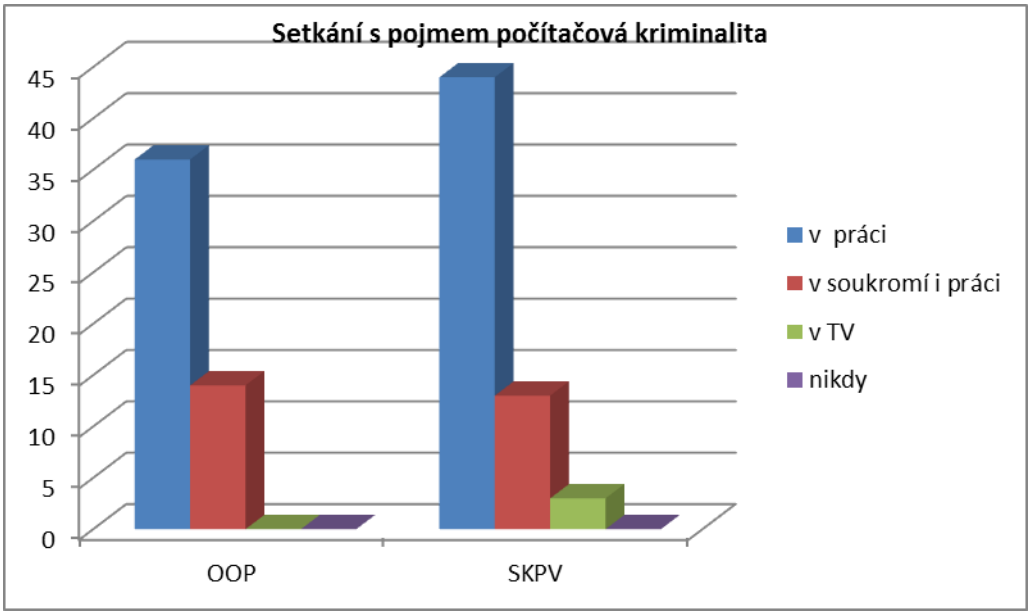
Obrázek 2 – Věkové zastoupení policistů na SKPV



Obrázek 3 – Věkové zastoupení policistů na obvodních odděleních

Tabulka 2 – Setkání se s pojmem: „počítačová kriminalita“

Zařazení	v práci	v soukromí i p	v TV	nikdy
OOP	36	14	0	0
SKPV	44	13	3	0

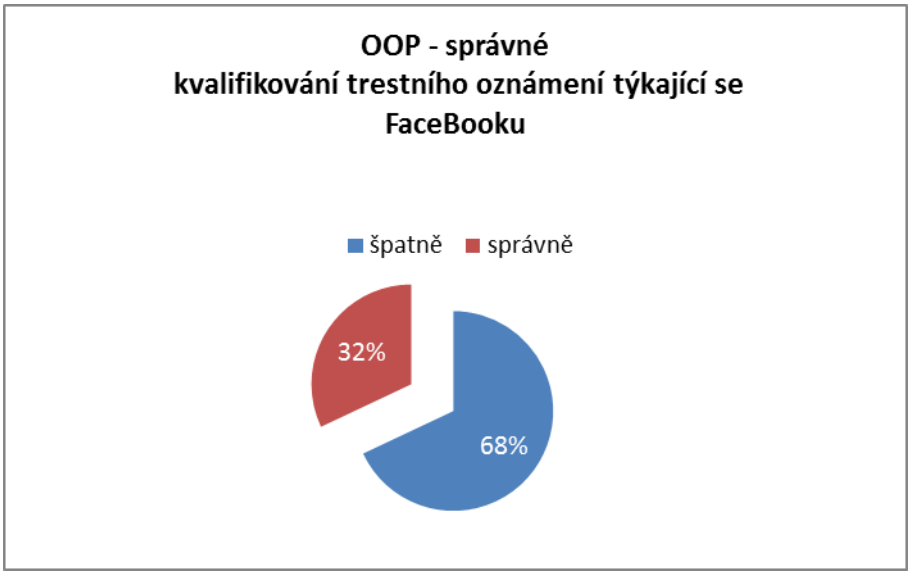


Obrázek 4 – Kde se policisté setkali s pojmem počítačová kriminalita

Na základě uvedené tabulky 2 a obrázku 4 je zjištěno, že nejvíce se policisté, a to bez ohledu na jejich zařazení, setkávají s pojmem „počítačová kriminalita“ v práci. Z toho je možno usuzovat, že většina policistů není o počítačové kriminalitě informována z medií a v soukromém životě se s ní setkalo jen malé procento policistů.

Tabulka 3 – Kolik policistů by správně kvalifikovalo trestní oznámení týkající se FaceBooku

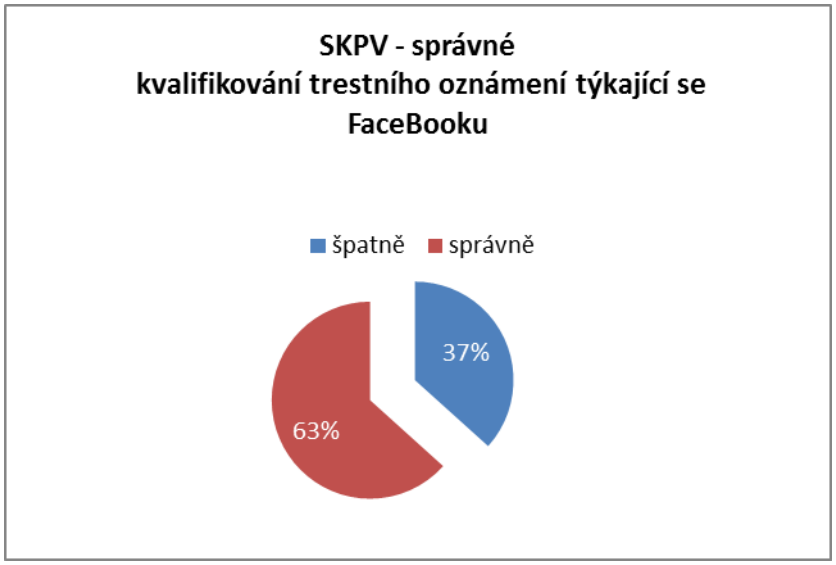
Zařazení	špatně	správně
OOP	34	16
SKPV	22	38



Obrázek 5 – Rozbor odpovědi týkající se kvalifikace trestného činu v oblasti FaceBooku

Speciální otázkou týkající se prověření znalostí policistů o oblasti Sociálních sítí a kvalifikace případných trestných činů byla otázka týkající se problematiky šíření, rozšiřování a sdílení fotografií, které si uživatelé sociální sítě Facebook umístí na svůj profil s tím, že k těmto fotografiím nenastaví žádná práva pro jejich zobrazení, tedy si je může prohlédnout kterýkoli uživatel této sociální sítě, který si jejich profil vyhledá. Správnou odpovědí samozřejmě je, že pokud uživatel nechá své fotografie dostupné pro všechny uživatele, stávají se dostupnými pro každého a tedy je možno je šířit, bez porušení zákonů, neboť každý uživatel Facebooku, tím že odsouhlasí Všeobecné podmínky používání této sociální sítě, zároveň souhlasí s tím, že pokud své fotografie, které předtím vložil na svůj profil, neznepřístupní ostatním uživatelům, jsou tyto dostupné pro všechny uživatele.

V této oblasti jsou znalosti policistů zařazených na Obvodních odděleních velmi slabé, neboť jak je vidět z obrázku 5, správně odpovědělo pouze 32% dotázaných, zatímco na odděleních kriminální policie, je znalost problematiky v této oblasti značně vyšší. Správně by tento čin kvalifikovalo 63% dotázaných.

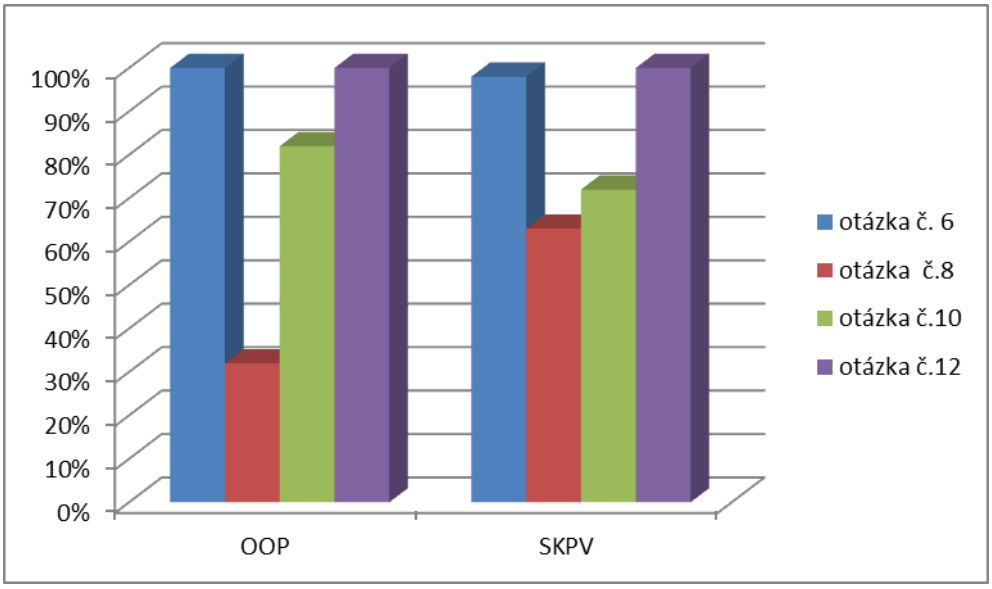


Obrázek 6 - Rozbor odpovědi týkající se kvalifikace trestného činu v oblasti FaceBooku

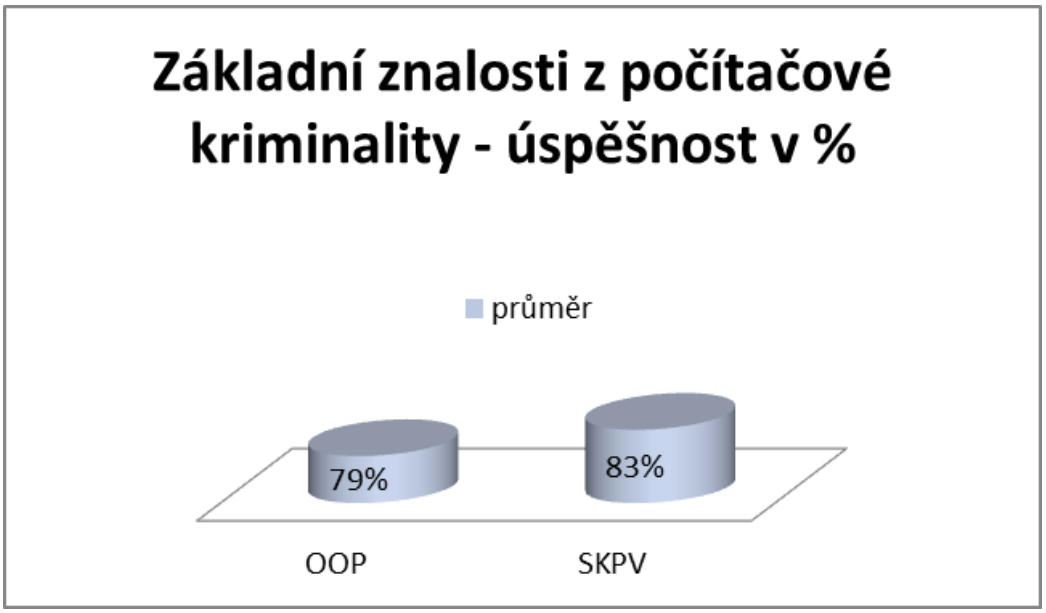
Provedenou analýzou základních znalostí v oblasti počítačové kriminality bylo tedy zjištěno, že 79% policistů zařazených na obvodních odděleních a 83% policistů kriminální služby má základní znalosti v oblasti počítačové kriminality a zná základní pojmy.

