Aplikace oprávnění Policie ČR při vyšetřování kybernetické kriminality

Bc. Pavel Zapletal

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Pavel Zapletal**
Osobní číslo:	**A18303**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Aplikace oprávnění Policie ČR při vyšetřování kybernetické kriminality**
Téma práce anglicky:	**Application of the Czech Republic Police Authorisation Methods in the Investigation of Cyber-crime**

Zásady pro vypracování

1. Zpracujte literární rešerši na problematiku kybernetické kriminality.
2. Uveďte oprávnění Policie ČR při vyšetřování kybernetické kriminality.
3. Zpracujte případovou studii na vybrané podvodné jednání přes počítač.
4. Analyzujte vybraná rizika ve vybrané oblasti kybernetické kriminality.
5. Navrhněte opatření pro jednotlivá vybraná rizika.

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

Seznam doporučené literatury:

1. SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.
2. ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.
3. KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou*. Praha: Policejní akademie České republiky v Praze, 2013. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7251-402-1.
4. JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. ISBN 978-80-247-1561-2.
5. PORADA, Viktor a Peter POLÁK. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. Učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 978-80-7380-589-0.

Vedoucí diplomové práce: **doc. Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 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 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 práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové 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 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, dne 12.8.2020

Bc. Pavel Zapletal, v. r.
podpis diplomanta

ABSTRAKT

Diplomová práce je zaměřena na kybernetickou kriminalitu vyšetřovanou Policií ČR. Obsahuje základní pojmy v oblasti kybernetické kriminality a definice účastníků trestního řízení. Vymezuje legislativní rámec řešené problematiky se zaměřením na trestní zákoník. V práci jsou uvedeny oprávnění Policie ČR podle trestního řádu, při vyšetřování daných trestných činů. Součástí diplomové práce je vypracovaná případová studie na podvodné jednání přes počítač. Případová studie se skládá z prvotního oznámení na policejní stanici, získávání a shromažďování informací šetřícím policistou, výslech osoby a následné předání kompletního spisového materiálu dozorujícímu státnímu zástupci. Byla provedena analýza vybraných rizik souvisejících s vybranou počítačovou kriminalitou. Metody analýzy rizik užité v práci jsou předem definovány. Pomocí metod analýzy rizik byla identifikována vybraná rizika související s počítačovou kriminalitou. Identifikovaná rizika byla ohodnocena a u stanovených rizik byla navrhnuta opatření pro jejich minimalizaci.

Klíčová slova: kybernetická kriminalita, pachatel, trestný čin, poškozený, trestní řízení

ABSTRACT

The diploma thesis is focused on cybercrime investigated by the Czech police. It contains basic terms in the field of cyber crime and definitions of participants in criminal proceedings. It defines the legislative framework of the issue with a focus on the Criminal Code. The thesis contains the authorizations of the Police of the Czech Republic according to the Criminal Procedure Code, when investigating the crimes. Part of the thesis is a case study on fraudulent behavior via computer. The case study consists of the initial notification at the police station, obtaining and collecting information by the investigating police officer, the interrogation of the person and the subsequent transmission of the complete file to the supervising prosecutor. Selected risks related to selected cyber crime were analyzed. The risk analysis methods used in the work are predefined. Selected risks related to cyber crime were identified using risk analysis methods. Next these risks are then evaluated and precautionary measures and laws are implied to ensure minimisation of these risks.

Keywords: Cyber crime, Perpetrator, Crime, Injured party, Criminal procedure

Tímto bych rád poděkoval svému vedoucímu diplomové práce panu doc. Ing. Martinu Hromadovi, Ph.D. za odborné vedení, cenné rady, svůj volný čas věnovaný průběžnému pročítání rozpracované a závěrečné verze diplomové práce.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Kybernetická kriminalita je v současnosti fenoménem ve světě kriminality, která posledních několik let výrazně roste. Státy celého světa se zaměřují na řešení kybernetické bezpečnosti. Rozvoj výpočetní techniky a závislost lidí na výpočetní technice sebou přináší svá úskalí. Promítnutí výpočetní techniky do většiny oblastí lidské společnosti je již téměř samozřejmostí. Zatímco základním uživatelům práci ulehčí, pro útočníky znamená možnost ovlivnit jednotlivce či společnost. Pachatelé hledají slabiny světa výpočetní techniky a následně vymýšlí, jak využít možnosti ulehčení práce uživatelů pro své protiprávní jednání. Tímto způsobem se postupně rozvíjí využívání kyberprostoru pro páchání trestné činnosti, vedoucí k získání finančního nebo jiného prospěchu.

Z důvodu aktuálnosti tématu kybernetické kriminality v oblasti bezpečnosti, jsem se rozhodl na danou problematiku zaměřit ve své diplomové práci. Lidé si často nejsou vědomi toho, že nepříjemná událost v souvislosti s napadením jejich dat, která se jim stala, je postižitelná trestním zákoníkem nebo jiným právním předpisem. Trestní zákoník sice neobsahuje oblast kybernetických trestných činů, avšak několik trestných činů v něm obsažených může být pácháno i v rámci kyberprostoru.

Práce se skládá z teoretické a praktické části. V teoretické části budou popsány základní oblasti kybernetické bezpečnosti s důrazem na kybernetickou kriminalitu. Čtenář bude seznámen s vyšetřováním kybernetické kriminality. Praktická část se bude skládat z oprávnění Policie České republiky (dále jen „Policie ČR“) podle trestního řádu, které je využíváno pro získávání důkazních prostředků a následné objasnění oznámení protiprávního jednání. Další kapitola bude věnována případové studii zaměřené na jedno z možných protiprávních jednání v kyberprostoru. Po případové studii bude také zahrnovat analýzu rizik z vybrané oblasti kybernetické kriminality. Rovněž je důležitá informovanost veřejnosti o protiprávním jednání v kyberprostoru, aby zbytečně svou neznalostí nezjednodušovali pachatelům jejich nezákonné chování.

I. TEORETICKÁ ČÁST

1 HISTORICKÁ VÝCHODISKA KYBERNETICKÉ KRIMINALITY

Za počátek počítačové kriminality považujeme skutek z roku 1801, kdy Jacquard vytvořil stroj, který umožňoval automatizaci činností spojených s tkaním speciálních látek. Pracovníci manufaktur se začínali bouřit, měli strach, aby vlivem automatizace nepřišli o svá zaměstnání. Právě to bylo důvodem k zamezení Jacquardovi v dalším vývoji. [1]

Zakladatel kybernetiky, Norbert Wiever, roku 1947 popsal kybernetiku jako vědu zabývající se komunikací a řízením uvnitř organismů a zařízení. V roce 1968 došlo ke vzniku sítě ARPANET a rovněž prvotnímu propojení čtyř školních počítačů. Nikdo ale neočekával, že dojde k velkému rozmachu v oblasti síťových technologií. [2]

S postupným rozvojem počítačových technologií přichází i nová úskalí. V roce 1996 se Jakulin začíná zmiňovat o protiprávním jednání, při kterém je počítač v roli nástroje nebo předmětu útoku, čímž postupně definuje pojem počítačové kriminality. [3]

S příchodem moderních informačních technologií vzniká i disciplína zabývající se kybernetickou bezpečností a reaguje tak na potřebu ochrany informací. Moderní informační technologie pracují s větším množstvím dat, kdy tyto disponují různou vypovídající hodnotou. Manipulace s elektronickými daty se postupně stávala jednodušší a bylo tak snadnější jejich kopírování, ukládání, provádění změn či jejich smazání a destrukce. [4]

Vývoj kybernetické kriminality lze rozdělit do tří etap. První etapu tvoří propojení čtyř počítačů na univerzitě a vytvoření počítačové sítě pro sdílení dat. Druhou etapu datujeme do období 80. let 20. století, kdy byl vytvořen první osobní počítač. Za tvorbou prvního počítače stála společnost International Business Machines. Poslední etapa je započata umožněním veřejnosti přístupu k internetu a s tím související přizpůsobení aplikací pro jejich uživatele. Internet v současnosti využívá většina společnosti každý den, což sebou kromě výhod přináší i mnoho rizik. Příkladem rizik je odcizení financí, osobních informací, virtuální komunikace s psychicky nemocnými lidmi a podobně. Čelit kybernetické kriminalitě není snadné. Lidé by měli při fungování v kyberprostoru vědět, co se pod tímto pojmem skrývá, znát druhy protiprávních jednání v tomto prostoru a mít určitou právní představu o činech řešených Policií ČR. Problém kybernetické kriminality spočívá v jejím skrytém průběhu, někteří lidé vůbec neberou v potaz možné nástrahy v tomto prostředí. Anonymita pachatele stěžuje Policii ČR možnost zjistit, kdo za takovýmto protiprávním jednáním stojí. Nejtěžší je však pachateli jeho protiprávní jednání v kyberprostoru prokázat. Vyšetřování kromě lhostejností uživatelů samozřejmě ovlivňuje i odborné vzdělání příslušníků Policie ČR, které

v současnosti není přímo zajišťováno. Policista se tedy především musí spoléhat na samostatné vzdělávání, aby byl schopen se ve stále rozvíjející se oblasti na určité úrovni orientovat. [5]

Abychom dokázali pochopit, co se skrývá pod pojmem kybernetická kriminalita, je třeba si říct, co je to kriminalita. Kriminalita zahrnuje všechna protiprávní jednání naplňující skutkovou podstatu některého z trestných činů uvedených v zákoně č. 40/2009 Sb. trestního zákoníku. Důsledný rozbor a popis kybernetické kriminality je proveden v knize Jana Kolouch a s názvem Cyber Crime. Kybernetickou kriminalitu zde vymezil jako kriminalitu, při níž za nástroj trestného činu jsou použity prostředky komunikačního a informačních technologií. Cílem útoku pachatele musí být prostředky komunikačních a informačních technologií. Aby byl skutek trestným činem, pachatel musí dané prostředky použít v kyberprostoru. [6]

První kapitola se zabývala počátky kybernetiky a rozvoji v oblasti výpočetních technologií, který sebou přinesl i protiprávní jednání v tomto prostoru. Zmíněny byly etapy vývoje kybernetické kriminality a byl vymezen pojem kybernetické kriminality.