Tabulka 4 – Procentuální hodnocení správných odpovědí na základní otázky v oblasti počítačové kriminality

Zařazení	otázka č. 6	otázka č.8	otázka č.10	otázka č.12	průměr
OOP	100%	32%	82%	100%	79%
SKPV	98%	63%	72%	100%	83%



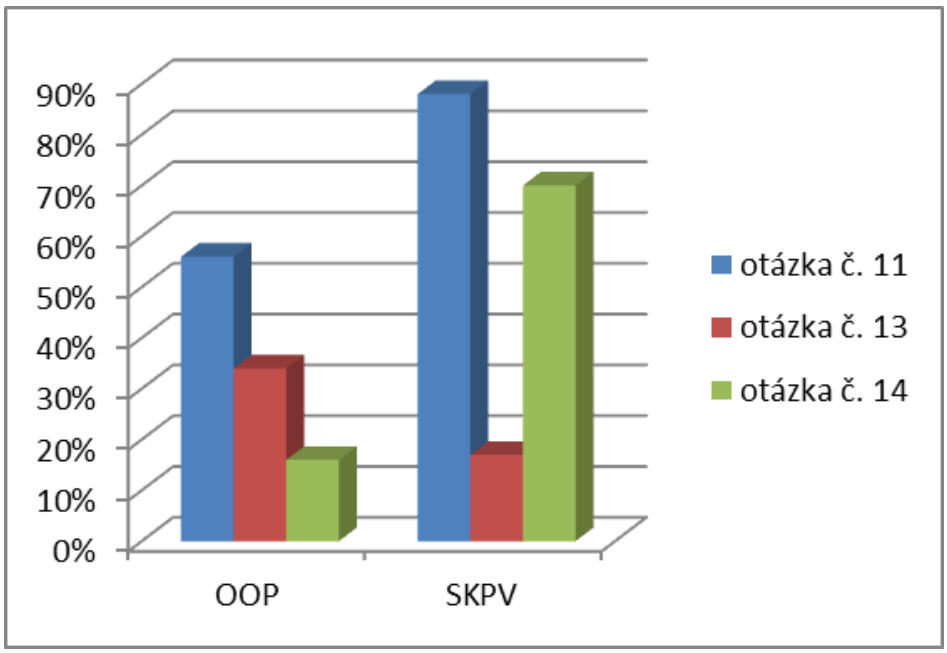
Obrázek 7 – Grafické zobrazení procentuálního hodnocení správných odpovědí základních vědomostí o počítačové kriminalitě



Obrázek 8 – Průměr ze správně zodpovězených otázek základních znalostí

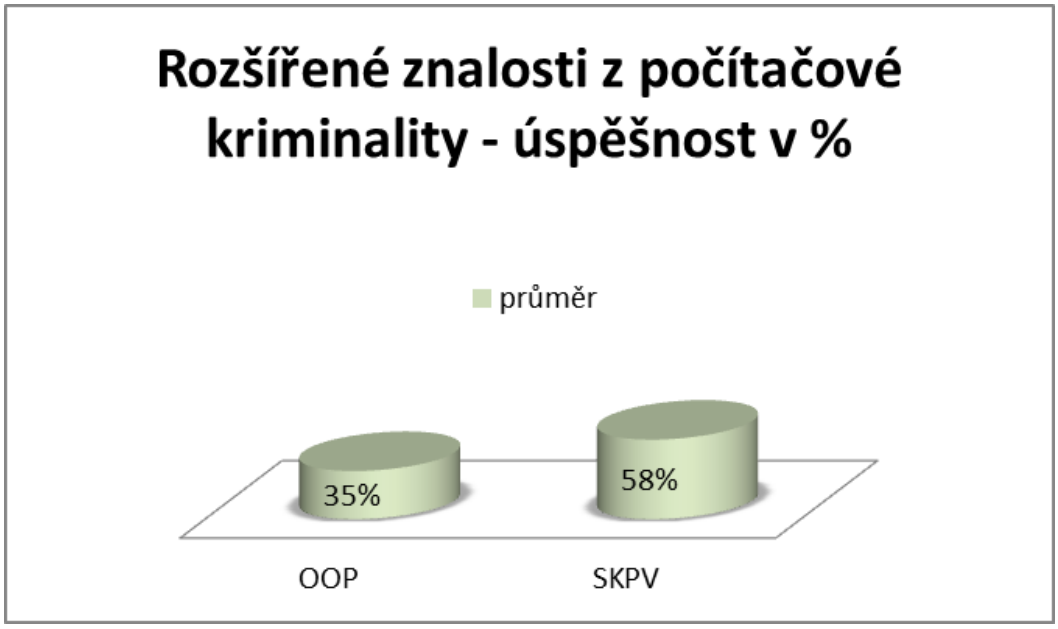
Tabulka 5 – Procentuální úspěšnost v otázkách z rozšířenějších znalostí v oblasti počítačové kriminality

Zařazení	otázka č. 11	otázka č. 13	otázka č. 14	průměr
OOP	56%	34%	16%	35%
SKPV	88%	17%	70%	58%



Obrázek 9 - Procentuální úspěšnost v otázkách z rozšířenějších znalostí v oblasti počítačové kriminality

V oblasti užších – speciálních – vědomostí týkajících se počítačové kriminality a zejména vyšetřování tohoto druhu trestné činnosti je to, jak je patrné z tabulky 5 a obrázku 9, výrazně horší a to jak na obvodních odděleních, kde správně odpovědělo pouze 35% policistů, tak i na straně služby kriminální policie, kde správně odpovědělo 58% dotázaných policistů. Neznalost správných postupů a absence speciálních znalostí je dána především tím, že policisté na obvodních odděleních se s vyšetřováním počítačové kriminality setkávají jen velmi zřídka. Tato problematika je především směřována na oddělení služby kriminální policie. Toto je patrné i z tabulky 5.



Obrázek 10 – Procentuální výsledky správných odpovědí z rozšířených znalostí v oblasti počítačové kriminality

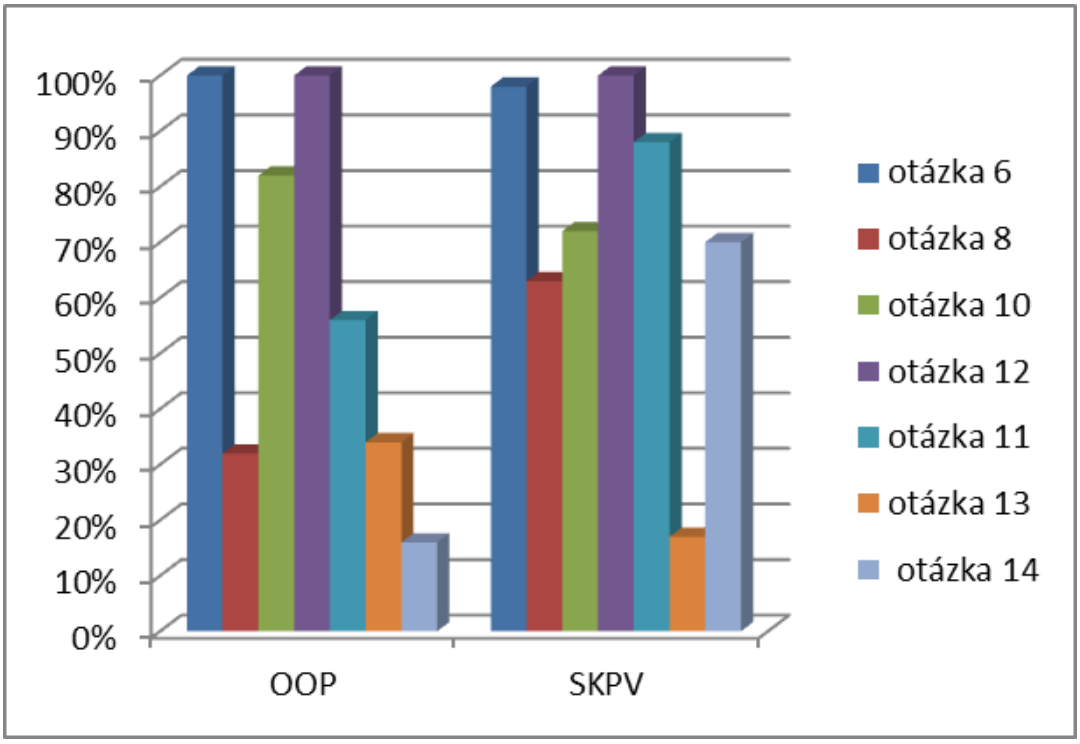
Tabulka 6 – Celkové výsledky v testu ze znalostí počítačové kriminality

Zařazení	otázka 6	otázka 8	otázka 10	otázka 12	otázka 11	otázka 13	otázka 14	průměr
OOP	100%	32%	82%	100%	56%	34%	16%	60%
SKPV	98%	63%	72%	100%	88%	17%	70%	73%

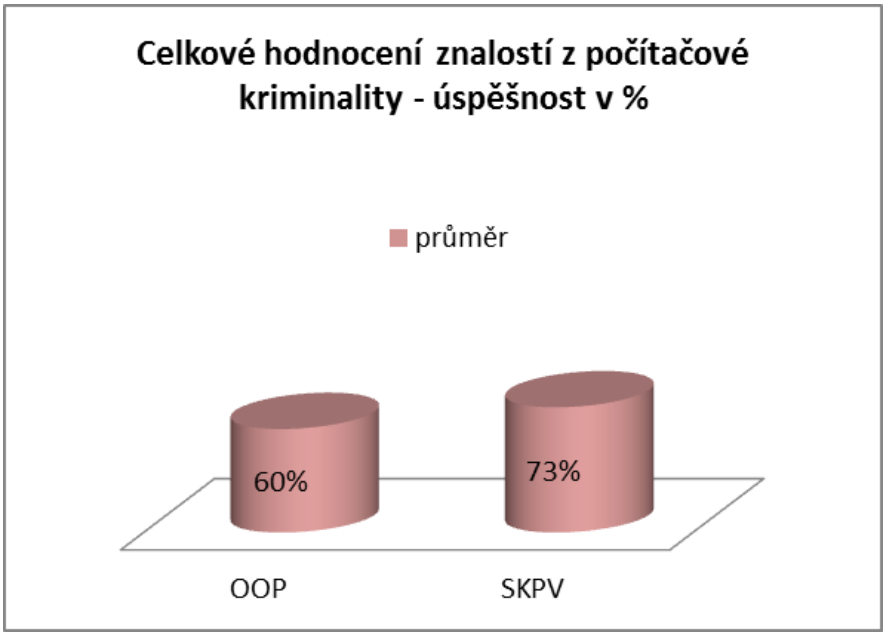
Tabulka 6 obsahuje celkové hodnocení znalostních otázek z oblasti znalostí pojmů a schopnosti kvalifikace trestných činů a způsobů a postupů při vyšetřování počítačové kriminality.

Na obvodních odděleních mají policisté znalosti v tomto oboru pouze z 60-ti procent. Mají tedy 60% základní znalost. Dokáží s 60-ti procentní pravděpodobností rozpoznat, zda se v případě oznámení jedná, či nejedná o počítačovou kriminalitu.

Policisté zařazení na oddělení služby kriminální policie mají znalosti v tomto oboru ze 73%. Jejich znalosti jsou o pouhých 13 % lepší než na znalosti policistů zařazených na obvodních odděleních.



Obrázek 11 – Celkové výsledky v testu ze znalostí počítačové kriminality



Obrázek 12 – Celkové hodnocení znalostí z počítačové kriminality – úspěšnost v %

Dotazovaní byli požádáni, aby odpovídali pouze sami, bez různých pomůcek a bez toho, aby odpověď vyhledávali v internetu, či v literatuře. K výše uvedeným zjištěným

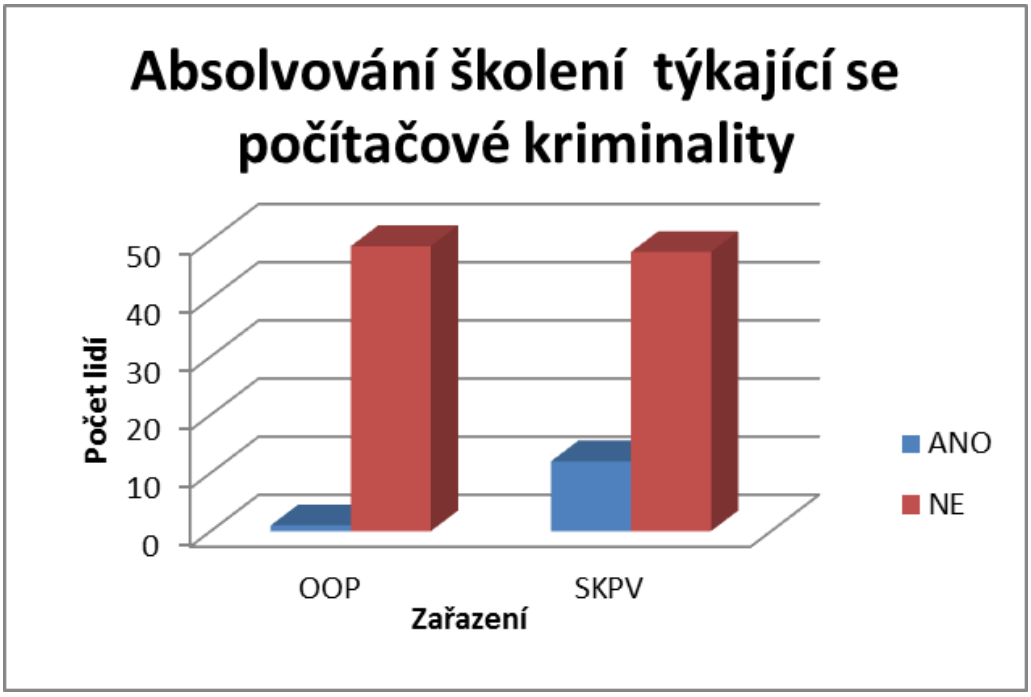
informacím je však nutno přidat i faktor strachu ze špatné odpovědi, který má každý člověk. Je nutno předpokládat, že ne všichni dotázaní policisté odpovídali pouze sami za sebe. Nejlepším příkladem tohoto je odpověď na otázku č. 13 a č. 14, která je závislá pouze na znalostech a není ji možno vyhledat. V tomto případě správně odpovědělo pouze 25% policistů zařazených na Obvodních odděleních a 47% policistů zařazených na oddělení služby kriminální policie.

Tyto výsledky jsou velmi alarmující, neboť, jak je uvedeno v kapitole 6 – Statistika, je prokázané, že počet případů počítačové kriminality má narůstající tendenci. Touto problematikou se tedy bude do budoucna muset zabývat s narůstajícím počtem i více policistů a proto je nutné, aby tito získali alespoň více než základní vědomosti a osvojili si základní postupy nutné k úspěšnému vyšetřování tohoto speciálního druhu kriminality.

Aby policisté získali potřebné znalosti, jsou organizována i školení, na kterých policisté, kteří se vyšetřováním počítačové kriminality zabývají již delší dobu, přednášejí policistům, kteří se s tímto vyšetřováním doposud nesetkali, a vysvětlují jim základní pojmy, nastiňují základní postupy vyšetřování, a hlavně vstupují do povědomí neznalých policistů, kteří je pak mohou v případě potřeby kontaktovat. Na těchto školeních nepřednášejí však pouze policisté, ale i přední odborníci zabývající se a působící v tomto druhu lidské činnosti. Dobrým příkladem mohou být zejména pracovníci společnosti Seznam.cz a.s., zástupci občanského sdružení E-bezpečí a podobně.

Tabulka 7 – Celkový počet policistů, kteří se zúčastnili školení v této oblasti

Zařazení	ANO	NE
OOP	1	49
SKPV	12	48



Obrázek 13 – Absolvování školení týkající se počítačové kriminality

Z celkového počtu dotázaných příslušníků zařazených na obvodním oddělení pouze 49 respondentů odpovědělo, že se takového školení nezúčastnilo a zúčastnil se pouze jeden policista. Ten uvedl, že toto školení mu přineslo mnoho užitečných informací.

Z celkového počtu příslušníků zařazených na oddělení služby kriminální policie odpovědělo 48 dotázaných, že se takového školení nezúčastnilo a 12 policistů odpovědělo, že se zúčastnilo.

Z uvedených zjištěných informací je patrné, že tato školení jsou přínosná, neboť komparací tabulky 7 a tabulky 6 vyjde najevo, že policisté zařazení na oddělení služby kriminální policie jsou, díky těmto školením, v tomto druhu kriminality více informovaní a mají lepší znalosti a to i přes to, že 67% z těch, kteří se školení zúčastnilo, uvedlo, že si nabyté znalosti již moc nepamatuje.

Pokud tedy na základě provedeného výzkumu bude požadováno odpovědět na základní otázku, stanovenou v úvodu této kapitoly, tedy: „Vědí policisté v České republice, co je to počítačová kriminalita a dokážou správně postupovat při přijímání trestního oznámení a následně při prověřování a vyšetřování tohoto specifického druhu trestné činnosti?“

Odpověď bude tedy na základě tohoto výzkumu znít: „Policisté v ČR mají základní povědomí o pojmu počítačový kriminalita, ale správně přijmout oznámení a následně provádět prověřování a vyšetřování je schopno pouze 35 % policistů.

Platnost pracovní hypotézy č. 1, tedy: „Policisté zařazení na Obvodním oddělení policie mají nižší znalosti z oboru počítačové kriminality než policisté zařazení na oddělení služby kriminální policie.“ Byla provedeným výzkumem rovněž potvrzena a to zejména tabulkou 6 a obrázkem 11 a 12.

Platnost hypotézy č. 2, tedy: „Policisté i přes svou nízkou informovanost, dokáží rozeznat počítačovou kriminalitu od ostatních druhů kriminality.“ Byla rovněž provedeným výzkumem potvrzena. Policisté svou neinformovanost a neznalost tohoto druhu kriminality řeší konzultací u problematiky znalých policistů.

Platnost hypotézy č. 3, tedy: „Policisté všeobecně neznají postupy při prověřování a následném vyšetřování počítačové kriminality.“ Byla spíše potvrzena, neboť provedeným výzkumem bylo zjištěno, že 25% policistů zařazených na obvodních odděleních a 47% policistů zařazených na oddělení služby kriminální policie by dokázalo uplatnit správné postupy a vést vyšetřování legálním a správným postupem do úspěšného cíle.

5 PREVENCE POČÍTAČOVÉ KRIMINALITY + VLASTNÍ NÁVRHY

Prevence počítačové kriminality, stejně jako prevence obecně, spočívá v eliminaci sociálně-patologických jevů. Snaží se snižovat příležitosti a omezovat motivy, které vedou člověka k páchání trestných činů. Do okruhu působnosti nepatří jen státní orgány a orgány činné v trestním řízení, ale i různá zájmová sdružení občanů, organizace, podnikatelské subjekty, ale i samotní občané.

Prevence je velmi důležitá pro úspěšný boj s tímto druhem trestné činnosti. Aby však byl boj státních orgánů, proti této kriminalitě, která je stejně závažná, jako ostatní druhy kriminality, úspěšný, musejí spolupůsobit dvě základní složky: Prevence a Represe.

Represe

Represí se rozumí jak odhalení pachatele trestného činu, tak i jeho následné potrestání, které je přiměřeně úměrné závažnosti činu, kterého se dopustil. Orgány činné v trestním řízení mají často velmi složitý úkol při odhalování pachatele trestného činu, jako fyzické osoby. V mnoha vyspělých zemích jsou zřizovány speciální skupiny a složky, které se odhalováním počítačové kriminality zabývají a jsou k tomuto úkolu vybaveny lepší technikou a zejména vyšším vzděláním v oboru informatiky. I tak je vyšetřování tohoto druhu kriminality velmi náročné a stává se, že některé trestné činy zůstanou neobjasněné a nepotrestané.

Největším problémem počítačové kriminality je skutečnost, že pachatel jako fyzická osoba není přítomna na místě spáchání činu. I když orgány činné v trestním řízení zjistí konkrétní počítač, ze kterého byla trestná činnost spáchána, lze jen velmi těžko ustanovit osobu, která počítač ke spáchání trestného činu použila.

Prevence

Orgány činné v trestním řízení se potýkají s mnohdy velmi složitým úkolem – odhalit pachatele. Aby v tomto boji byly úspěšné, a je třeba nejen působení represivní, ale

podstatné je i působení preventivní. Prevenci, podle jejího zaměření, lze v základu rozdělit na:

- Technologickou

Tímto pojmem se rozumí ochrana počítačových systémů, počítačových sítí a i samotných počítačů před hackerskými útoky. U technologií z pohledu hacker/správce systému platí, že ochrana technologií je vždy o krok pozadu za vývojem nástrojů a postupů vytvářených útočníky. Z tohoto důvodu je důležité, aby tato část prevence úzce navazovala na prevenci psychologickou, neboť samotná technologická prevence, i v případě, že odpovídá nejnovějším standardům a trendům není plně funkční, pokud selže lidský faktor.

- Psychologickou

Pod pojmem psychologická prevence je zahrnuto šíření informací mezi obyvatelstvo, a mezi pracovníky firem a společností. Informacemi, které je nutno mezi tyto uživatele internetu šířit jsou zejména příklady počítačové kriminality, tedy jaké trestné činy se dají pomocí internetu spáchat. Dále jsou to postupy, které útočníci používají k úspěšnému spáchání takové trestné činnosti. Jsou to informace o tom, jak může být internet a jeho neuvážené používání, nebezpečné. Zejména důležité je vštípit uživatelům internetu povědomí o tom, jak špatná a negativní je protizákonná činnost páchaná prostřednictvím internetu. Patří sem i varování uživatelů internetu, že všechny technické a softwarové ochrany nejsou dokonalé a že zkušený útočník je dokáže prolomit a proto je při používání internetu na místě opatrnost.

Dalším možností rozdělení prevence je rozdělení podle úrovně preventivních aktivit na Primární, Sekundární a Terciální prevenci.

Primární prevence je zaměřena zejména na aktivity vzdělávací, aktivity volného času, poradenské aktivity a osvětu, při které pozitivně působí na hodnotová měřítka lidí, zejména dětí a mládeže. Tato prevence je, nebo by měla být, uplatňována především v rodinách a školách.

Sekundární prevence je zaměřena na osoby, které jsou potencionálními pachateli, nebo obětmi trestné činnosti. Jedná se jedince, kteří patří do nějaké rizikové skupiny (drogově

závislí, osoby se speciální sociální péčí, a podobně). Snaží se působit zejména na vysvětlení a zjišťování kriminogenních situací a pozitivně ovlivňovat sociálně patologické faktory u takových jedinců.

Terciální prevence se snaží u již kriminálně narušených jedinců udržet výsledky a vliv předchozích pozitivních intervenčních vlivů. Snaží se socializovat takové jedince jejich začleněním do sociálně funkčního prostředí, nebo rekonstruovat sociálně nefunkční prostředí, ve kterém se tito jedinci pohybují.

5.1 Současný stav prevence

V současné době je preventivní působení v oblasti počítačové kriminality nedostačující. Policejní složky působí preventivně hlavně ve školství. Pořádají přednášky na základních i středních školách a učilištích. Zde je užívána zejména prevence psychologická. Studentům a žákům jsou přednášeny konkrétní příklady trestné činnosti, u kterých je kladen velký důraz na to, jaké následky taková trestná činnost přinesla obětem. Studenti jsou zejména nabádáni, aby při práci s internetem byly obezřetní a nesdělovali prostřednictvím internetu informace, které nejsou nezbytně nutné pro jejich činnost. Tuto preventivní činnost samozřejmě neprovádějí pouze policisté, ale i vyučující na těchto školách.

Asi nejznámějším projektem v oblasti prevence počítačové kriminality je projekt E-bezpečí, který provozuje Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci, na kterém spolupracují instituce jako Ministerstvo vnitra, Policie ČR, Olomoucký a Královehradecký kraj, Vodafone, Google, Seznam a další. Tento celorepublikový projekt je zaměřen na poradenství, prevenci, výzkum, vzdělávání a osvětu, související s nebezpečným a rizikovým používáním internetu a dalšími fenomény s touto problematikou souvisejícími.

5.2 Prevence ve firmách

Firmy a obchodní či výrobní společnosti a organizace jsou dnes již, až na malé procento výjimek, vybaveny informačními technologiemi a jen zřídka nejsou připojeny k internetu. Z tohoto důvodu je nutné preventivně působit i v tomto sektoru.