2 ZÁKLADNÍ POJMY

Oblast kybernetické kriminality zahrnuje velké množství pojmů, kdy níže budou specifikovány pojmy, které jsou nejvíce spojovány s popisovanou problematikou.

2.1 IP adresa

Ve výkladovém slovníku kybernetické bezpečnosti nechybí pojem IP adresa, což je unikátní číslo v každé počítačové síti, rozlišující síťová rozhraní připojená k počítačové síti. [7]

IP znamená internetový protokol. K přidělování IP adres dochází na základě podnětu organizace, jejíž náplní je registrace, spravování a evidence IP adres. IP adresu není možné si vymyslet podle sebe. Jedinečnost číselného označení IP adresy je základem pro připojení v síti s jinými počítači. IP adresa je přiřazována počítačům jednotlivě a s rozdílným číselným označením. Nejvíce se používá 32 bitová IPv4 a 128 bitová IPv6. U virtuálních serverů pracujících na jediném fyzickém zařízení, je možné, aby více domén mělo jedinou adresu. Jestliže má počítač více síťových adaptérů, nemusí mít pouze jednu adresu. [8,9]

2.2 Kyberprostor

Kyberprostor je chápan jako prostor internetové sítě bez kontroly jakékoliv organizace, v němž probíhá komunikace přes počítačové sítě a může dojít i ke kybernetickému útoku. [10]

V cizojazyčné literatuře je definován jako prostor neexistující ve fyzickém světě, který byl vytvořen počítačovými systémy a jediný fyzický pohyb v něm, spočívá v pohybu myši a užití klávesnice. [11]

Termín kyberprostor byl poprvé použit americkým spisovatelem Wiliamem Gibsonem. K využití pojmu došlo v 80. letech minulého století, kde jako autor vědeckofantastické literatury slovo kyberprostor uvedl ve své povídce Burning Chrome. Kyberprostor zde popsal jako: *„Konsenzuální datovou halucinaci, vizualizovanou v podobě imaginárního prostoru, tvořeného počítačově pracovanými daty a přístupného pouze vědomí uživatelů.“* Postupem času se popis kyberprostoru měnil a začal být posuzován spíš z hlediska vztahu kyberprostoru k počítačovým sítím. [12]

2.3 Oběť trestného činu x poškozený v trestním řízení

Pojem oběť trestného činu vymezil zákon č. 45/2013 Sb. o obětech trestných činů. *„Obětí je fyzická osoba, které bylo nebo mělo být trestným činem ublíženo na zdraví, způsobena majetková a nemajetková újma, nebo na jejíž úkor se pachatel trestným činem obohatil.“* [13]

V trestním zákoníku se setkáváme s postavením poškozeného v trestním řízení. V ustanovení § 43 zákona č. 141/1961 Sb. je definován poškozený jako: „*Ten, komu bylo trestným činem ublíženo na zdraví, způsobena majetková škoda nebo nemajetková újma, nebo ten, na jehož úkor se pachatel trestným činem obohatil (poškozený), má právo činit návrh na doplnění dokazování, nahlížet do spisů (§ 65), zúčastnit se sjednávání dohody o vině a trestu, zúčastnit se hlavního líčení a veřejného zasedání konaného o odvolání nebo o schválení dohody o vině a trestu a před skončením řízení se k věci vyjádřit. Jde-li o trestný čin zanedbání povinné výživy (§ 196 trestního zákoníku), rozumí se pro účely tohoto zákona majetkovou škodou, jež byla poškozenému způsobena trestným činem, i dlužné výživné“.* [14]

2.4 Pachatel trestného činu

Pachatelem může být kdokoliv, jde o subjekt trestného činu. Podmínkou je, aby svým protiprávním jednáním naplnil znaky alespoň některého z trestných činů. Za pachatele trestného činu je považován i spolupachatel nebo účastník. Pod pojmem účastník si lze představit organizátora, návodce nebo pomocníka. Trestná je také příprava nebo pokus trestného činu. [2]

2.5 Počítačová kriminalita vs. kybernetická kriminalita

Za počítačovou kriminalitu z pohledu kriminalistiky považujeme protiprávní jednání s využití prostředků výpočetní techniky v prostředí komunikačních systémů, sítí, softwarového vybavení a databází výpočetní techniky. [15]

Slovenský policejní sbor pracuje s pojmem počítačové kriminality založeném na neoprávněné, protizákonné a nemorální činnosti, zneužívající informace získávané pomocí výpočetní techniky. [16]

Někteří autoři definují kybernetickou kriminalitu stejnou definicí pro počítačovou kriminalitu. V současné době se několik autorů již neopírá čistě o nutnost využití počítače. Jako rozdíl je uváděno protiprávní jednání v kyberprostoru. Kybernetická kriminalita nemusí být

tedy páchána pouze pomocí počítače. Příkladem je třeba spáchání Podvodu podle ustanovení § 209 z. č. 40/2009 Sb., trestního zákoníku, v kyberprostoru přes mobilní síť.

2.6 Počítačová stopa vs. digitální stopa

Počítačovou stopou je změna na nosiči informací, vzniklá v souvislosti s trestným činem. Výpočetní techniku používá k protiprávnímu jednání. Je zjistitelná a využitelná díky nynějším metodám, operacím a prostředkům. [17]

„Digitální stopa je jakákoliv informace s vypovídající hodnotou, uložená nebo přenášená v digitální podobě.“ [18]

2.7 Trestný čin

Trestným činem je v trestním právu vykládán jako pro společnost nebezpečný čin, jehož znaky jsou popsány v trestním zákoníku č. 40/2009 Sb.. Podle trestního zákoníku jsou posuzovány trestné činy, spáchané na území České republiky. Oproti přestupkovému jednání je u trestných činů uvedeno, že je zapotřebí úmyslného jednání. Výjimkou je, pokud u samotného trestného činu není výslovně uvedeno, postačující zavinění z nedbalosti. Trestné činy se dělí na přečiny a zločiny, které se liší formou zavinění a výší trestní sazby [19,20]

Druhá kapitola se zabývá vymezením základních pojmů, se kterými se setkává policejní orgán při vyšetřování kybernetické kriminality. V pojmech jsou popsána základní postavení osob v trestním řízení. Nechybí zde rozdíly mezi počítačovou a kybernetickou kriminalitou a také rozdíly mezi počítačovou stopou a digitální stopou.

3 PRÁVNÍ RÁMEC

Problematikou kybernetické bezpečnosti se zabývá více právních předpisů, kdy některé z nich budou dále zmíněny, zejména ty, které se týkají Policie ČR.

3.1 Zákon o kybernetické bezpečnosti

Vytvoření zákona č. 181/2014 Sb. o kybernetické bezpečnosti vyplynulo s výrazným nárůstem využívání informačních technologií firmami a společnostmi. Používání informačních technologií má kromě zrychlení předávání informací, rozvoji služeb i negativní dopady. Negativním dopadem pro společnost může být myšleno zneužití či útok na výpočetní technologie. Při útocích na kritickou infrastrukturu, může být ohrožen přímo i stát. Zákon o kybernetické bezpečnosti obsahuje především prvky prevence před kybernetickými incidenty a případná minimalizace následných škod. [21]

3.2 Trestní zákoník

Obecně lze říci, že trestní zákoník č. 40/2009 Sb. specifikuje trestné činy vyšetřované zpravidla Policií ČR. Ve zvláštní části trestního zákoníku můžeme najít cekem 13 hlav, ve kterých jsou rozepsány jednotlivé skutkové podstaty trestných činů. Kybernetické trestné činy netvoří samotnou jednu hlavu trestního zákoníku, nýbrž jde o trestné činy zahrnuté v různých oblastech. Aby mohl být skutek považován za trestný čin, musí naplnit skutkovou podstatu minimálně jednoho trestného činu. Přiřazování trestných činů oblasti kybernetické kriminality bude blíže stanoveno v jiné kapitole. Kybernetická kriminalita se stále vyvíjí, a proto bude potřeba na ni reagovat i změnou a doplněním právních předpisů.

3.3 Strategie prevence kriminality v ČR 2016 - 2020

Usnesením vlády ČR č. 66 z ledna roku 2016 vláda schválila Strategii prevence kriminality v ČR na léta 2016 - 2020. Strategie se mimo jiné zabývá i tématem nových hrozeb a přístupů k prevenci kriminalit, současně je ve strategii zmíněna i kybernetická kriminalita, zahrnutá pod téma kriminality ve virtuálním prostředí. Nárůst kybernetické kriminality stoupne ročně v průměru o jednu třetinu. Většina kybernetické kriminality zůstává ovšem neodhalena. Následuje stručný výčet několika oblastí z trestního zákoníku týkajících se trestných činů spadajících pod kybernetickou kriminalitu. Za podstatnou kapitolu je považována osvěta společnosti a její informovanost o rizicích a ochranou před nimi. Mnohdy je velmi obtížné pro

samotnou oběť uvědomit si a rozpoznat, že na ní byl spáchán trestný čin. Ve výčtu všech podstatných strategií pro ČR najdeme i Národní strategii kybernetické bezpečnosti ČR na období let 2015 až 2020. [22]

3.4 Národní strategie kybernetické bezpečnosti na období let 2015 - 2020

Dokument Národní strategie kybernetické bezpečnosti je v gesci Národního bezpečnostního úřadu. V dokumentu jsou uvedeny vize ČR v oblasti kybernetické bezpečnosti. Jsou zde definovány principy, které ČR bude respektovat a dodržovat. Následuje popis výzev, jakým je třeba čelit. V neposlední řadě v dokumentu nalezneme hlavní cíle pro dosažení, co nejvyšší úrovně kybernetické bezpečnosti. Závěr je věnován tématu implementace hlavních cílů, odkazujících se zejména na Akční plán k Národní strategii kybernetické bezpečnosti ČR na období let 2015 až 2020. V Akčním plánu jsou k hlavním cílům přiřazeny příslušné úkoly, odpovědný subjekt a časový rámec jejich splnění. [23]