Jak již výše uvedeno k ochraně informačních a počítačových systémů nepostačí pouze vybavit organizaci nejnovější technologií, mezi které patří různý zabezpečovací hardware a software (antivirové programy, Firewally, apod.), ale je zde potřeba i prevence psychologické, u všech, ale zejména u klíčových zaměstnanců organizace. Každého takového zaměstnance je nutno řádně proškolit a poučit o možných následcích jeho rizikového chování. Toto proškolení by mělo být pravidelně opakováno. Je potřeba stanovit přesná bezpečnostní opatření a přesné postupy při zacházení s informacemi a technologiemi existenčně důležitými pro bezproblémový chod organizace. Veškerá důležitá data, která jsou uchovávána v organizaci je nutno ukládat v zašifrované podobě.

Významným opatřením je zavedení kontrolních mechanizmů, které neskrytě pravidelně, ale i skrytě náhodně prověřují funkčnost nastavených bezpečnostních opatření. Při zjištění porušení těchto pravidel, je důležité na toto porušení upozornit a vyvodit z něho příslušné důsledky.

Bezpečnostní software lze rozdělit na několik podskupin dle způsobu ochrany:

- **Zálohovací software**

  Je známo, že 94% firem, které se stanou obětí krádeže dat, anebo u nich dojde ke ztrátě důležitých dat, ukončí svou činnost do 3 měsíců od této ztráty, protože nejsou schopny v konkurenčním prostředí přežít. Pomocí zálohovacího software je možno takovým ztrátám předejít. Pro zálohování je možno využít zejména RAID, který patří spíše od hardwarové ochrany. Dále je možno využít velkého množství dostupných softwarových produktů pracujících na bázi Cloudu (DropBox, SugarSync, BOX a podobně), kdy se data ukládají na vzdálené uložiště. Nejčastěji doporučovaným programem na zálohování dat je pak Cobian Backup, který dokáže data zálohovat na stejném i vzdáleném PC a to i formou ftp přenosu.

- **Software pro šifrování dat a DLP** (Data loss prevention)

  Nástrojů pro šifrování je rovněž velké množství, ale asi nejznámějším a nejvyužívanějším je program TrueCrypt, který umožňuje vytvořit virtuální disk, na který se pak ukládají data pod silným šifrováním (metody šifrování: AES, Serpent a Twofish). Tato aplikace je volně stažitelná a je dostupná pro operační systém Windows, Linux ve všech jeho distribucích i pro IOS používaný na strojích Apple.

- **Software pro přístup k zařízením**

  Jsou to aplikace, které kontrolují přístup jiných zařízení k počítači, zejména přes datové vstupy/výstupy, jako je třeba USB, Bluetooth, IR a podobně. Zabraňují přístupu neoprávněných osob k datům v chráněném PC prostřednictvím jiných zařízení připojených k těmto vstupům.

- **Software pro správu a ochranu hesel**

  Tyto nástroje se používají pro ochranu přístupu k webovým stránkám, jako jsou e-shopy, internetová bankovnictví, e-maily a podobně. Slouží k zabezpečení přístupu uživatelů k těmto stránkám a zabránění neoprávněného přístupu osob k nim. Tyto nástroje rovněž mohou sloužit k řízení přístupu k zašifrovaným datům.

Pokud podniky, firmy a organizace, ale i běžní občané začnou používat výše uvedené nástroje a pokud zlepší svou gramotnost v oblasti výpočetní techniky a jejího fungování, bude prevence zvýšena na takovou míru, že k páchání trestné činnosti v této oblasti bude docházet jen ve speciálních případech a budou se jí dopouštět pouze odborníci ve svém oboru.

6 STATISTIKA NÁRŮSTU TRESTNÉ ČINNOSTI V POČÍTAČOVÉ KRIMINALITĚ

To, že je počítačová kriminalita u policie pojmem opravdu zcela novým dokazuje i samotný fakt, že policie si pro počítačovou trestnou činnost vede samostatné statistické údaje teprve od začátku roku 2011. Do tohoto časového zlomu byly veškeré trestné činy, které svou charakteristikou spadají do oblasti počítačové kriminality, zařazovány pod obecnou nebo hospodářskou trestnou činnost a nebyly nijak blíže rozlišovány. Z tohoto důvodu tedy nebylo možno zpracovat spolehlivé statistické údaje.

V následující tabulce je přehled celkového nárůstu počítačové trestné činnosti. Jedná se o trestné činy, které byly spáchány prostřednictvím internetové nebo jiné počítačové sítě.

Tabulka 8 - Přehled vykázaných trestných činů za jednotlivá čtvrtletí od počátku roku 2011 do 1. čtvrtletí 2013

	I. 2011	II. 2011	III. 2011	IV. 2011	I. 2012	II. 2012	III. 2012	IV. 2012	I. 2013
Násilí a vyhrožování proti skupinám osob a jednotlivců (§ 352)	0	2	2	3	0	0	1	2	1
Nebezpečné vyhrožování (§ 353)	8	15	19	22	12	15	19	30	4
Vydírání (§175)	8	13	16	24	5	17	23	28	5
Ohrožování mravnosti (§191)	5	7	7	7	7	12	12	14	5
Ostatní mravnostní trestné činy (§190, 192, 193, 194)	19	48	68	85	26	50	69	91	44
Podvod (§209)	168	386	573	874	345	627	888	1205	260
Ohrožování výchovy mládeže (§ 201, 202)	19	22	31	40	5	17	27	40	3
Tr. činy proti předpis. o nekalé soutěži (§ 248)	0	1	1	1	2	3	1	0	1
Poruš. autor. práv. k databázi (§ 270)	18	48	79	145	79	133	180	231	17
Poškoz. a zneuž. záznamu na nosiči info. (§231,2)	14	25	39	58	27	54	73	102	32
Nebezpečné pronásledování (§354)	9	19	16	23	13	15	25	33	5
Podněcování k rasové nenávisti (§356)	2	2	2	2	1	3	2	2	0
Neoprávněné nakládání s osobními údaji (§180)	0	0	1	2	2	4	1	3	1
Hanobení národa, rasy etnické a jiné skupiny (§355)	1	1	2	4	1	1	3	3	1
Porušování tajemství dopravovaných zpráv (§182)	0	4	5	6	2	3	5	5	1
Sexuální nátlak (§186)	0	0	0	0	0	2	2	12	0
Šíření poplašné zprávy (§357)	0	0	1	2	2	2	2	2	0

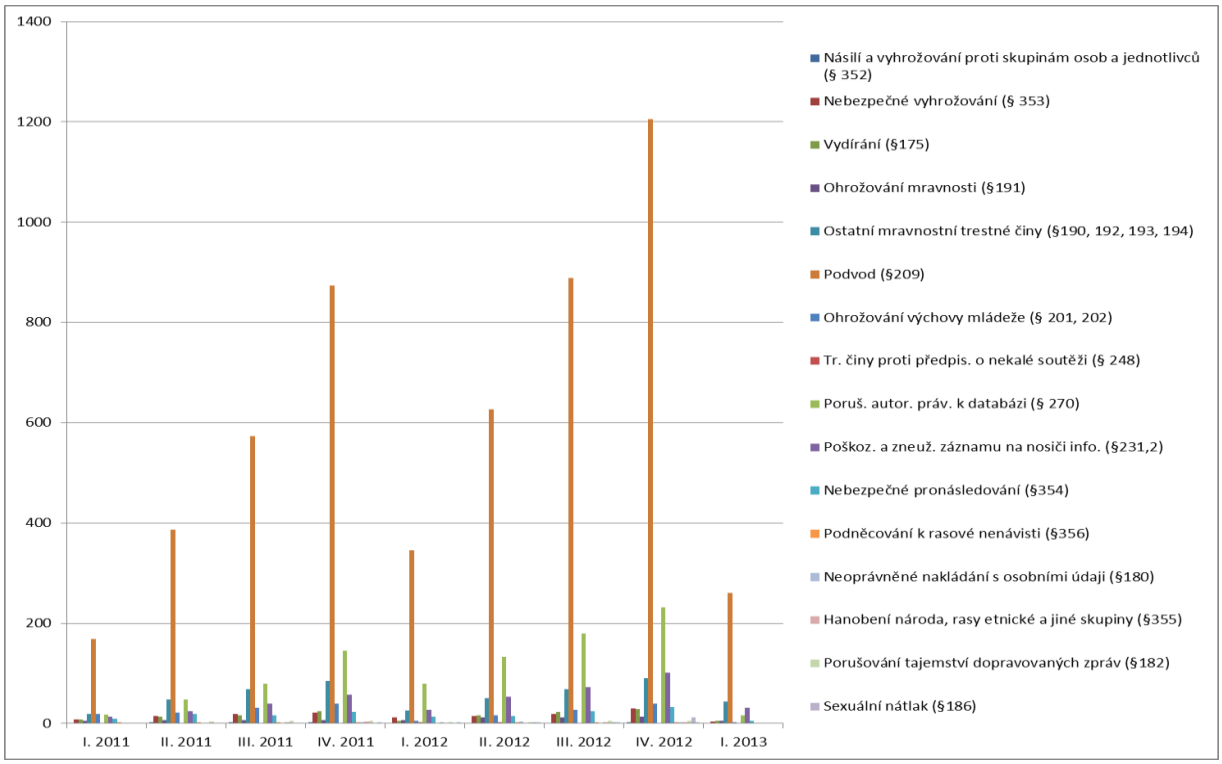
V tabulce je zahrnut i rok 2013, avšak zde byly v době zpracování práce k dispozici pouze údaje za měsíce leden a únor, tedy ne celé čtvrtletí. Uvedená čísla v jednotlivých sloupcích (čtvrtletích) vyjadřují nárůst vykázaných trestných činů od začátku kalendářního roku. Tedy IV. Čtvrtletí je součtem vykázaných trestných činů za celý rok.

Zajímavé je i zjištění, jak se trestná činnost vyvíjí v průběhu jednoho roku. Následující tabulka zobrazuje nárůst vykázaných trestných činů a tedy i nárůst trestné činnosti v průběhu roku 2011.

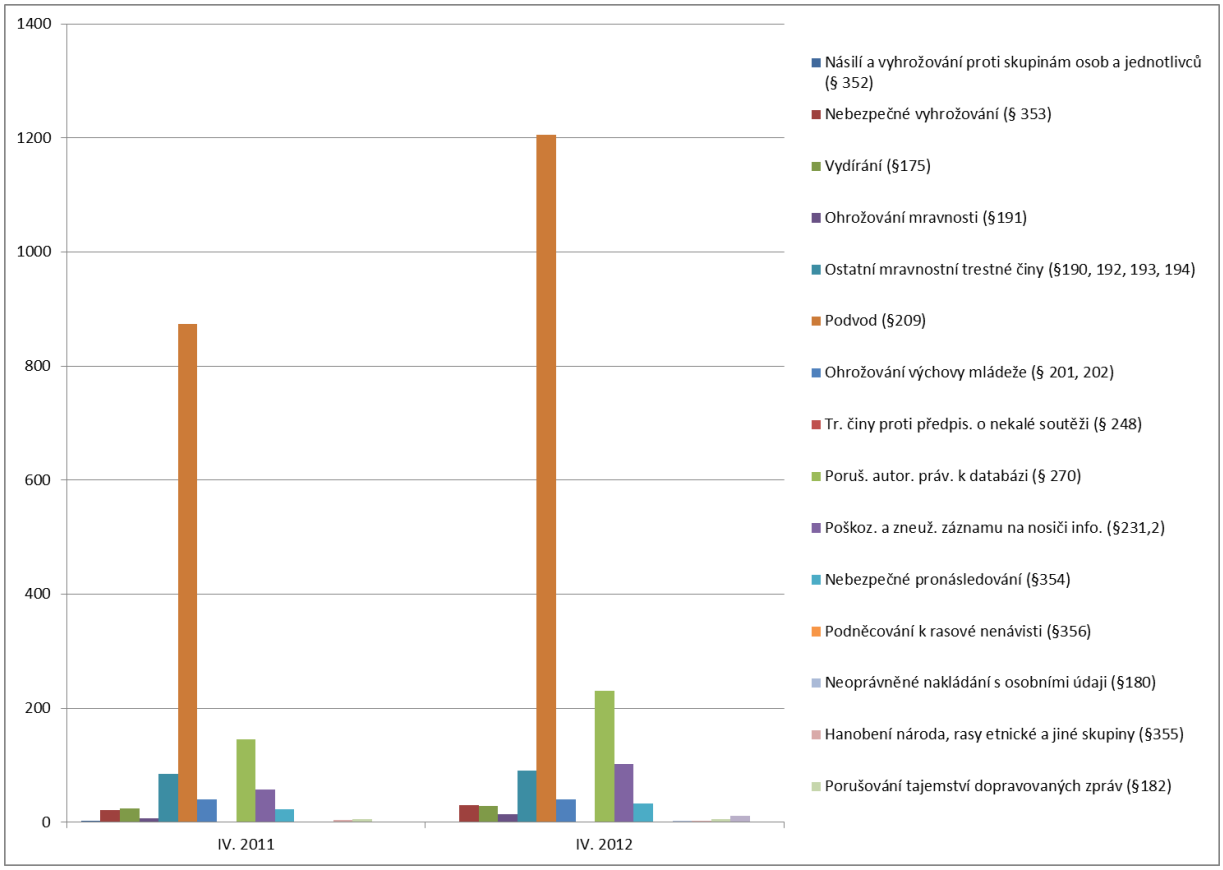
Tabulka 9 - Nárůst trestné činnosti za rok 2011 (po měsících)