3.5 Audit národní bezpečnosti

V reakci na zhoršující se bezpečnostní situaci v Evropě, byl v roce 2016 Ministerstvu vnitra přidělen úkol ze strany Bezpečnostní rady státu, aby vytvořilo skupinu, pro zpracování analýzy odolnosti a schopností České republiky čelit bezpečnostním hrozbám a navrhnout opatření pro minimalizaci zjištěných hrozeb. Téhož roku byl daný dokument prezentován. Jednou z kapitol jsou i hrozby v kyberprostoru. Kybernetické hrozby jsou zde rozděleny na kyberterorismus, nepřátelské kampaně, kyberšpionáž, narušení nebo snížení odolnosti IT infrastruktury a narušení nebo snížení bezpečnosti eGovernmentu. Specifikovaným hrozbám byla přiřazena míra rizika pro ČR, kdy pouze kyberterorismu a narušení nebo snížení bezpečnosti eGovernmentu byla přiřazena střední rizikovost, u ostatních výše uvedených bylo riziko uvedeno jako vysoké. Ke každé z podoblastí kybernetických hrozeb byly uvedeny jejich rizika a problémy. Dále je provedena SWOT analýza obsahující hrozby, příležitosti, silné a slabé stránky. Na závěr jsou uvedena doporučení k posílení odolnosti. [24]

3.6 Úmluva Rady Evropy č. 185 o kyberkriminalitě

Úmluva Rady Evropy o kyberkriminalitě byla schválena v listopadu roku 2001, Výborem ministrů Rady Evropy. Jde o právní předpis, který byl vytvořen pro sjednocení kybernetické kriminality v národně právní oblasti. Jednotlivé státy mají povinnost upravit své právní řády

tak, aby byly trestány trestné činy v oblasti kybernetické kriminality, popsané v Úmluvě o kyberkriminalitě. Úmluva o kyberkriminalitě byla ze strany České republiky podepsána v roce 2005 a platná začala býti od 1. prosince roku 2013. V Úmluvě jsou mimo jiné definovány čtyři skupiny kybernetických trestných činů. Jedná se o trestné činy:

- související s počítači,
- související s porušováním autorských a souvisejících práv,
- související s obsahem,
- proti utajování, integritě a dostupnosti počítačových dat a systémů.

Obsah Úmluvy o kybernetické kriminalitě je tvořen preambulí, základními pojmy, opatřeními pro vnitrostátní úroveň, mezinárodní spolupráci a závěrečnými ustanoveními.

K Úmluvě o kybernetické kriminalitě existuje i její dodatkový protokol z roku 2003, ve kterém jsou uvedeny další trestné činy, nepopsané v původním dokumentu úmluvy. [6]

Třetí kapitola byla zaměřena na zákony, další právní normy a dokumenty zabývající se kybernetickou kriminalitou a kybernetickou bezpečností. Některé z výše uvedených právních předpisů se nezabývají pouze kybernetickou kriminalitou nebo kybernetickou bezpečnostní, ale i dalšími problematickými oblastmi. Z textů tedy byly vyňaty pouze informace týkající se těchto dvou oblastí, především kybernetické kriminality a poté byly implementovány do výše uvedené kapitoly.

4 INSTITUCE A KYBERNETICKÁ BEZPEČNOST

Na kybernetickou kriminalitu a kybernetickou bezpečnost se zaměřuje několik institucí. Uvedeny budou ty nejvýznamnější v daných oblastech.

4.1 Národní úřad pro kybernetickou a informační bezpečnost

Vznik Národního úřadu pro kybernetickou bezpečnost k 1. srpnu roku 2017 byl důsledkem změny původního zákona o kybernetické bezpečnosti č. 181/2014 Sb. na zákon č. 205/2017 Sb. Pro kybernetickou bezpečnost a ochranu utajovaných informací je v postavení ústředního správního orgánu. Zaměřuje na oblast kryptografické ochrany, informační a komunikační systémy a také se zabývá bezpečnostní správou provozu služby navigačního systému Galileo. Spolupracuje s CERT a CSIRT týmy. Zajišťuje kybernetická cvičení v ČR i ve světě. Pracovní náplní ředitele Úřadu pro kybernetickou a informační bezpečnost je mimo jiné i členství v pracovním orgánu Bezpečnostní rady státu, kterým je Výbor pro kybernetickou bezpečnost. [25,26]

4.2 CERT a CIRT

CERT neboli Computer Emergency Response Team je tým, jehož prvopočátky v České republice sahají do roku 2004 vznikem prvního týmu CESNET-CERTS, uznaného úřadem Trusted Introducer a mezinárodní infrastrukturou. Tým měl za úkol řešit bezpečnostní problémy v oblasti e-infrastruktury CESNET. [27]

CERT i CSIRT (Computer Security Incident Response) jsou v dnešní době považovány za relativně stejné týmy, které mají odpovědnost za vyřešení bezpečnostních incidentů a hrozeb v stanoveném poli působnosti. Odlišují se od sebe svou historií, kdy jako první vznikl CERT tým. K vytvoření prvního CERT týmu přiměl USA tzv. Morrisův červ z roku 1988. Morrisův červ nese název po studentu americké univerzity, který desetinu všech připojených zařízení k internetu, vyřadil z chodu. Za vznikem prvního CERT týmu stála Carnegie Mellon University, která si pro zkratku CERT zajistila ochrannou známku. Nové týmy, které chtěly nést název CERT, museli o toto požádat Carnegie Mellon University, proto vznikly CSIRT týmy. Oba druhy týmů využívají internet ke své činnosti a starají se o jeho fungování. Každý CSIRT tým musí být schopen reagovat na hrozbu a spolupracovat v případě vzniku ohrožení bezpečnostním incidentem například zjišťováním osoby útočníka nebo odstraněním pro-

blému. CERT a CSIRT jsou součástí mezinárodní bezpečnostní infrastruktury, kdy musí postupovat podle určitých pravidel. CSIRT a CERT tým musí veřejně uvádět svého provozovatele, jeho pracovní náplň, pravomoci, odpovědnost týmu, členy a kdy a kde můžeme daný tým nalézt. Oba týmy vznikají na základě dobrovolnosti členů. Existují také národní a vládní CSERT/CSIRT týmy. Národní týmy jsou považovány za poslední možnost pro vyřešení bezpečnostního incidentu, zatímco vládní týmy řeší bezpečnostní incidenty v rámci státní správy a samosprávy při možném ohrožení bezpečnosti státu a jeho služeb. [22]

4.3 Příslušná ministerstva České republiky

Ministerstvo obrany má odpovědnost za plánování, rozvoj schopností a výstavbu u armády ČR, kdy musí dodržovat povinnosti člena Evropské unie a NATO pro kybernetickou obranu. V oblasti kybernetické bezpečnosti dohlíží na vojenské sítě, informační a komunikační systémy zaštiťované Ministerstvem obrany. Zajišťuje také připravenost a s tím související schopnost snížit dopady kybernetických útoků při vojenských a hybridních operacích, dopady snahy získat informace z vojenské oblasti prostřednictvím kybernetické špionáže a rovněž nepřátelských propagací jiného státu pro splnění vytyčených vojenských cílů v kyberprostoru. [24]

Ministerstvo vnitra ČR má na starosti veřejný pořádek a vnitřní bezpečnost. V oblasti kybernetické bezpečnosti zajišťuje modernizaci výkonu státní správy prostřednictvím informačních a komunikačních technologií. Jedná se například o datové schránky nebo základní registry. U složek integrovaného systému můžeme zmínit třeba linku 112. [24]

Ministerstvo zahraničních věcí má za úkol splnění povinností vyplývajících z Akčního plánu k Národní strategii kybernetické bezpečnosti ČR. Povinnosti se týkají zejména vztahů s cizími státy a jejich organizacemi. [24]

4.4 Zpravodajské služby

Zpravodajské služby mají za úkol zjišťování skutečností nasvědčujících možnému ohrožení České republiky jako státu i samotných obyvatel. Výjimkou není ani prověřování skutečností v kyberprostoru a následné informování státních orgánů o hrozbách a rizicích v daném prostoru. [24]

4.5 Policie České republiky

Policie České republiky je ozbrojený bezpečnostní sbor, který se v oblasti trestněprávní roviny zabývá trestnými činy, které mají spojitost mimo jiné i s kybernetickou kriminalitou. Samotnou oblast kybernetické kriminality bychom v trestním zákoníku č. 40/2009 Sb. jen těžko hledali. Jednotlivé trestné činy, které jsou v zákoníku uvedeny, popisují prostřednictvím skutkové podstaty jejich protiprávnost. V některých případech jsou tyto činy páchány v kyberprostoru. V další kapitole budou uvedeny konkrétní trestné činy a jejich zařazení v jednotlivých hlavách právního předpisu.

Čtvrtá kapitola obsahuje informace o institucích, působících v rámci České republiky, které se zabývají dohledem a zajišťováním kybernetické bezpečnosti na jejím území. U každé z popisovaných institucí je uvedeno, co je jejich náplní a úlohou v oblasti kybernetické bezpečnosti nebo přímo u kybernetické kriminality.

5 KYBERNETICKÉ TRESTNÉ ČINY

Při prověřování protiprávního jednání souvisejícího s kybernetickou kriminalitou, policejní orgán vychází z trestných činů uvedených v trestním zákoníku. Seznam trestných činů týkajících se kybernetické kriminality nebo takových, které mohou mít spojitost s trestným činem v kyberprostoru, bude uveden níže.

Z trestných činů proti životu můžeme zařadit:

- § 144 Účast na sebevraždě.

Trestné činy proti svobodě:

- § 175 Vydírání.

Tresné činy proti právům na ochranu osobnosti, soukromí a listovního tajemství:

- § 180 Neoprávněné nakládání s osobními údaji,
- § 181 Poškození cizích práv,
- § 182 Porušení tajemství dopravovaných zpráv,
- § 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí,
- § 184 Pomluva.

Trestné činy proti lidské důstojnosti v sexuální oblasti:

- § 191 Šíření pornografie,
- § 192 Výroba a jiné nakládání s dětskou pornografií.

Trestné činy proti majetku:

- § 209 Podvod,
- § 230 Neoprávněný přístup k počítačovému systému a nosiči informací,
- § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému sytému a jiných takových dat,
- § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti. [20]

Pátá kapitola zahrnuje trestné činy uvedené v trestním zákoníku, které mívají spojitost s kybernetickou kriminalitou. Jaké konkrétní zákonné ustanovení bude přiřazeno k protiprávnímu jednání, záleží vždy na spáchaném skutku. Protiprávní jednání může naplnit skutkovou

podstatu jednoho z výše uvedených trestných činů, ale v některých případech i vícero trestných činů. Pro přesnou kvalifikaci protiprávního jednání je nutné, aby měl policejní orgán nashromážděných co nejvíce podkladů k danému skutku. Čím více detailů bude Policie ČR ke konkrétnímu jednání znát, tím snazší pro ni bude určení přesné právní kvalifikace.