Rok 2011	Nárůst trestné činnosti												
Trestný čin	Leden	Únor	Březen	Duben	Květen	Červen	Červenec	Srpen	Září	Říjen	Listopad	Prosinec	Celkem
Násilí a vyhrožování proti skupinám osob a jednotlivců (§ 352)	1	1	0	1	2	2	2	2	2	3	2	3	21
Nebezpečné vyhrožování (§ 353)	2	7	8	10	13	15	18	20	19	20	21	22	175
Vydírání (§175)	1	7	8	9	10	13	13	15	16	19	22	24	157
Ohrožování mravnosti (§191)	3	4	5	5	6	7	9	8	7	8	7	7	76
Ostatní mravnostní trestné činy (§190, 192, 193, 194)	2	16	19	23	36	48	52	59	68	74	79	85	561
Podvod (§209)	47	80	168	233	300	386	428	498	573	683	780	874	5050
Ohrožování výchovy mládeže (§ 201, 202)	1	16	19	19	19	22	24	29	31	33	35	40	288
Tr. činy proti předpis. o nekalé soutěži (§ 248)	2	2	0	1	1	1	1	1	1	2	2	1	15
Poruš. autor. práv. k databázi (§ 270)	6	13	18	23	41	48	60	64	79	93	133	145	723
Poškoz. a zneuž. záznamu na nosiči info. (§231,2)	3	5	14	16	18	25	28	32	39	47	54	58	339
Nebezpečné pronásledování (§354)	0	3	9	15	18	19	19	18	16	18	21	23	179
Podněcování k rasové nenávisti (§356)	0	1	2	2	1	2	2	2	2	2	2	2	20
Neoprávněné nakládání s osobními údaji (§180)	0	1	0	1	0	0	0	1	1	1	1	2	8
Hanobení národa, rasy etnické a jiné skupiny (§355)	0	0	1	1	1	1	1	2	2	3	4	4	20
Porušování tajemství dopravovaných zpráv (§182)	0	0	0	2	0	4	5	6	5	5	5	6	38

Následující dva grafy dokazují tvrzení uvedené v úvodní části, tedy že počet spáchaných trestných činů v oblasti počítačové kriminality má narůstající tendenci.

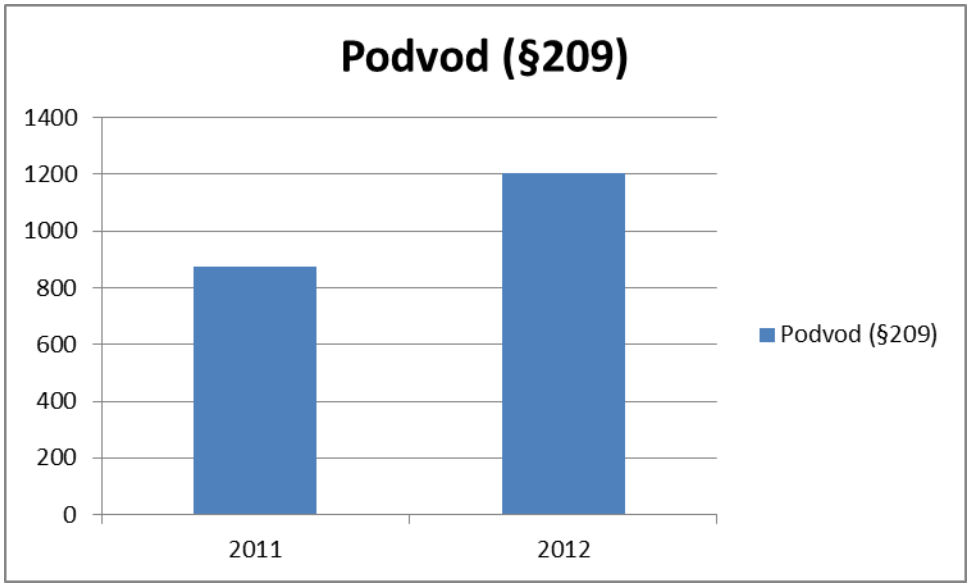


Obrázek 14 - Graf nárůstu trestné činnosti za období 2011 – 2012



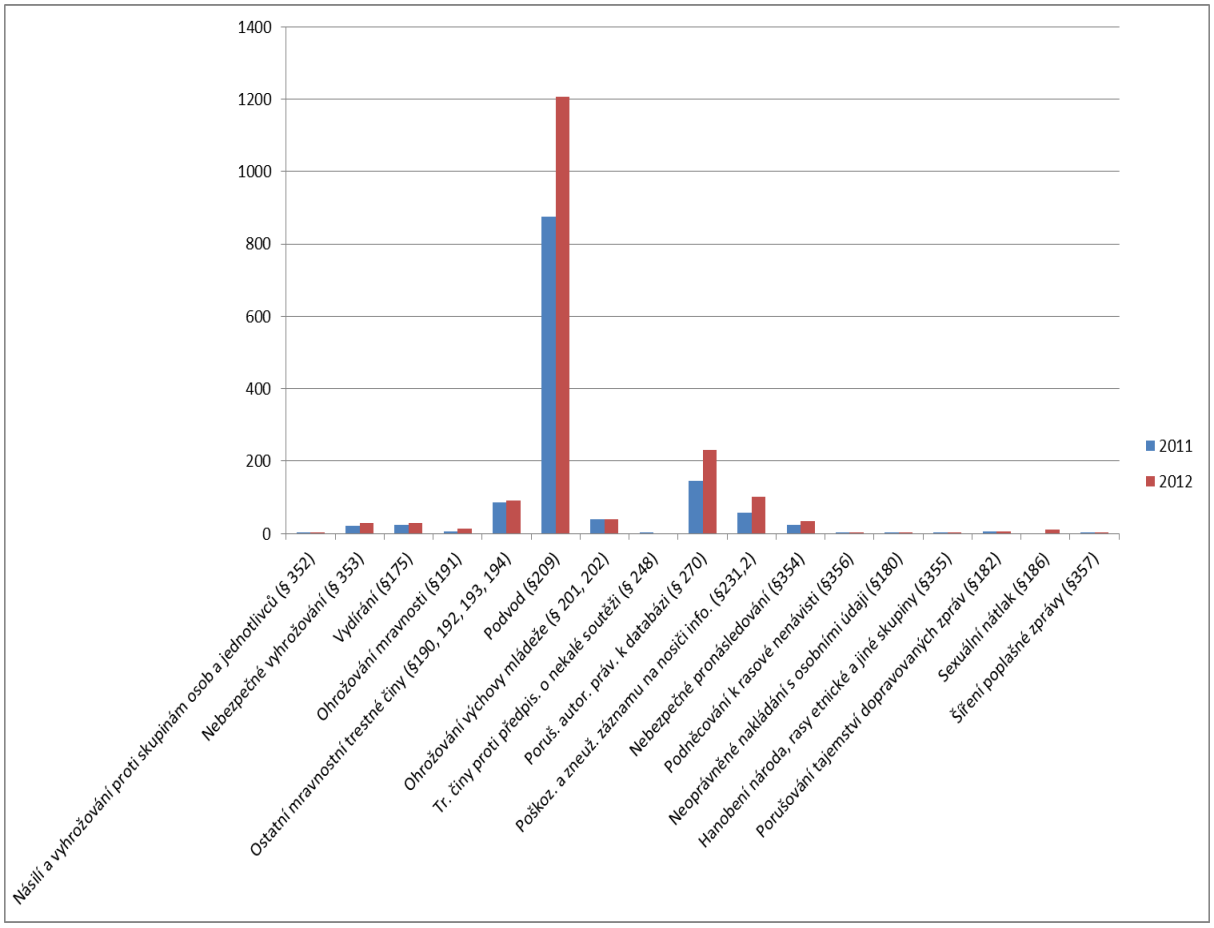
Obrázek 15 - Srovnání trestné činnosti za roky 2011 a 2012 – Nárůst kriminality

Za rok 2011 bylo vykázáno celkem 874 spáchaných trestných činů Podvod dle ust. §209 tr. zákoníku, kdežto o rok později již těchto trestných činů bylo vykázáno 1205.



Obrázek 16 - Nárůst trestného činu Podvod (§209 tr. zákoníku)

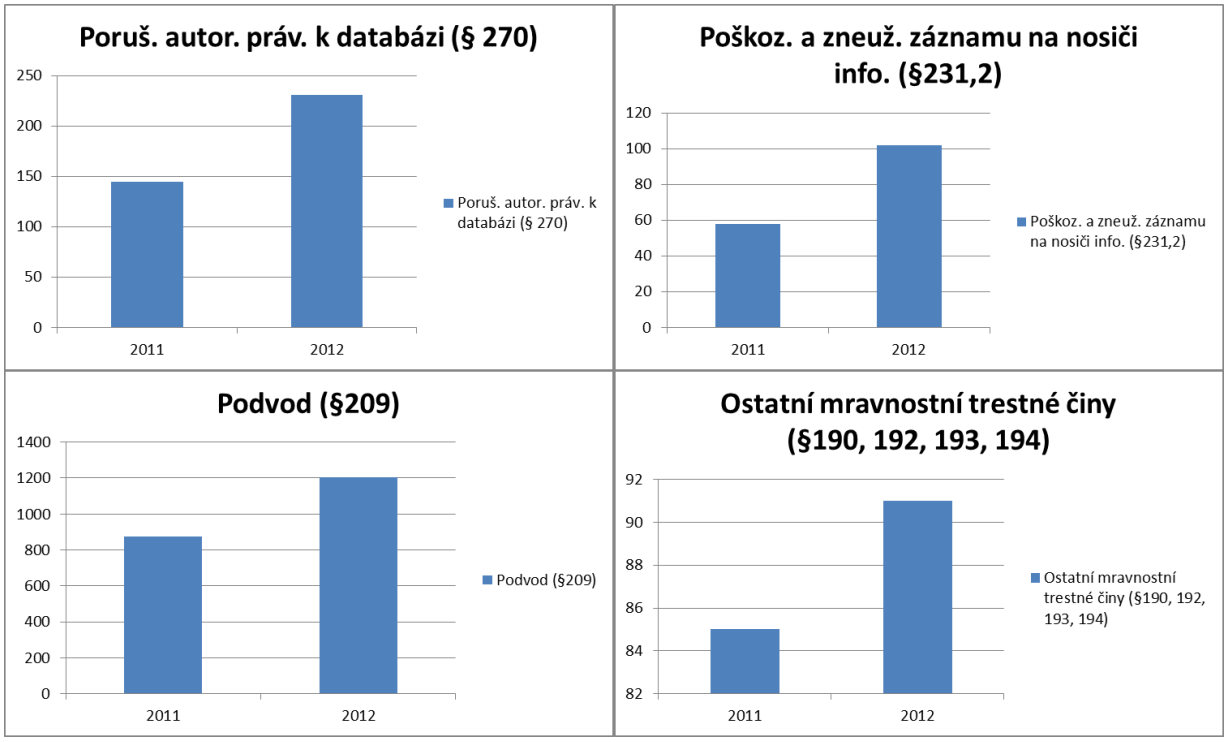
Stejnou vzrůstající tendenci má i většina ostatních nejčastěji vyšetřovaných trestných činů, což dokazuje následující graf.