6 AKTUÁLNĚ PROBÍRANÁ TÉMATA

Kapitola nazvaná aktuálně probíraná témata se zaměřuje na vybrané oblasti často veřejně probíraných protiprávních jednání. Jednotlivé podkapitoly nenesou přímo názvy paragrafového znění. Jedná se o názvy vytvořené laickou veřejností, opírající se o různá právní ustanovení v trestním zákoníku.

6.1 Kyberšikana

Kyberšikana je v současné době velmi často používaným termínem souvisejícím s rozmachem v oblasti elektronických zařízení. Dnešní společnost využívá počítače i mobilní telefony každý den. Ke kyberšikaně dochází přes mobilní telefony nebo pomocí internetu. Příkladem kyberšikany prostřednictvím telefonů jsou bezhlasé telefonáty nebo posílání krátkých sms zpráv. V případě využití internetu jsou například zasílány šikanující emailové zprávy nebo zprávy na sociálních sítích jako Facebook a podobně. Hlavním rozdílem mezi šikanou a kyberšikanou je v tom, že kyberšikana probíhá i v kyberprostoru bez fyzické přítomnosti útočníka u oběti. [27]

Kyberšikana jako taková není trestným činem podle trestního zákoníku. Chování kyberšikany můžeme v trestním zákoníku identifikovat například v ustanovení § 175 Vydírání. V některých případech může dojít k naplnění skutkové podstaty trestných činů § 191 Šíření pornografie či § 192 Výroba a jiné nakládání s dětskou pornografií. Psychické vypětí oběti může v nejhorších případech dospět i k trestnému činu podle § 144 Účast na sebevraždě.

6.2 Kyberstalking

Pod pojmem stalking si můžeme představit systematické, opakující se, dlouhodobé a stupňující se vyhledávání oběti ze strany pachatele. Jednou z forem stalkingu je i kyberstalking. Dané pronásledování se vyznačuje používáním pachatele informačních a komunikačních technologií. Kybernetické pronásledování je v trestním zákoníku možné přiřadit k ustanovení § 354 Nebezpečné pronásledování a někdy s tím i související protiprávní jednání podle § 353 Nebezpečné vyhrožování. [5,28]

Na vzestupu je v současné době tzv. stalkerware. Co je to stalkerware? Jedná se o počítačový software, který pachatel nainstaluje do elektronického zařízení oběti. Po nainstalování softwaru získává útočník přístup k soukromým datům oběti, jakými jsou například fotografie, aplikace, zprávy nebo informacím zveřejněným prostřednictvím sociálních sítí. Útočník

svou oběť může i odposlouchávat. Zjištění takového útoku není vůbec snadné. Oběť by k podezření mohla dospět zjištěním rychlejšího vybíjení baterie nebo umožněním instalování neznámých aplikací, zvýšeným přenosem dat. Společnost Kaspersky eviduje 380 aplikací, které mohou pracovat jako stalkerware. V nejčastějších případech za útočníkem stojí partner, který má přístup k zařízení jeho oběti. Společnost Kaspersky také uvádí, že za prvních osm měsíců roku se útočnici pokusili získat přístup k zařízení téměř 38 tisíců lidí. [29]

6.3 Sexting

Před definováním pojmu sexting je třeba si říci, co je základem takového chování. Problém vzniká již na straně budoucí oběti, i když si nic takového nepřipouští. Budoucí oběť z důvodu zamilovanosti nebo větší kamarádské důvěře zašle svému příteli či přítelkyni fotografie nebo videonahrávku, jelikož byla o to partnerem nebo přítelem požádána. Oběti bohužel v některých případech takové fotografie nebo video svých intimních partií vytvoří a zašle budoucímu pachateli. Určitou dobu se nemusí nic dít, ale v případě partnerského rozchodu nebo ukončení přátelství, muže být takovýto soubor zneužit. Sexting je založen na elektronickém rozesílání dat se sexuálním obsahem. Kromě výše popsaných zasílání erotických fotografií a videí zde patří i textové zprávy. Každý člověk by si měl pořádně promyslet, zda je ochoten podstoupit riziko, že by se daný soubor s jeho osobou někdy v budoucnu mohl dostat k jiné osobě a podle toho se rozhodnout. [10]

Kvalifikace jednání pachatele je v tomto případě složitá. Příkladem může být vydírání oběti bývalým partnerem, aby se k němu vrátila, jinak danou fotografii či video rozešle svým kamarádům nebo zveřejní jej na internetu. Takovéto jednání je možné kvalifikovat podle ustanovení § 175 Vydírání z. č. 40/2009 Sb., trestního zákoníku. Když pachatel fotografie či videa svého bývalého pantera nebo přítele zveřejní, je teoreticky možné kvalifikovat i podle ustanovení § 191 Šíření pornografie z. č. 40/2009 Sb., trestního zákoníku.

6.4 Kybergrooming

Kybergrooming je dalším útokem na oběť v kyberprostoru, označován jako velice nebezpečný kybernetický útok. Probíhá zejména přes internetové chaty, seznamky, ale v současnosti nejvíce přes sociální sítě. Jde o chování útočníka přes internet, jehož cílem je získat důvěru oběti a dohodnout si s obětí osobní setkání. Obětmi bývají především děti a z nich převládají slečny před chlapci. U pachatelů již jejich specifikace není snadná. Útočníky bý-

vají osoby s nižším či vyšším intelektem a různým sociálním postavením. Dítě často útočníka zná a je na něm závislé. Pachatelem bývají i rodinní známí. Následkem kybergrooming může býti sexuální zneužití dítěte, využití oběti pro výrobu dětské pornografie a podobně. [30]

Výše popsaná protiprávní jednání je možné přiřadit k určitým právním ustanovením v trestním zákoníku. V případě zneužití dítěte pro výrobu dětské pornografie je přímo zákonné ustanovení podle § 192 Výroba a jiné nakládání s dětskou pornografií. Při zneužití dítěte se pachatel dopouští protiprávního jednání podle § 187 Pohlavní zneužívání. Dalšími spáchanými trestnými činy mohou být následující paragrafová ustanovení: § 168 Obchodování s lidmi, § 171 Omezování osobní svobody, § 175 Vydírání, § 201 Ohrožování výchovy dítěte, § 209 Podvod, § 353 Nebezpečné vyhrožování a § 354 Nebezpečné pronásledování. [31]

V šesté kapitole jsou blíže popsány pojmy kyberšikana, kyberstalking, sexting a kybergrooming. Kromě definování těchto pojmů, jsou k nim uvedeny i příklady možných protiprávních jednání a jejich následná právní kvalifikace podle trestního zákoníku. Jedná se pouze o příklady, vše se odvíjí od konkrétní situace a detailů vzniklého protiprávního jednání.

7 PACHATELÉ KYBERNETICKÉ KRIMINALITY

Pachatelem jakéhokoliv trestného činu podle trestního zákoníku, je osoba, který svým jednáním naplní skutkovou podstatu některého z daných trestných činů. Jaké jsou motivy pachatele, typy pachatelů a jakým způsobem je páchána kybernetická trestná činnost, to bude uvedeno v následujících bodech.

7.1 Motivy pachatele

Nejprve je potřeba si říci, co se skrývá pod slovním spojením motiv pachatele. Motiv pachatele je impulsem pachatele ke spáchání trestné činnosti. Častými motivy bývá vidina finančního obohacení, politický důvod, pobavení se, emoční vypětí, psychická porucha či sexuální podtext. Motiv může být jeden, ale někdy se také jedná o kombinaci několika různých motivů. [32,33]

Zjištění motivu pachatele vždy napomáhá vyšetřovatelům při objasňování každého trestného činu, jinak tomu není ani v případě vyšetřování kybernetické kriminality. Od motivu útočníka se dále odvíjí právní kvalifikace. [34]

Pro typování možného pachatele u kybernetické kriminality z určitého počtu prověřovaných osob je důležité zjištění motivu zejména, když hledáme pachatele z řad zaměstnanců poškozené společnosti nebo jejich bývalých členů. Úkolem orgánů činných v trestním řízení je zjištěný motiv prokázat. [33]

7.2 Způsoby páchání

Protiprávní jednání v kyberprostoru je v současnosti velice aktuální téma s rostoucí kriminalitou v tomto prostřední. Jde o netradiční kriminalitu vůči běžné kriminalitě. Pachatelé zde nevyužívají násilí ve formě zbraní střelných, bodných či sečných. Specifickou oblastí je místo, jelikož místo spáchání trestného činu, místo následku a místo oběti protiprávního jednání bývá odlišné. Následek takového jednání může například nastat v jiném státě, než z jakého státu je útok veden. Problémem často bývá, že ani oběť takového trestného činu si není vědoma protiprávního jednání vůči její osobě. Hlavní roli v pro vyšetřovatele kybernetické kriminality sehrává digitální stopa. Specifikací digitální stopy je snadnost jejího znehodnocení, které by zkomplikovalo vyšetřování orgánům činným v trestním řízení. [35]

Páchání kybernetických trestných činů je založeno nejen na zneužití počítačové sítě nebo výpočetní techniky, ale rovněž i na chování pachatele v době před, během a po samotném

zneužití. V České republice jsou podle toho rozděleny způsoby páchání kybernetické kriminality na:

- Neoprávněné změny v uložených datech,
- Neoprávněné zásahy do vstupních dat,
- Informační trestná činnost,
- Napadení cizího počítače, jeho programového vybavení a souborů dat v databázích,
- Neoprávněné pronikání do počítačů, počítačového systému a jeho databází,
- Neoprávněné pokyny k počítačovým operacím. [36]

7.2.1 Neoprávněné změny v uložených datech

Za pachatele neoprávněné změny v uložených datech bývá v četných případech označen pracovník společnosti, jehož pravomoci spočívají v přístupu do systému, kde může pracovat s datovými soubory. Provede změnu v uložených datech, aby mohl dosáhnout svého cíle. Po splnění stanoveného cíle vrátí změnu v uložených datech do původní verze. [37,38]