Obrázek 17 - Porovnání jednotlivých trestných činů za roky 2011 a 2012

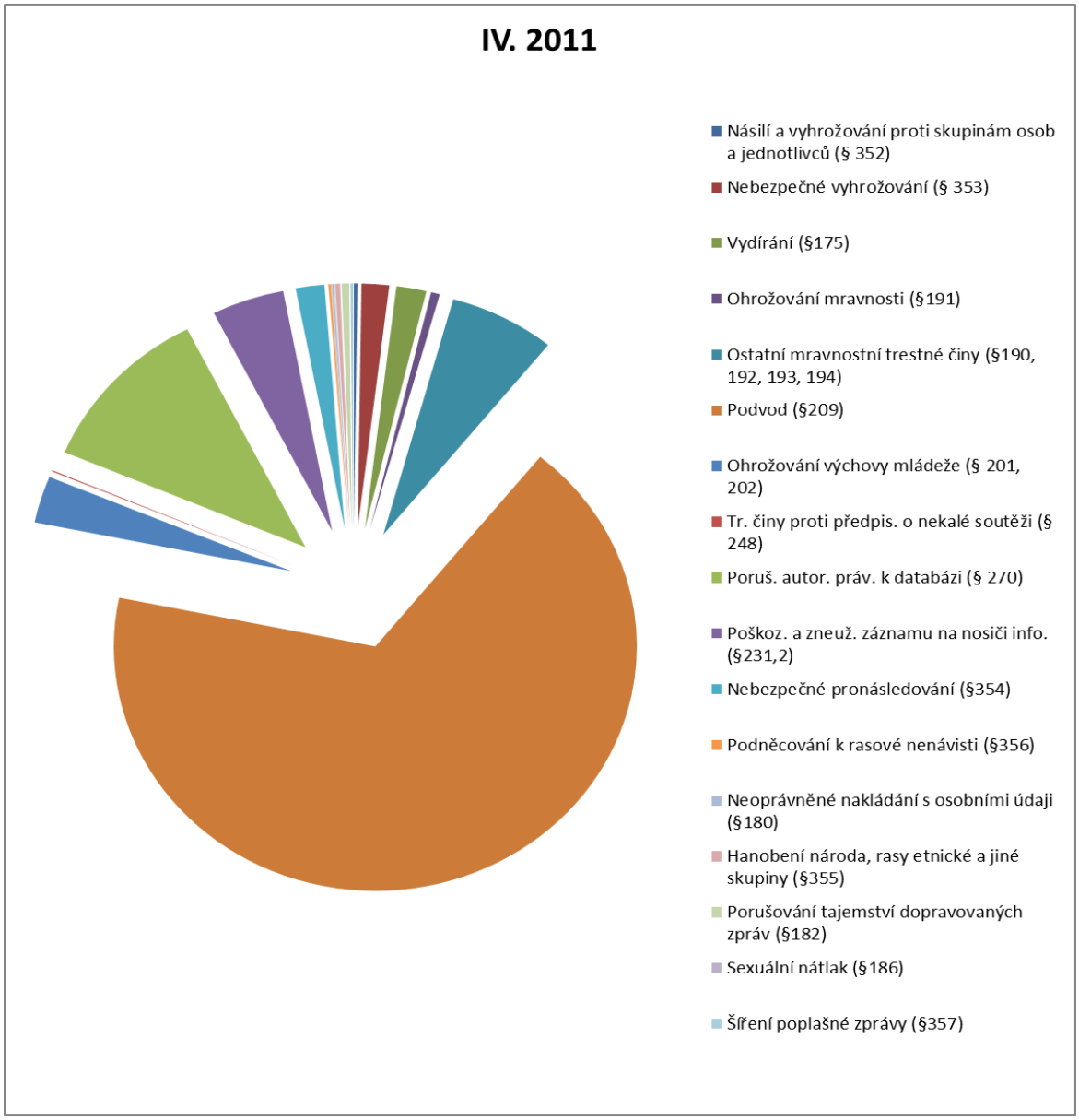
Nejčastějšími trestnými činy, které Policie České republiky vyšetřuje, a které spadají do oblasti Počítačové kriminality, jsou zejména trestný čin Podvod dle ust. §209 tr. zákoníku, Porušování autorských práv, práv souvisejících s právem autorským a práv k databázi dle ust. §270 tr. zákoníku, Mravnostní trestné činy jako jsou Výroba a jiné nakládání s dětskou pornografií (§192 tr. zákoníku), Svádění k pohlavnímu styku (§202 tr. zákoníku), Ohrožování výchovy dítěte (§201 tr. zákoníku) a další, ale také trestné činy Nebezpečné vyhrožování dle ust. §353 tr. zákoníku) a Nebezpečné pronásledování dle ust. §354 tr. zákoníku.

I tyto trestné činy, pokud jsou porovnány za jednotlivá období, tedy pokud jsou porovnána za jednotlivé roky, vykazují opět vzrůstající tendenci.

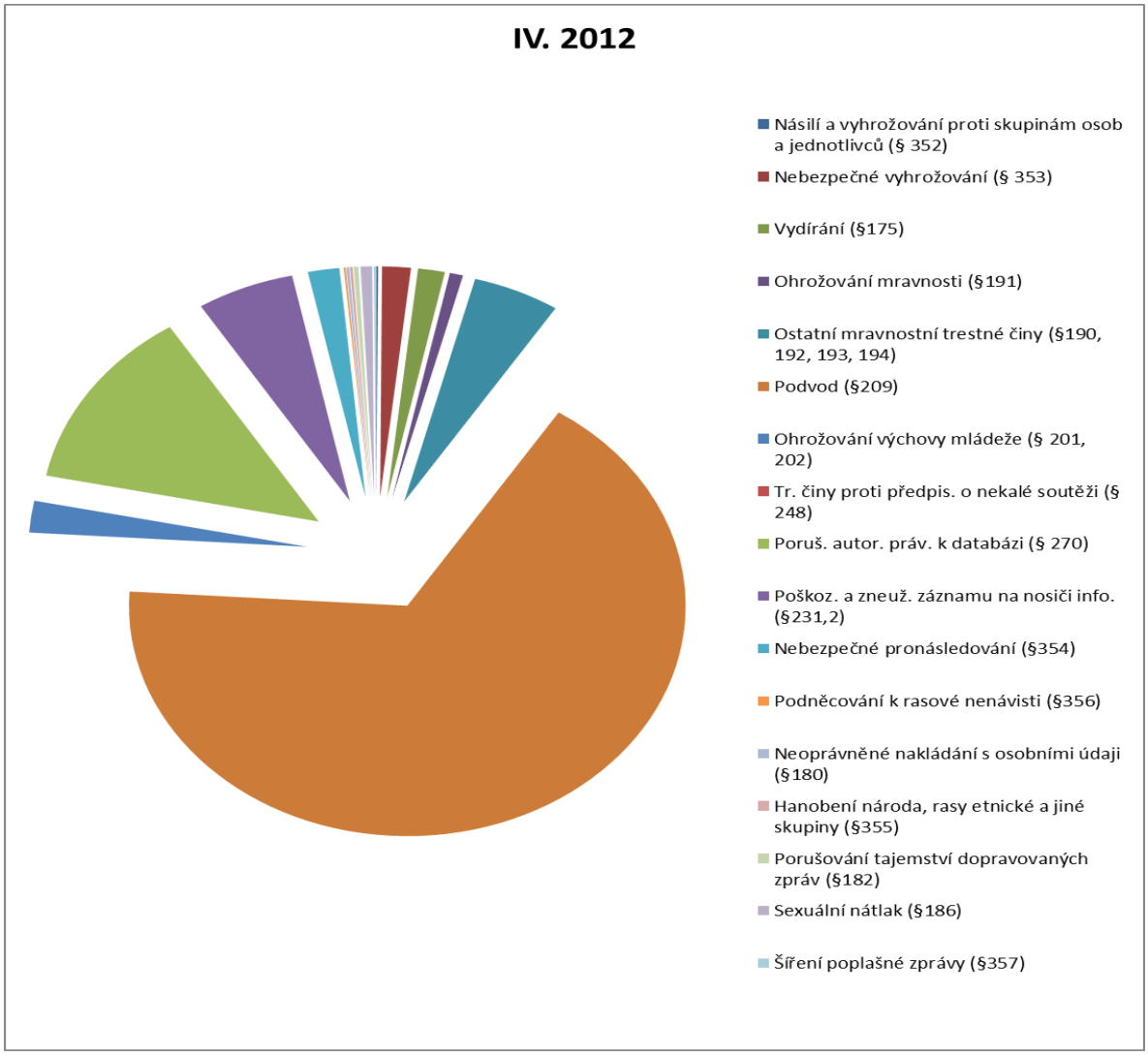


Obrázek 18 - Porovnání jednotlivých vykázaných trestných činů za roky 2011 a 2012

Poměrné zastoupení jednotlivých trestných činů je znázorněno na následujících dvou grafech.



Obrázek 19 - Četnost jednotlivých trestných činů v celkovém počtu počítačové kriminality za rok 2011



Obrázek 20 - Četnost jednotlivých trestných činů v celkovém počtu počítačové kriminality za rok 2012

Porovnáním výše uvedených grafů je patrné, že zastoupení jednotlivých trestných činů v celkovém nápadu trestné činnosti v oblasti počítačové kriminality se příliš nemění.

7 VLASTNÍ NÁVRH LEGISLATIVNÍHO CHARAKTERU

Na základě výše popsaných postupů prověřování a vyšetřování počítačové kriminality je patrné, že některé z těchto postupů jsou poměrně složité a hlavně zdlouhavé. Vyšetřování tak trvá i půl roku, v některých případech i rok. Časově nejnáročnějším je postup při vyžadování informací na základě soudem vydaného příkazu dle ust. §88a tr. řádu, které se po novele tohoto zákonného ustanovení protáhlo o další čas nutný k podání návrhu státnímu zástupci a ne přímo k soudu, jak tomu bylo do vydání uvedené novely.

Vyšetřovatelé se často při vyšetřování setkávají i s tím, že soud odmítne vydat příkaz dle ust. §88a tr. řádu pro více subjektů a vydá jej pouze pro jeden konkrétní a pak je nutno takový postup opakovat až do získání požadovaných informací.

Příklad: (ideální stav – zjišťovaná IP adresa je přidělena přímo konkrétní osobě):

Bylo podáno trestní oznámení z podezření ze spáchání podvodu prostřednictvím internetu, kdy neznámý pachatel na internetových inzertních stránkách www.sbazar.cz vystavil inzerát, ve kterém nabídl k prodeji notebook, jehož prodejní cena činila 25.000,- Kč. Na inzerát zareagoval kupující, který na v inzerátu uvedenou e-mailovou schránku, odepsal, že má o zboží zájem. Prodejce mu ze své schránky odpověděl, aby mu kupující poslal na jeho účet peníze předem s tím, že jakmile bude transakce provedena on mu pak zašle nabízené zboží. Kupující tedy ze svého účtu provedl převod a čekal na zboží. Když mu toto po týdnu nepřicházelo, pokusil se na uvedeném e-mailu kontaktovat prodejce, který však již nereagoval. Kupující se proto dostavil na nejbližší oddělení policie k podání trestního oznámení, které zde bylo přijato.