7.2.2 Neoprávněné zásahy do vstupních dat

Pachatel neoprávněného zásahu do vstupních dat má přístup k vstupním dokladům nebo k místu zpracování daných dokladů. Upravením vstupního dokladu před využitím počítače, dospěje pachatel k zisku finanční hotovosti například výběrem z účtu pomocí cizího občanského průkazu (získaného ztrátou nebo nálezem) nebo prostřednictvím tzv. bílého koně. Bílým koněm může být například osoba bez domova, které pachatel před protiprávním jednáním nabídne finanční hotovost za založení bankovního účtu na své jméno. Bílý kůň následně pachateli předá bankovní kartu, včetně přihlašovacích údajů a za to je mu ze strany útočníka vyplacena dohodnutá částka. Další možností je, že útočník zajistí vytvoření dokladu s falešnými údaji, který zneužije k převedení prostředků. Následně s nelegálně získanými prostředky manipuluje samotný pachatel, případně si pro tuto činnost zvolí prostředníky. [37,38]

7.2.3 Informační trestná činnost

Informační trestné činy jsou trestné činy založené na šíření informací, které může mít za následek způsobení újmy, docílit páchání trestné činnosti, ale také shromažďovat data o lidech pro pozdější protiprávní jednání. Můžeme sem zahrnout například trestné činy jako § 180 Neoprávněné nakládání s osobními údaji nebo třeba § 191 Šíření pornografie. [37]

7.2.4 Napadení cizího počítače, jeho programového vybavení a souborů dat v databázích

Útok spočívá ve vytvoření a šíření škodlivých programů. Někdy jsou pachatelem zvoleny škodlivé programy, které vymažou vybraná data nebo provedou blokaci počítače poté, co nastane předem stanovená situace. Proces šíření viru začíná naprogramováním počítačového viru. Druhá část spočívá v šíření škodlivého programu do počítače a v poslední části dochází k útoku viru na data a programy počítače. [37,38]

7.2.5 Neoprávněné pronikání do počítačů, počítačového systému a jeho databází

V tomto případě je využívána zejména internetová síť pro připojení pachatele do vybraného počítače, jeho systému nebo databází. Pachatel musí být schopen obejít ochranná opatření jako například heslo. Pachatelé mohou mít dva cíle. Jedním z nich je ukázat, že se dokáže dostat k databázím, které si pouze prohlédne a se získanými daty nijak dále nemanipuluje. Druhým cílem může být použití získaných dat třeba pro jiné protiprávní jednání nebo k obchodování s nimi. [37,38]

7.2.6 Neoprávněné pokyny k počítačovým operacím

Pachatel neoprávněného pokynu k počítačovým operacím, potřebuje mít přístup k souborům a povolení pro nakládání s nimi, včetně možnosti tvorby a využití vlastních programů nebo nástrojů systému. Pokyn může být zadán samotným útočníkem nebo pomocí jeho programů jsou provedeny neoprávněné počítačové operace. [37,38]

Sedmá kapitola se zabývá pachateli kybernetické kriminality. Jsou zde uvedeny nejčastější motivy a způsoby páchání takovéto trestné činnosti. Vyšetřovatelé při vyšetřování mimo jiné vychází i z těchto znalostí, které jim částečně napomáhají při ustanovení pachatele.

8 VYŠETŘOVÁNÍ KYBERNETICKÉ KRIMINALITY

Kybernetická kriminalita je součástí vědního oboru kriminalistiky. Kriminalistika se zabývá metodami a postupy využívanými k dopadení pachatelů. Vychází z provedených zkoumání obětí, pachatelů a způsobu páchání trestné činnosti. Policisté při svých služebních úkonech používají prostředky, operace a metody kriminalisticky technické a expertní činnosti. Služebními úkony je v tomto případě myšlena prevence, odhalování a vyšetřování kriminality. Protiprávní jednání v kyberprostoru je specifické tím, že při něm zpravidla nezůstávají klasické kriminalistické stopy hmatatelné povahy. Vznikly tedy metody využitelné pro úzkou oblast kriminalistiky, které napomáhají mimo jiné i efektivnímu vyšetřování kybernetické kriminality. Vyšetřování kybernetické kriminality sebou nese obtíže spojené s rychlým vývojem a složitými IT systémy. Vyšetřující policisté musí mít určité znalosti v oblasti informačních technologií, protože pachatelé takovýchto činů jsou chytří a dokáží za sebou smazat zanechané stopy. Poškozený někdy nestojí o to, aby bylo protiprávní jednání zjištěno. Mohla by tím třeba poškozená banka přijít o své zákazníky a býti poškozené její renomé. V roce 1999 vznikla Skupina informační kriminality pod Ředitelstvím služby kriminální policie kriminálního úřadu na Policejním prezídiu. Skupina informační kriminality byl orgánem zaměřeným na metodiky řízení kriminální policie. Pracovní náplní orgánu bylo vytvořit základy pro zjišťování a dokumentaci protiprávního jednání přes internet. Základy měla vytvořit i pro oblast ochrany dat, ochrany duševního vlastnictví v souvislosti s výpočetní technikou, elektronických plateb, obchodů a kryptografické komunikace. [39]

Pro započetí vyšetřování kybernetické kriminality se musí Policie ČR o trestném činu dozvědět. Problémem je rafinovaně skrývané protiprávní jednání v kyberprostoru. Oznamovatelem může být například nespokojený zaměstnanec, který nemá žádný zisk z protiprávního jednání společnosti. Skutek někdy oznámí i sám poškozený. Způsobené škody prostřednictvím kyberprostoru bývají vysoké. Vyšetřování je složité a vyšetřovatelé se musí po delší dobu maximálně soustředit, aby se podařily zjistit a zajistit důležité skutečnosti pro další proces vyšetřování. [39]

Policejní orgán při vyšetřování kybernetické kriminality, se stejně jako u jakékoli jiné kriminality snaží zajistit veškeré potenciální kriminalistické stopy, které by mu mohly napomoci při následném usvědčení pachatele a prokázání jeho viny před soudem.

8.1 Důkazní materiály

Policejní orgán při zajišťování a vyhodnocování důkazních materiálů vychází z českého právního řádu. V oblasti veřejného ani soukromého práva není omezován. Neomezené provádění důkazů a jejich vyhodnocování je možné využít i pro elektronické důkazní materiály. Policejní orgán v přípravném trestném řízení využívá procesních úkonů spojených s vyšetřováním a pátráním. Pro objasnění protiprávního jednání, zjištění pachatele a tím naplnění účelu trestního řádu, je potřebná práce ze strany Policie ČR. Dodržování procesní stránky prováděných úkonů policejním orgánem je zásadní pro naplnění účelu trestního řádu. Procesní úkon z hlediska trestního řádu je úkonem orgánů činných v trestním řízení přiřazovaným k jakékoliv změně v trestně procesních vztazích. Procesní úkony zásadnější pro trestní řízení a zasahující do osobních práv osob, mají přesně stanovenou obsahovou a procesní strukturu. [34,39]

V zákonném ustanovení podle § 89 odst. 2 zákona č. 141/1961 Sb. trestného řádu je uvedeno, co může být považováno za důkaz a kdo může důkazní materiál předložit, vyhledat nebo navrhnout jeho provedení. Za důkazní materiál může být považováno cokoliv, co může napomoci k objasnění protiprávního jednání, přičemž takový důkazní materiál může být od kohokoliv. V trestním řádu nalezneme i související právní ustanovení podle § 110a. V daném paragrafu je hovořeno o tom, že policejní orgán může využít i znalecký posudek, který si sám nevyžádal. Znalecký posudek musí splňovat všechny náležitosti, jako v případě vyžádaného posudku od samotného policejního orgánu. Policejní orgán takovému znalci umožní nahlédnout do spisového materiálu a seznámit se s dalšími podstatnými podklady důležitými pro vypracování znaleckého posudku. U kybernetické kriminality hovoříme například o poskytnutí kopie nosičů nebo ohledání stavu systému počítače a obsahu jeho databází. Trestní řád vychází z předpokladu, že v případě bližšího nespecifikování způsobu provádění důkazů, bude policejnímu orgánu stanoven ze strany soudu. V ustanovení § 112 odst. 1 trestního řádu najdeme i rozlišení listinných a věcných důkazů. Nosiče dat, počítače a další technická zařízení řadíme k věcným důkazům. [34]

8.2 Kriminalistické stopy

Pojem kriminalistická stopa bývá popisován různě, ale podstata zůstává stejná. Kriminalistická stopa je tedy změnou v příčinné či jiné souvislosti s kriminalisticky významnou událostí. Za jinou souvislost je považována zejména souvislost časová nebo místní. Popisovaná změna musí existovat minimálně do jejího zjištění a musí být možné danou změnu zkoumat

pomocí kriminalistických prostředků a metod. Příčinnou souvislostí může být chování pachatele na místě činu, následek použitím nástrojů k páchané trestné činnosti, ale i změny spojované s obranou oběti. Za souvislost časovou nebo místní se považuje průběh protiprávního jednání, které se odehrává v určitou dobu a na určitém místě. Kriminalisticky významnou událostí jsou trestné činy nebo přestupky uvedené v příslušných zákonech, škodlivé působení přírodních sil, nešťastné náhody, náhlá úmrtí nebo sebevraždy. Aby měla stopa kriminalistický významu, nesmí zaniknout dříve, než dojde k jejímu zjištění. Kdyby stopa zanikla dříve, tak by ji policejní orgán nemohl zjistit a tudíž ani zajistit pro následné trestní řízení. Příkladem mohou být stopy vozidla na trávníku pozemku, kde došlo k protiprávnímu jednání. K provedení zkoumání současnými kriminalistickými prostředky a metodami znamená, že není možné bez existujících metod a prostředků u nastalé změny provést zkoumání a tím ji použít při dokazování trestné činnosti. [17]

8.2.1 Význam kriminalistických stop

Kriminalistická stopa má pro policejní orgán kriminalisticky taktický a technický význam. Za kriminalisticky taktický význam jsou považovány informace o tom, jak se dané protiprávnímu jednání odehrálo, o zúčastněných osobách a podobně. Pro objasnění skutku je důležitá i kriminalisticky technická hodnota stopy. Bohužel není možné říci, že by každá zajištěná stopa měla takovou hodnotu. Jedná se o možnost ztotožnění pachatele, zvířete nebo věcí, které stojí za vytvořením kriminalistické stopy. [17]

8.2.2 Kriminalistické stopy u kybernetické kriminality

Kybernetická kriminalita sebou přináší kromě klasických stop i specifické stopy přímo pro její problematiku. Zajišťované kriminalistické stopy se liší případ od případu. Stopy týkající se kybernetické kriminality je možné rozdělit na paměťové, materiální a další důkazy pro soud. [36]

8.2.3 Paměťové stopy

U paměťových stop se již podle názvu jedná o stopy získané z paměti osob na základě provedených výslechu možných svědků, prověřovaných nebo oběti. Paměťové stopy mohou vyšetřovatelům pomoci získat informace podstatné pro další úkony. Mohou být použity také jako důkazní materiál u soudu. Paměťové stopy obsahují veškeré informace, které by mohly napomoci k objasnění daného jednání. Jde tedy například o průběh událostí a informací

o chování a jednání pachatele během celého procesu protiprávního jednání. U počítačových stop je důležitá co nejrychlejší reakce, jelikož dané stopy po nějaké době již nemusí vůbec existovat. [36]

8.2.4 Materiální stopy a další důkazy pro soud

Materiální stopy a další důkazy můžeme rozdělit na:

- počítačové stopy,
- věcné, listinné důkazy a stopy,
- a účetní stopy.

Specifickými stopami jsou především počítačové stopy. Jedná se informaci či její změnu na materiálním nosiči, ke které byla použita výpočetní technika. Ke změně a vzniku stopy dochází při dopouštění se protiprávního jednání. Jde o stopy nesoucí jinou významnou informaci. Jejich hodnota může být kriminalisticky taktická i důkazní. Setkáváme se se třemi druhy počítačových stop. První druhem jsou stopy na nosičích informaci a data v nich obsažená. Patří zde například cd, dvd, paměťové karty, pevné disky a podobně. Druhým zástupcem jsou stopy na kancelářské a organizační technice, která ukládá a zapisuje digitální data. Do této skupiny můžeme zařadit elektronická zařízení novější mobilní telefony, diktafony, faxy a jiné, kde dochází k ukládání, změnám a smazání digitálních dat. Na moderních tiskárnách můžeme zjistit i na které tiskárně proběhl tisk a jaký soubor byl vytištěn. Jako třetí typ jsou stopy na výpočetní technice a neoprávněná manipulace s danou technikou, které například sníží možnost používání výpočetní techniky. [36]

Jako dalšími specifickými stopami a důkazním materiálem pro soud jsou věcné, listinné důkazy a stopy, které poukazují na změnu nebo padělek listin. Při páchání kybernetické kriminality se využívají různé doklady. Doklady mohou být skutečné, ale nelegálně upravené nebo vytvořené. Danou trestnou činnost mohou provázet i nové písemnosti. [36]

Účetní stopy jsou další specifickou skupinou kriminalistických stop u kybernetické kriminality. Nachází se například v účetních uzávěrkách, výkazech, ale i v údajích prvotních dokladů. Účetní stopy mohou mít různou podobu. Mohou mít papírovou podobu, podobu elektrických dat nebo může jít i o konkrétní program. [36]

8.3 Situace při vyšetřování kybernetické kriminality

Typická situace při vyšetřování kybernetické kriminality je přiřazována spojitosti se zvláštním režimem podle zákonů, které chrání informace, hospodářské, státní nebo bankovní tajemství. K vyšetřování kybernetické kriminality přiřazujeme čtyři typické vyšetřovací situace. První situace spočívá v tom, že na základě nashromážděných informací můžeme v jednání spatřovat trestný čin, avšak nemůžeme jednoznačně určit konkrétního pachatele ani způsob spáchání trestného činu. Následek nebo vzniklá škoda a motiv trestného činu mohou býti známy, ale není to podmínkou. Při takovéto situaci se policisté nejprve snaží zjistit co nejvíce informací o způsobu spáchání a osobě pachatele trestného činu. V případě, že už byla provedena analýza protiprávního jednání v rámci poškozené společnosti a byly prohlédnuté potřebné soubory nebo již bylo s paměťovými médii manipulováno, policejní orgán musí zajistit revizní nebo kontrolní zprávu. Policie ČR musí dále provést šetření ke zjištění osoby, které s paměťovým médiem manipulovala a zeptat se jí z jakého důvodu a jakým způsobem s daným médiem pracovala. Policejní orgán rovněž přibere znalce z oboru výpočetní techniky, zkonzultuje s ním zajištění důležitých materiálů pro zkoumání a provede příslušné úkony. Pokud nebylo protiprávní jednání analyzováno poškozenou společností, nebylo nijak manipulováno s paměťovým médiem ani nebyly prohlédnuty potřebné soubory, policejní orgán rovněž přibere znalce z oboru výpočetní techniky. Znalec s příslušnými zaměstnanci poškozené společnosti nebo s vlastníkem programů, databází a systémů, zajistí potřebného zařízení, databáze nebo programové vybavení, aby mohl provést odborné zkoumání. [40]

Druhou častou vyšetřovací situací je situace, kdy pomocí nashromážděných informací je v jednání pachatele spatřován trestný čin a je znám i způsob provedení. Nejsou však zjištěny skutečnosti umožňující ztotožnit osobu pachatele. Opět následek nebo vzniklá škoda a motiv trestného činu mohou býti známy, ale také nemusí. Kromě získávání důkazních materiálů k známým skutečnostem, se policisté v počátku zaměřují na získání informací vedoucích ke zjištění osoby pachatele. Počet možných pachatelů je často zúžen podle způsobu provedení. Analýza provedená za přítomnosti znalce z oblasti výpočetní techniky a dalších odborníků zjišťujících způsob provedení, je důležitým podkladem pro následné typování možného pachatele. Policejní orgán mimo jiné provádí i šetření k osobě pachatele z jiných zdrojů spolupracujících s policií. [40]

Další vyšetřovací situace spočívá v zjištění informací, ze kterých je zřejmé, že byl spáchán trestný čin a získané informace vedou ke konkrétní osobě pachatele. Není znám způsob

spáchání trestného činu. Způsobená škoda nebo následek a motiv činu doposud nejsou známy. Při dané počáteční vyšetřovací situaci policista sdělí obvinění osobě pachatele. Policejní orgán zajistí objekty důležité k provedení zkoumání z oblasti výpočetní techniky. Pro policejní orgán jsou stěžejní výslechy obviněného a znalců nebo odborníků zaměřené na objasnění a prokázání způsobu provedení. Pachatel má při výslechu dvě možnosti. Při odmítnutí vypovídat se policejní orgán musí snažit zajistit jiné důkazní materiály ke způsobu spáchání. Při vypovídaní pachatele o technických detailech spáchání protiprávního jednání a podobně, je vhodné protokol o výslechu obviněného zaslat znalci pro lepší představu k provedení znaleckého zkoumání, ale také pro možnost ověření pravdivosti tvrzení. Policista provádějící vyšetřování si musí být vědom toho, že při dokazování je třeba prokázat naplnění všech znaků skutkové podstaty trestného činu nebo trestných činů. Rychle rozvíjející se výpočetní technologie umožňují pachatelům vynalézat stále nové způsoby páchání trestné činnosti související s kybernetickou kriminalitou. [40]

Poslední nejčastější vyšetřovací situace spočívá v tom, že jsou zjištěny informace vedoucí k označení protiprávního jednání za trestný čin. Osoba pachatele i způsob provedení je znám. Vzniklá škoda, následek mohou býti známy, a to platí i pro motiv činu. Policejní orgán ve spolupráci s odborníky provede vyhodnocení získaných podkladů. Následuje sdělení obvinění osobě pachatele. Dále již vyšetřující policista pracuje na poskládání získaných podkladů do logických souvislostí a zajištění zkoumání z oboru výpočetní techniky. Tahle vyšetřovací situace umožňuje policejnímu orgánu si vytyčit obecné vyšetřovací verze o trestném činu a zaměřit se na prověření a prokázání protiprávního jednání. [40]

8.4 Znalec a trestní řízení

Soudním znalcem je fyzická osoba, která byla předsedou senátu nebo ministrem spravedlnosti jmenována znalcem v konkrétním oboru. Soudní znalec může být jmenován i znalcem několika oborů. Ke znalcům se v současné chvíli vztahuje zákon č. 36/1967 o znalcích a tlumočnících, který bude v blízké době nahrazen zákonem č. 254/2019, účinným od 01. 01. 2021. Hlavní náplní znalců jsou podání vysvětlení, odborná vyjádření a znalecké posudky z oblasti jejich oboru. V oblasti trestního řízení orgány činné v trestním řízení žádají znalce o odborná vyjádření i znalecké posudky. Znalec musí pro jeho jmenování splnit přísná kritéria, jelikož má pro trestní řízení trestním řádem přiznané významné procesní postavení. Znaleckou činnost provádějí kromě samotných znalců, také ústavy. Znalci musí postupovat v souladu s právními normami. Příkladem je třeba ustanovení § 89 odst. 2 nebo ustanovení