Případ dostal přidělen policista, který na základě získaných informací následně požádal oznamovatele o spolupráci, kdy z hlaviček přijatých e-mailových zpráv zjistil IP adresu odesilatele. Na stránkách www.ripe.net zjistil, že IP adresa patří do adresního rozsahu společnosti XY. Proto dle stanoveného postupu sepsal návrh na vyžádání informací dle ust. §88a tr. řádu a tento zaslal Okresnímu státnímu zastupitelství (dále jen OSZ). Doručení návrhu na OSZ trvalo 4 dny. Státní zástupce, který spis dozoroval, obdržel tento návrh a začal studovat trestní spis, aby vyhodnotil, zda je tento návrh oprávněný a zda tedy i on může vydat Žádost o vydání příkazu dle ust. §88a tr. řádu soudu. Prostudování spisu spolu

s vydáním žádosti a jejím doručením k soudu trvalo 7 dní. Okresní soud, po přijetí žádosti o vydání příkazu, přidělil tuto žádost konkrétnímu soudci, který následně musel ve svém rozvrhu najít čas a prostudoval opět celý spisový materiál, aby tak i on posoudil oprávněnost žádosti. To trvalo dalších 10 dní. Následně soudce vydal příkaz, který odeslal spolu se spisem zpět na OSZ. OSZ po obdržení příkazu a spisového materiálu tento odeslalo vyšetřujícímu policistovi. Toto trvalo dalších 5 dní. Policista po obdržení soudního příkazu musel zkontrolovat, zda jsou v soudním příkazu uvedena všechna data správně, neboť i zde dochází k překlepům, a následně odeslal tento příkaz Oddělení zvláštních činností policie (dále jen ÚZČ), které jediné má právo takový příkaz uplatnit u dožadované společnosti. ÚZČ soudní příkaz přijalo a následně jej se svým průvodním dopisem odeslalo dotčené společnosti poskytující internetové připojení. Toto trvalo 10 dní. Společnost soudní příkaz obdržela, vypracovala odpověď a tuto odeslala zpět na ÚZČ. ÚZČ odpověď vyhodnotilo, zda je dostatečná vzhledem k příkazu soudu a odeslalo jej dožadujícímu policistovi. Toto trvalo 14 dní. Celkový čas, který je třeba k provedení zjištění osoby, či zařízení, kterému je přidělena konkrétní IP adresa, je tedy 45 dní!!!

V neideálním případě je počáteční stav totožný s předcházejícím případem, avšak na základě takto získaných informací je zjištěno, že IP adresa je poskytovatelem poskytnuta další, menší společnosti, lokálnímu poskytovateli internetového připojení. Tedy celý proces je nutno znovu opakovat. Znovu dalších 45 dní, které jsou třeba ke zjištění již konkrétní osoby. Policisté, kteří se s takovým případem již setkali, se pokusili tento čas zkrátit tím, že navrhli OSZ, aby vyžádal soudní příkaz na konkrétní společnost a všechny další společnosti poskytující internetové připojení, které byly tímto postupem zjištěny. V mnoha případech tento postup byl zamítnut jako neoprávněný a nezbylo než celý proces podstoupit znovu a opakovaně.

Zde tedy, jak bylo již uvedeno v úvodu této práce, dochází k průtahům trestního řízení, které někdy bývá označováno (neprávem) jako neodůvodněné.

Další skutečností je, že policie musí proplatit osloveným společnostem poskytujícím připojení k internetu jejich účelně vynaložené náklady ke zpracování takto vyžádané informace. Společnosti si tak účtují práci pracovníka, který vyžádané informace zpracoval, papír, opotřebení techniky a další položky.

Vzhledem k výše uvedenému došlo a dochází ke zbytečným prodlevám při vyšetřování a nárůstu nákladů na získání takových informací. Vyvstává zde tedy otázka, zda by toto zbytečné prodlužování vyšetřování nebylo možno nějak odstranit. Nabízí se zde poměrně jednoduché řešení. Takovým řešením by mohl být návrh národní databáze, do které by jednotliví, ať již velcí, či lokální poskytovatelé internetového připojení vkládali jednotlivé IP adresy a k nim i osoby, či zařízení, kterým je tato IP adresa přidělována. Existencí takové databáze by bylo možno zkrátit průběh mnoha prověřovaných i vyšetřovaných věcí o nejméně 45 dní a samozřejmě by policii odpadly poplatky za účelně vynaložené náklady, které musí policie platit právě providerům za výše popsaným způsobem získávané informace.

7.1 Návrh podoby databáze IP adres

Aby taková databáze byla co nejlépe využitelná, bylo by vhodné, aby obsahovala tyto klíčové informace:

- IP adresa
- Zobrazení adresního rozsahu, do kterého IP patří
- Jméno provozovatele internetového připojení (dále jen ISP), který má uvedený adresní rozsah ve své správě
- Kontakt na ISP (telefonický, e-mailový, poštovní adresa sídla ISP)
- Jméno lokálního poskytovatele (pokud je mu předmětná IP adresa přidělena)
- Kontakty na lokálního poskytovatele (telefon, e-mail, poštovní adresa sídla)
- Rozlišení zda je IP adresa přidělena zařízení (router, switch, AP apod.) či konkrétnímu PC
- Jméno osoby, které je IP adresa přidělena na základě smlouvy s koncovým odběratelem internetového připojení
- Kontakty na takovou osobu (telefon, e-mail, adresa bydliště uživatele)

- Adresa umístění přípojky (tedy místa, kde je umístěno zařízení, kterému je IP adresa přidělena)

- Informace o zařízení, kterému je IP adresa přidělena (router, AP, switch apod.) obsahovala by informace typu: Zařízení je v režimu DHCP, NAT 1:1, NAT 1:N a podobně, čímž by bylo pro tazatele jednoduché pak napsat konkrétní žádost směřovanou samotnému ISP o poskytnutí LOGu.

7.2 Přístup k databázi

V České republice již existují podobné databáze. Jedná se zejména o databázi nazývanou Centrální registr obyvatelstva, dále pak o Centrální registr vozidel a podobnou databází je i databáze Rejstříku trestů, případně databáze Katastru nemovitostí. V takových databázích jsou uvedeny i poměrně citlivé osobní informace. Přístup k nim je upraven v příslušných předpisech tak, aby byl v souladu se zákonem na ochranu osobních údajů.

Policie má v současné době přístup právě do všech výše zmiňovaných databází a to v souladu se zákonem na ochranu osobních údajů. Každý policista je řádně a prokazatelně poučen a proškolen, jak s informacemi takto získanými smí nakládat, za jakých podmínek je smí z databází získávat. Porušení těchto podmínek je velice přísně trestáno. Policista, který potřebuje pro úspěšné plnění úkolů v trestním řízení získat konkrétní informaci z takové databáze, musí při dotazu uvést číslo jednací spisového materiálu, pro který takový dotaz činí. Toto se následně náhodně zpětně kontroluje jak kontrolními orgány policie ČR, tak kontrolními orgány GIBS, tak i kontrolními orgány Úřadu pro ochranu osobních údajů.

Stejné podmínky by se týkaly i navrhované databáze IP adres. Databáze by samozřejmě tak jako ostatní jmenované, byla spravována příslušnými úřady a ty by měly i kontrolu na přístupy jednotlivých tazatelů.

Do navrhované databáze by měli přístup i jednotliví ISP, ale tento jejich přístup by byl omezený pouze na vkládání, tedy zápis dat. Možnost editace by jim byl také umožněn, ale pouze nad daty, která do databáze sami předtím vložili, a tuto editaci by měli za povinnost řádně odůvodnit.

ISP by neměl přístup k informacím jiným, než sám zadal, aby se tak zabránilo nekalé obchodní soutěži.

7.3 Propojení databází s ostatními databázemi ČR

Navrhovaná databáze by mohla být propojena i například s centrálním registrem obyvatel, kdy například pokud by po dotazu do databáze IP adres bylo na výstupu jako odpověď získáno jméno konkrétní osoby, byla by na výstupní stránce nabídnuta i možnost vyhledání takové osoby v Centrálním registru obyvatel. Dalším příkladem propojení databází by mohlo být propojení adresy přípojky internetu s databází Katastru nemovitostí, kdy by se na požadavek zobrazila mapa s přesným umístěním internetové přípojky.

7.4 Vymahatelnost

Je samozřejmostí, že jednotliví poskytovatelé internetového připojení by neměli zájem a ani chuť informace do takové databáze vkládat a proto by bylo na místě stanovit institut vymáhání takové povinnosti. Ten by byl určen zejména možností udělit za nedodržování této povinnosti příslušnou pokutu a při opakovaném zjištění nedodržování této povinnosti i zastavením podnikatelské činnosti.

Na dodržování této činnosti by bylo nutno zřídit nějaký oprávněný orgán k provádění kontrolní činnosti. Tímto orgánem by mohla být například Česká obchodní inspekce, která již v současné době dbá nad dodržováním podmínek stanovených obchodním zákonem a příslušnými vyhláškami. Dalším orgánem, který by byl oprávněn takovou kontrolní činnost provádět, by mohl být Živnostenský úřad, který jako jednu ze svých činností má i dohled nad dodržováním pravidel podnikání v ČR. Nebylo by tedy nutno zřizovat úplně nový kontrolní orgán, ale využít již stávající kontrolní mechanizmy.

7.5 Zhodnocení

Vytvoření navrhované databáze by urychlilo většinu vyšetřovacích postupů v případech prověřování a vyšetřování počítačové kriminality a tím by přispělo k rychlému dopadení pachatele. Snížilo by se tak i finanční zatížení policie, neboť by již nebylo nutno platit Účelně vynaložené náklady na získání informací.

Samozřejmě je nutno počítat i s protichůdnými názory. Bylo by možno namítat, že díky vybudování takové databáze by již internet ztratil svou současnou anonymní podobu. Tato anonymita by však nebyla nikterak snížena. Nijak by nebyla dotčena základní práva občanů, neboť ta by byla zaručena zákonem na ochranu osobních údajů a nastavenými kontrolními mechanizmy. Stejně tak by nebyla dotčena ani práva společností provozujících internetové připojení. Těm by pouze přibyla jedna povinnost – vkládat údaje o IP adresách do databáze. Kontrolní činností by se zabývaly již stávající úřady, tedy by nebylo nutno zřizovat úřad nový.

Z výše uvedeného je patrné, že ani zřízení takové databáze by nebylo finančně nedosažitelné. Náklady na zřízení databáze by se týkaly pouze technického řešení serveru, na kterém by uvedená databáze byla provozována. Dále by bylo nutno vzít v úvahu náklady nutné na vybudování softwarové základny, kdy by bylo možno využít stávajících produktů a pouze je patřičně upravit. Co se kontrolních činností týče, bylo by nutné na zvolený kontrolní úřad přijmout pracovníka, který má dobré znalosti v tomto oboru, který by zaškolil všechny stávající pracovníky.

Vzhledem k tomu, že částka ušetřená díky vzniku a provozu této databáze by rozhodně překročila náklady nutné k jejímu vybudování, je dán předpoklad, že tento návrh by byl nejen přínosem pro bezpečnost občanů a posílení jejich důvěry v orgány činné v trestním řízení, ale byl by i ekonomicky nenáročný a tedy proveditelný.

Vybudování této databáze by zabralo určitý čas nutný k pořízení techniky a proškolení kontrolních orgánů a následnému naplnění databáze samotné. Tento časový úsek by však nebyl delší než 1 rok.

ZÁVĚR

V práci orgánů činných v trestním řízení často dochází k průtahům v trestním řízení, které jsou často státními zástupci označovány jako neodůvodněné průtahy trestního řízení. Ve většině případů se však nejedná o neodůvodněné průtahy. Jedná se zejména o zastaralé způsoby získávání informací od třetích stran, které jsou rovněž účastníky trestního řízení.

Jedním z cílů této diplomové práce tedy bylo navrhnout postupy, kterými by se práce orgánů činných v trestním řízení zrychlila a zjednodušila.

Dalším cílem práce bylo ověřit tvrzení autora této práce, že policisté zařazeni na základních útvarech policie ČR nemají dostatečné znalosti v oblasti počítačové kriminality, týkající se znalosti základních pojmů, způsobů vyšetřování a přijímání trestního oznámení a navrhnout možnou nápravu tohoto stavu.

Dílčím, vedlejším cílem bylo vytvořit metodiku použitelnou orgány činnými v trestním řízení, která by vysvětlovala základní pojmy, jejichž znalost je nutná k úspěšnému vedení trestního řízení, upřesňovala základní postupy používané při prověřování a vyšetřování trestné činnosti. Dále uvést policisty neznalé základních termínů a pojmů z oboru počítačové techniky a počítačové kriminality do tohoto oboru a popsat základní způsoby prověřování a vyšetřování tohoto druhu kriminality.