§ 105 až § 111 zákona č. 141/1961 Sb. trestního řádu, ustanovení § 175 zákona č. 40/2009 Sb., ale také různá ustanovení správního řádu, občanského řádu nebo třeba právní normy související s oceňováním majetku a podobně. V trestním řádu jsou přesně stanoveny důvody k přibrání znalce. V ustanovení § 105 odst. 1 daného zákonu je uvedeno, že může být znalec přibrán, když je potřeba odborné vědomosti vedoucí k objasnění skutečností pro trestní řízení. Proti odbornému vyjádření či znaleckému posudku není přípustný opravný prostředek. Trestní řád umožňuje přibrání znalce i podle § 110 trestního řádu, které se využívá pouze ve výjimečných nebo velmi složitých případech, kdy je třeba specifické vědecké zhodnocení. Zde je možné přibrat ke znaleckému zkoumání vědecký ústav, organizaci zabývající se znaleckými úkony, vysokou školu nebo státní orgán. Podle § 116 odst. 2 je vyžadováno zkoumání duševního stavu v oblasti zdravotnictví. Zkoumání je nařizováno na návrh státního zástupce soudcem. V tomto případě může být podána stížnost proti tomuto usnesení či nařízení soudce. Znalecký posudek může být předložen i ze strany oběti nebo pachatele. Trestní řád umožňuje i takovou variantu. Aby mohl být znalecký posudek považován za důkazní materiál, musí být v souladu s ustanovením § 110a. To znamená, že musí obsahovat stanovené náležitosti a znalec musí být poučen o následcích nepravdivého znaleckého posudku. Z ustanovení § 106 trestního řádu lze odvodit, kdo má znalce poučit. Jde o orgán činný v trestním řízení, který si znalecký posudek vyžádal. Znalec musí být ve smyslu § 106 trestního řádu poučen v případě přibrání osobou poškozenou nebo obviněnou. V trestním řádu však není stanoveno, zda je nutné poučit subjekt v případě vyžádání odborného vyjádření. V případě poučení nejde o procesní chybu, ale není možné subjekt postihovat za nepravdivost odborného vyjádření. To platí i u znalce. Rozdílem mezi odborným vyjádřením a znaleckým posudkem je, že u odborného vyjádření nemusí být osoba v postavení znalce. Z hlediska odbornosti by měl mít vyšší kvalitu posudek od znalce. Odborná vyjádření jsou tedy využívána zejména v případech méně náročných na odbornost a méně závažných. Příkladem jsou například znalecké posudky při rozboru krve na množství alkoholu, oceňování majetku a podobně. Ve stanovisku Nejvyššího státního zastupitelství č. 9/2003 Sb. se uvádí, že znalec je přibírán orgány činnými v trestním řízení, když je potřebný pro složitost posuzované otázky s potřebou většího množství času, nutné využívání znalostí z odborných knih, používání podstatných vědeckých poznatků a podobně. Práce znalce by měla být využita také pro posouzení příčinných souvislostí mezi jednáním a následkem pachatele. Odborné vyjádření stojí vždy až za znaleckým posudkem, když je třeba přibrat znalce. U znaleckých činností se předpokládá dokončené vysokoškolské vzdělání a neustálé samostudium znalce.

Zatímco pro odborné vyjádření postačuje osoba s odbornými znalostmi z oboru, kdy u některých oborů postačuje mít středoškolské odborné vzdělání nebo jen vyučení v oboru s maturitou. Posouzení potřebnosti znaleckého posudku nebo odborného vyjádření je tak zejména na policejním orgánu, který musí zhodnotit složitost a úroveň potřebné odbornosti podle potřebného úkonu. Odborné vyjádření je jen listinným důkazem, proti kterému nelze podat námitky ani na odborné znalosti zpracovávající osoby. Trestní řád neumožňuje provést podání vysvětlení s osobou zpracovávající odborné vyjádření ani v postavení svědka. Při neuspokojivém výsledku odborného vyjádření může být daná osoba pouze vyzvána k napravení určitých nesrovnalostí. [41]

8.5 Specifika předmětu a podmětu vyšetřování

Ustanovení § 89 odst. 1 zákona č. 141/1961 Sb. trestního řádu obsahuje požadavky podstatné pro trestní stíhání. Specifika předmětu vyšetřování záleží na skutkových podstatách trestných činů a formách páchání trestné činnosti. Zvláštností předmětu je, že povahu kybernetické kriminality je nutno dovodit podle způsobu spáchání trestného činu. U kybernetické kriminality je specifické, že u každé z forem páchání se prokazuje:

- jaký počítač byl použit k protiprávnímu jednání,
- jestli jde o jeden skutek nebo o několik skutků,
- zda za protiprávním jednáním stojí jedna osoba nebo více osob,
- jak bylo protiprávní jednání provedeno,
- jaké měl pachatel oprávnění k využívání počítače, nosiče informací a provedení takového typu úkonu,
- jaké jsou znalosti pachatele o programech, výpočetní technice a sítí s elektronickými komunikacemi,
- jaký byl motiv pachatele,
- jestli byla zajištěna výpočetní technika použitá k protiprávnímu jednání a kdy k zajištění došlo,
- za jaké situace došlo k protiprávnímu jednání,
- zda vznikla nějaká škoda a v jaké výši,
- a jiné. [36]

Specifika podnětů pro vyšetřování kybernetické kriminality vyplývají ze způsobu zjištění takového protiprávního jednání a následného sdělení policejnímu orgánu. Protiprávní jednání může být oznámeno prostřednictvím oznámení od občana. Oznámení od občana může

míst několik forem. Písemnou formu, kdy je podnět zaslán policejnímu orgánu například poštou nebo datovou zprávou. Telefonickým oznámení na linku 112 nebo linku 158. Oznámení může být podáno i osobně na jakémkoliv útvaru Policie ČR. Písemné oznámení bývá někdy podáváno i přes státní zastupitelství. Poškozený podává oznámení zejména kvůli náhradě způsobené škody a pro odhalení a následné potrestání pachatele. Někdy jsou oznámení podávána za organizaci nebo třeba za občanské sdružení. Oznamovatelé kybernetických trestných činů většinou nejsou zkušení v problematice počítačových sítí a informačních systémů. Tomu odpovídá i obsah samotného oznámení, které často nebývá podrobně popsáno. Jde většinou o obecný text, který potřebuje policejní orgán doplnit pro určení, zda jde o trestný čin či nikoliv a případně pro potřeby dalšího prověřování. Policejní orgán při prověřování takového oznámení by měl od počátku komunikovat s pracovníky Odboru kriminalistické techniky a expertíz nebo Kriminalistického ústavu, jež spadají pod Policii ČR, případně se znalci. Tento krok je podstatný pro následnou realizaci neodkladných a neopakovatelných úkonů. [36]

Podnět může být podán také od kontrolních, revizních a inspekčních orgánů různých organizací. Mělo by se jednat o nejčastější a kvalitně popsané oznámení týkající se trestného činu v oblasti kybernetické kriminality. Bohužel realita je jiná. Často oznámení nejsou ani podávána, jelikož protiprávní jednání není vůbec zjištěno. Důvodem neoznámení takového jednání bývá strach ze ztráty klientů a ohrožení dobrého jména společnosti. V případě oznámení od některého z orgánů organizace bývají svým obsahem na vyšší úrovni než při oznámení od samotného občana. Policejní orgán musí stejně provést ověření oznámení, případně vyžádat doplnění informací důležitých pro trestní řízení. Některá oznámení mohou obsahovat problém spočívající ve standardní administrativní chybě. Nesrovnalosti jsou důsledně prověřovány u dokladů pro správné zúčtovací operace. Odhalování protiprávního jednání v kyberprostoru mají za povinnost také další orgány, například zpravodajské služby. Ty pak policejnímu orgánu prostřednictvím trestního oznámení zasílají podklady k možnému spáchání trestného činu v kyberprostoru. Skrytost kybernetických trestných činů může spočívat v nedostatečné kontrole při vybírání finanční hotovosti, právním předpisem nestanovená pravidla pro správné ukrývání informací ohledně přístupu ke konkrétním datům, chyby v počítačových systémech v nesouladu se spolehlivostí a bezpečností u používaných počítačů, ale také v odhalení neoprávněného hospodaření s penězi na základě obcházení kontrolního systému a další. [36]

Protiprávní jednání může být zjištěno samotným policejním orgánem, na základě kvalitní operativní pátrací činnosti ze strany útvaru či útvarů služby kriminální policie a vyšetřování. Policie ČR může využívat operativní techniky u zvlášť závažných trestný činu, toto vyplývá ze zákona č. 273/2008 Sb. o Policii ČR. Další oprávnění vyšetřovatele je již zahrnuto v trestním řádu. Hovoříme například o použití agenta, sledování věcí a osob nebo předstíraný převod. Policejní orgán má možnost použít i informátora k získání potřebných informací. Informace se kriminalisté snaží získat využitím jiných osob a zdrojů a nosičů informací. Podklady získané samotnou Policií ČR bývají pro trestní řízení v té nejlepší kvalitě, a to i proto, že policejní orgán ví, jaké informace přesně pro trestní řízení potřebuje a na jejich získání se zaměřuje. [36]

Ostatní druhy podnětů spočívají zejména v anonymních oznámeních nebo informacích od soukromých bezpečnostních a detektivních agentur. Jejich četnost není tak vysoká jako některých z výše popsaných podnětů. Anonymní oznámení využívají osoby například pro poškození jména dané osoby a podobně. Takové podněty mohou obsahovat lživé informace. Podněty od bezpečnostních a detektivních organizací mohou pomoci k odhalení trestného činu, avšak musí být bráno v potaz jejich postavení v trestním řízení. Poznatky jsou někdy získávány i ze strany médií nebo při odhalování jiného trestného činu. [36]

Osmá kapitola se zaměřuje na vyšetřování kybernetické kriminality. Nejprve jsou uvedeny základní informace o samotném vyšetřování trestné činnosti. Podkapitola týkající se důkazního materiálu obsahuje informace, co je považováno za důkazní materiál a jak může policejní orgán důkazní materiál získat. Celé vyšetřování je založeno na získávání důkazních materiálů pro ustanovení pachatele, proto je snahou Policie ČR nashromáždit důkazů co nejvíce. Následuje popis kriminalistické stopy, jejího významu pro trestní řízení a jejich rozdělení a bližší specifikace z oblasti kybernetické kriminality. Další podkapitolu tvoří vyšetřovací situace. Jedná se o časté kombinace okolností, se kterými se vyšetřovatelé kybernetické kriminality setkávají. Dané kombinace okolností jsou rozděleny do čtyř častých vyšetřovacích situací. U konkrétních okolností jsou uvedeny některé z prvotních kroků policejního orgánu. Znalec v trestním řízení je další z podkapitol. V podkapitole je rozebráno postavení a úloha znalce v trestním řízení. Závěr obsahuje informace k předmětu a podmětu vyšetřování, které jsou specifické pro kybernetickou kriminalitu. Předmět obsahuje obecné otázky

týkající se konkrétního protiprávního jednání, na které se snaží vyšetřovatel během vyšetřování odpovědět. Za podmět se považuje způsob, jakým se policejní orgán dozví o protiprávním jednání.