Všechny uvedené cíle byly splněny a to za použití vlastních znalostí autora, získaných jak studiem na Fakultě aplikované informatiky Univerzity Tomáše Bati ve Zlíně, tak i informací a zkušeností získaných z vlastní dlouholeté praxe, kdy autor pracuje jako vyšetřovatel, jehož zaměřením je právě počítačová a internetová kriminalita, stejně jako informací získaných studiem použité literatury. Další použitou metodou byla metoda výzkumu mezi policisty Územního odboru Hodonín. Pro tento výzkum byla zvolena kvantitativní strategie, za použití deduktivní metody, která vychází z teorie, nebo obecně formulovaného problému. Byla použita základní deduktivní metoda provedená formou dotazníkového šetření.

Tímto výzkumem byly ověřeny všechny pracovní hypotézy, tedy, že policisté mají pouze základní povědomí o pojmu počítačová kriminalita, že dokáží, samostatně a ve složitějších případech po konzultaci, správně přijmout trestní oznámení a konečně že spíše

nedokáží samostatně prověřovat a vyšetřovat trestnou činnost v oblasti počítačové kriminality a potřebují radu či konzultaci svých zkušenějších kolegů.

V této práci bylo navrženo a rozpracováno vytvoření národní databáze IP adres, jejíž existence by značnou měrou přispěla k urychlení a zjednodušení práce orgánů činných v trestním řízení a zejména k odstranění průtahů v trestním řízení získáváním informací od třetích stran – účastníků trestního řízení – formou dotazů do této autorem navrhované databáze IP adres.

Dalším cílem této práce bylo provést analýzu preventivních opatření v oblasti počítačové kriminality a popřípadě navrhnout zlepšení stávajících anebo vytvoření nových preventivních opatření za účelem zlepšení stavu v této oblasti. Tento cíl byl rovněž splněn. Byla provedena analýza současného stavu preventivních opatření a na jejím základě byly následně doporučeny základní metody prevence a rozšíření stávajících metod, jejichž důsledným používáním a dodržováním by bylo minimalizována hrozba počítačové kriminality na nejnižší možnou míru.

CONSLUSION

The work of law enforcement management often leads to delays in criminal proceedings; prosecutors are often referred them as unjustified delay criminal proceedings. In most cases there are not unreasonable delays. In particular outdated ways of obtaining information from third parties there are also parties to the criminal proceedings.

One of the main aims of that Diploma thesis was to design procedures that would work with law enforcement control speed and ease.

Another goal was to verify the claim of the author of this work that officers assigned to the basic police departments do not have sufficient knowledge in the field of cybercrime, concerning the knowledge of basic concepts, methods of investigation and receiving the complaint and suggest a possible remedy for this condition.

Another objective was to develop methodology applicable law enforcement authorities in criminal proceedings, which would explain the basic concepts, knowledge of which is necessary for the successful conduct of criminal proceedings, provided the basic procedures used in the examination and investigation of crime. In addition, state police ignorant of basic terms and concepts in the field of computer engineering and computer crime in this field and sleep in basic means of examining and investigating this type of crime.

All of these objectives were met and using their own knowledge of the author, obtained as studying at the Faculty of Applied Informatics of Tomas Bata University in Zlín, as well as information and experience gained from its own long-standing practice, the author works as an investigator, whose focus is on The Computer and Internet crime, as well as information derived from the study of literature. Another used method was the research among the officers of the Territorial Department in Hodonín. That research was focused on quantitative strategy, using deductive methods, based on theory, or generally formulated problem. There was used the basic form of the structured interview questionnaire.

This research was verified all working hypothesis, therefore, that the police have only a basic understanding of the concepts of computer crime, they can, individually and in more complex cases, after consultation, properly accept the complaint and, finally, that more

cannot independently verify and investigate crimes related to computer crime and need advice or consultation of their more experienced colleagues.

In that work there has been designed and elaborated the creation of the national database of IP addresses whose existence would greatly contributed to accelerate and simplify the work of the law enforcement proceedings and in particular the delays in criminal proceedings, obtaining information from third parties - in criminal proceedings.

SEZNAM POUŽITÉ LITERATURY

[1] CHMELÍK, J. Vyšetřování trestné činnosti mládeže a páchané na mládeži v teorii a praxi. Praha: MV ČR, Sekce personální práce a vzdělávání, 1995

[2] DISMAN, Miroslav. *Jak se vyrábí sociologická znalost: příručka pro uživatele*. 4., nezměn. vyd. Praha: Karolinum, 2011, 372 s. ISBN 9788024619668.

[3] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.

[4] *Kriminalistika: časopis pro kriminalistickou teorii a praxi*. Praha: Odbor vydavatelství a tisku MV ČR, 2013, roč. 46, č. 1. ISSN 1210-9150.

[5] MAREŠOVÁ, Alena a Milada MARTINKOVÁ. O významu poznávání obětí trestné činnosti. *Ministerstvo vnitra České republiky* [online]. 2009, č. 1, s. 1 [cit. 2013-03-01]. Dostupné z: http://www.mvcr.cz/clanek/o-vyznamu-poznavani-obeti-trestne-cinnosti.aspx

[6] MARTÍNEK, Zdeněk. *Agresivita a kriminalita školní mládeže*. Vyd. 1. Praha: Grada, 2009. ISBN 80-247-2310-7.

[7] MATĚJKA, Michal. *Počítačová kriminalita*. Vyd. 1. Praha: Computer Press, 2002, x, 106 s. ISBN 80-722-6419-2.

[8] NAKONEČNÝ, Milan. *Motivace lidského chování*. 1.vyd. Praha: Academia, 1997, 270 s. ISBN 80-200-0592-7.

[9] Policie ČR, Oddělení Statistiky

[10] TOMÁŠEK, Jan. *Úvod do kriminologie: jak studovat zločin*. Vyd. 1. Praha: Grada, 2010. ISBN 80-247-2982-2.

[11] *Trestní zákoník a trestní řád: úplné znění k 1.1.2010*. 1. vyd. Olomouc: ANAG, 2009, 423 s. Právo (ANAG). ISBN 978-80-7263-561-0.

[12] *Trestní zákoník a trestní řád: průvodce trestněprávními předpisy a judikaturou*. Praha: Linde, 2010, 2 sv. (xviii, 1317, xviii, 1184 s.). ISBN 978-80-7201-803-12.

[13] *Úplné znění zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád)*. Vyd. 6. Praha: Armex, 2011, 291 s. Edice kapesních zákonů. ISBN 978-80-87451-04-5X.

[14] VEČERKA, Kazimír. *Prevence kriminality v teorii a praxi*. Vyd. 1. Praha: Institut pro kriminologii a sociální prevenci, 1996, 202 s. Studie (Institut pro kriminologii a sociální prevenci). ISBN 80-860-0824-X.

[15] WEISS, Petr. *Sexuální zneužívání dětí*. Vyd. 1. Praha: Grada, 2005, 264 s. Psyché (Grada Publishing). ISBN 80-247-0929-5.

[16] ZOUBKOVÁ, Ivana. *Kontrola kriminality mládeže*. 1. vyd. Dobrá Voda u Pelhřimova: Aleš Čeněk, 2002, 231 p. ISBN 80-864-7308-2.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

OOP Obvodní oddělení policie České republiky.

SKPV Služba kriminální policie a vyšetřování.

OSZ Okresní státní zastupitelství.

OČTŘ Orgány činné v trestním řízení.

TČ Trestný čin

MVČR Ministerstvo vnitra České republiky.

ÚZČ Útvar zvláštních činností policie České republiky.

Atd. A tak dále.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Vážení kolegové,

Nejprve mi dovolte, abych představil sebe a cíl a důvod svého výzkumu, pro který jsem zvolil tuto dotazníkovou metodu šetření.

Jmenuji se Václav Pechlát a jsem nejen policistou zařazeným na SKPV OOK ÚO Hodonín, ale také jsem posluchačem závěrečného ročníku magisterského studia Fakulty aplikované informatiky na Univerzitě Tomáše Bati ve Zlíně, oboru Bezpečnostní technologie, systémy a management. Jako téma pro svou diplomovou práci jsem si zvolil: „Odhalování a kontrola počítačové kriminality“, kdy součástí této práce je i výzkum, realizovaný dotazníkovou metodou šetření, jehož cílem je zjistit povědomí policistů zařazených na obvodních odděleních, odděleních služby kriminální policie, a to jak oddělení obecné kriminality, tak i oddělení hospodářské kriminality, o počítačové kriminalitě.

Dotazník je anonymní a bude sloužit pouze jako materiál pro mou diplomovou práci. Jeho výsledky budou prezentovány pouze v praktické části této práce a nebudou ani nikde jinde publikovány. Vyplnění dotazníku nezabere více než 5 minut a proto Vás žádám o pochopení a pravdivé zodpovězení všech otázek.

1) Na jakém útvaru policie jste zařazen?

   A) OOP

   B) SKPV OOK

   C) SKPV OHK

2) Uveďte váš věk:

   A) 18 – 25

   B) 26 – 35

   C) 36 – 45

D) 46 a více

3) Setkal jste se někdy s pojmem počítačová kriminalita?

A) Ano v práci

B) Ano v soukromém životě

C) Ano, avšak pouze v televizi

D) Ne, nesetkal

4) Byl/a jste někdy na školení zaměřeném na oblast počítačové kriminality?

A) Ano

B) Ne

5) Pokud jste se školení z oblasti počítačové kriminality zúčastnil, bylo pro Vás přínosné? (Pokud jste nebyl/a, neodpovídejte)

A) Ano bylo, většinu z předávaných informací si pamatuji

B) Ano bylo, ale dost z předávaných informací si již nepamatuji

C) Ne, nebylo, nepochopil jsem téměř žádnou mě zprostředkovanou informaci

6) Počítačová kriminalita znamená:

A) že někdo ukradl počítač

B) že někdo spáchal trestný čin prostřednictvím počítače

C) že někdo spáchal trestný čin tím, že fyzicky poškodil počítač nebo jeho příslušenství (nějakým nástrojem, jako například palicí)

7) Znáte podstatná specifika počítačové kriminality, která je nutno zjišťovat při přijímání trestního oznámení z oblasti počítačové kriminality?

A) Ano

B) Ne

8) Jak budete kvalifikovat trestní oznámení: „Někdo mi z mého profilu na FaceBooku stahuje moje veřejně přístupné fotografie a rozesílá je mým známým, i neznámým osobám?“

   A) Neoprávněný přístup k počítačovému systému a nosiči informací

   B) Porušování autorského práva

   C) Poškození cizích práv

   D) Není protiprávní jednání

9) Víte koho kontaktovat v případě, že budete přijímat nebo prověřovat oznámení z oblasti počítačové kriminality, pokud si nebudete jistí, zda tomuto oznámení rozumíte?

   Prosím uveďte příslušné oddělení, případně jméno:

   ……
   ……
   ……
   ……

10) Která ustanovení nemůže patřit do oblasti počítačová kriminalita?

   A) Podvod
   B) Pomluva
   C) Znásilnění
   D) Ublížení na zdraví
   E) Zpronevěra
   F) Vydírání
   G) Porušování autorských práv
   H) Padělání a pozměnění veřejné listiny

11) Které ustanovení trestního řádu upravuje získávání informací o uskutečněném telekomunikačním provozu

   A) §8 odst. 1 tr. řádu

   B) §8 odst. 2 tr. řádu

C) §80 tr. řádu

D) §88 tr. řádu

E) §88a tr. řádu

12) Hacker je

A) Pachatel trestného činu Podvod, který prostřednictvím internetu v inzerátu nabídne zboží, nechá si za něj poslat peníze a zboží pak nedodá.

B) Pachatel trestného činu Výroba a jiné nakládání s dětskou pornografií páchaného prostřednictvím počítače a internetu

C) Pachatel trestného činu Neoprávněný přístup k počítačovému systému a nosiči informací

D) Pachatel trestného činu Nebezpečné pronásledování spáchaného prostřednictvím internetu

13) Smí policista vyžádat informace o uživateli konkrétní IP adresy a jeho připojení na konkrétní stránky v přesně určeném čase od poskytovatele internetového připojení žádostí dle ust. §8/1 tr. řádu?

A) Ano

B) Ne

14) Je nutno žádat soud cestou Okresního státního zastupitelství o vydání příkazu dle ust. §88a tr. řádu v případě, že je potřeba zajistit od poskytovatele internetového připojení, smlouvu o poskytování internetu osobě, které byla v určitém časovém období přidělena určitá IP adresa?

A) Ano

B) Ne