Závěr teoretické části

Následně bude shrnuta teoretická část s výhledem na praktickou část. Teoretická část diplomové práce se skládá z devíti kapitol, včetně této kapitoly. V rámci první části práce jsou postupně popsány jednotlivé dílčí oblasti vztahující se ke kybernetické kriminalitě a kybernetické bezpečnosti. Čtenáři může posloužit pro vytvoření představy o kybernetické kriminalitě. Obsahová část je tvořena od základních pojmů přes instituce a právní předpisy až po základní informace o procesu vyšetřování kybernetické kriminality ze strany policejního orgánu. Následovat bude praktická část, ve které budou dále uvedeny zákonná ustanovení z trestního řádu umožňující policejnímu orgánu získávat informace pro trestní řízení. Dále bude uvedeno protiprávní jednání přes počítač spočívající v naplnění skutkové podstaty Podvodu podle § 209 trestního zákoníku. Nebude chybět rozbor několika rizik spojených s podvodným jednáním. Na závěr bude provedena analýza rizik pro oblast kybernetické kriminality páchané na mládeži s využitím sociálních sítí.

II. PRAKTICKÁ ČÁST

9 OPRÁVNĚNÍ POLICIE ČR PŘI VYŠETŘOVÁNÍ KYBERNETICKÉ KRIMINALITY

Začátkem každého prověřování ze strany policejního orgánu je buď oznámení od fyzické či právnické nebo vlastní zjištění policejního orgánu. Při prověřování protiprávního jednání, policista z příslušného útvaru Policie ČR zjišťuje skutečnosti, zda skutek naplňuje skutkovou podstatu přestupku nebo trestného činu. V případě přestupku, policejní orgán postupuje zejména v souladu se zákonem o Policii ČR č. 273/2008 Sb. a zákona o odpovědnosti za přestupky a řízení o nich č. 250/2016 Sb. V téhle práci se budeme zabývat pouze trestním řízením, tedy především zákonem č. 141/1961 Sb., trestním řádem.

9.1 Ustanovení § 7 trestního řádu

Policejní orgán při spolupráci s dalšími policejními útvary v rámci České republiky, využívá žádosti podle ustanovení § 7 z. č. 141/1961, trestního řádu, kde je uvedeno: *„Orgány činné v trestním řízení jsou povinny si navzájem pomáhat při plnění úkolů vyplývajících z tohoto zákona“*. [14] Rovněž se používá paragrafového znění podle § 53 odst. 1 z. č. 141/1961, trestního řádu: *„Soud, státní zástupce a policejní orgán vykonávají jednotlivé úkony trestního řízení ve svém obvodu zpravidla sami. Mimo svůj obvod vykonávají jednotlivé úkony trestního řízení dožádáním okresního soudu, státního zástupce nebo policejního orgánu, v jehož obvodu má být úkon proveden, nebo prostřednictvím videokonferenčního zařízení; není-li úkon prováděn prostřednictvím videokonferenčního zařízení, vykonají jej mimo svůj obvod sami, jen jestliže věc nesnese odkladu nebo je-li toho pro řádné posouzení věci nezbytně třeba*“. [14] Takovéto oprávnění je využíváno při zjištění skutečností v systémech Policie ČR nebo zjištěním, že by jiný policejní útvar mohl pomoci při objasňování skutečností. Kromě informací napomáhajícím ke zjištění nebo usvědčení pachatele mohou získané informace rovněž vést k odložení skutku podle ustanovení § 159 odst. 1 z. č. 141/1961, trestního řádu. Příkladem je situace, kdy oznamovatel si již někdy v minulosti takovéto oznámení vymyslel.

9.2 Ustanovení § 7b trestního řádu

Pro oblast kybernetické kriminality je důležité ustanovení § 7b z. č. 141/1961, trestního řádu. V prvních dvou odstavcích výše uvedeného právního ustanovení, jsou uvedeny základní

podmínky pro uchování důležitých dat pro trestní řízení a pro zamezení přístupu k počítačovému systému.

Odstavec 1: *„Je-li zapotřebí zabránit ztrátě, zničení nebo pozměnění dat důležitých pro trestní řízení, která jsou uložena v počítačovém systému nebo na nosiči informací, lze nařídit osobě, která uvedená data drží nebo je má pod svojí kontrolou, aby taková data uchovala v nezměněné podobě po dobu stanovenou v příkazu a učinila potřebná opatření, aby nedošlo ke zpřístupnění informace o tom, že bylo nařízeno uchování dat“.* [14]

Odstavec 2: *„Je-li to zapotřebí k zabránění pokračování v trestné činnosti nebo jejímu opakování, lze nařídit osobě, která drží nebo má pod svojí kontrolou data, která jsou uložena v počítačovém systému nebo na nosiči informací, aby znemožnila přístup jiných osob k takovým datům“.* [14]

V obou případech je potřeba vydání příkazu. Příkaz může být vydán předsedou senátu, ale v přípravném řízení také státním zástupcem nebo policejním orgánem. Policejní orgán vydává příkaz pouze v případech, kdy věc nesnese odkladu. V tomto případě ani policejní orgán nepotřebuje zpětného vydání souhlasu, jak je tomu například u předstíraného podvodu nebo sledování osob, které bude popsáno v dalších podkapitolách. Vydaný příkaz je pak od příslušeného orgánu bez zbytečného odkladu doručen osobě, které se týká. Příkaz může být vydán maximálně na 90 dnů. [14]

9.3 Ustanovení § 8 trestního řádu

Oprávněním Policie ČR jsou rovněž žádosti zejména státním orgánů, fyzickým a právnickým osobám podle ustanovení § 8 odst. 1 z. č. 141/1961, trestního řádu: *„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. Státní orgány jsou dále povinny neprodleně oznamovat státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin“.* [14] Policejní orgán využívá takového oprávnění pro vyžádání informací nebo podkladů od fyzických nebo právnických osob, které jsou důležité pro trestní řízení.

V některých případech je uplatňováno ustanovení § 8 odst. 4 písm. b) trestního řádu, u oznamovatelů trestného činu, kde je uvedeno: *„Plnění povinností podle odstavce 1 lze odmítnout s odkazem na povinnost zachovávat tajnost utajovaných informací chráněných zvláštním zá-*

konem nebo státem uloženou nebo uznanou povinnost mlčenlivosti; to neplatí, b) při vyřizování dožádání orgánu činného v trestním řízení o trestném činu, kde dožádaná osoba je současně oznamovatelem trestného činu". [14] Takové oprávnění je využíváno zejména v případech, kdy se oznamovatel hájí mlčenlivostí ke sdělení bližších informací ohledně oznamovaného skutku.

Záměrně odděleně jsou uvedeny další odstavce uplatnitelné pro vyšetřování kybernetické kriminality. Jedním z nich je ustanovení § 8 odst. 2 trestního řádu, které je využíváno pro získání informací podléhajících bankovnímu tajemství. Kromě daňové problematiky je zde využíváno následujícího znění: *„Jestliže je toho v trestním řízení třeba k řádnému objasnění okolností nasvědčujících tomu, že byl spáchán trestný čin, k zjištění povahy, rozsahu nebo umístění věcí pro účely jejich zajištění, k zjištění majetkových poměrů obviněného nebo pro účely zajištění výkonu trestní sankce, může státní zástupce a po podání obžaloby nebo návrhu na potrestání předseda senátu požadovat údaje, které jsou předmětem bankovního tajemství. Údaje získané podle tohoto ustanovení nelze využít pro jiný účel než pro trestní řízení, v jehož rámci byly vyžádány"*. [14] Policejní orgán tak může získat informace o bankovním účtu, který je součástí spisového materiálu. Státnímu zástupci musí v zasílaném návrhu na postup podle § 8 odst. 2 trestního řádu uvést konkrétní důvody, proč vyžaduje získání informací k bankovnímu účtu. Dále v žádosti uvede přesného číslo žádaného bankovního účtu a název příslušné banky. Neměla by chybět ani informace, jakým způsobem policejní orgán přišel k danému číslu bankovnímu účtu.

Zvláštní význam má pro policejní orgán v případě kybernetické kriminality, pátý odstavec, ve kterém je uvedeno*: „Nestanoví-li zvláštní zákon podmínky, za nichž lze pro účely trestního řízení sdělovat informace, které jsou podle takového zákona utajovány, nebo na něž se vztahuje povinnost mlčenlivosti, lze tyto informace pro trestní řízení vyžadovat po předchozím souhlasu soudce. Tím není dotčena povinnost mlčenlivosti advokáta podle zákona o advokacii"*. [14] Vyšetřovatelé mohou dané paragrafové znění využít pro utajované informace, avšak není blíže specifikováno, jak takové informace získat.

9.4 Ustanovení § 82 - 85 trestního řádu

Ustanovení § 82 - 85 trestního řádu se zabývají domovními prohlídkami, osobními prohlídkami a prohlídkami nebytových prostor. Jedná se o další oprávnění policejního orgánu uplatňované u kybernetické kriminality. V daných paragrafových zněních jsou uvedeny důvody

k provedení domovní prohlídky, kdo může nařídit každou z prohlídek a včetně postupu u domovních prohlídek. Osoba, u které je prohlídka prováděna má povinnost strpět dané úkony. Domovní prohlídku lze provést pouze v případech, kdy má policejní orgán důvodné podezření, že se na některém z daných míst nachází osoba nebo věc důležitá pro trestní řízení.

9.5 Ustanovení § 88a trestního řádu

Potřebné informace týkající se IP adres je možné získat na základě paragrafu 88a z. č. 141/1961 Sb., trestního řádu. V tomto paragrafu jsou přesně definované konkrétní trestné činy a trestní sazby, pro které je možné využít daného oprávnění. V odstavci jedna jsou uvedeny podmínky pro jeho uplatnění.

Odstavec 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“*. [14] Po skončení trestního řízení je orgán činný v trestním řízení povinen informovat samotného uživatele. To platí v případě, že je totožnost uživatele

známa. Skutečnosti, ve kterých není třeba vyrozumívat uživatele, jsou uvedeny v třetím odstavci. Vydání příkazu k údajům o uskutečněném telekomunikačním provozu není potřeba, jestliže policejní orgán získá souhlas přímo od uživatele zařízení. [14]

9.6 Ustanoven § 158 odst. 6 trestního řádu

Policejní orgán pro získávání informací využívá základního kamene pro všechny trestné činy, a tím je výslech osob. Výslech osoby spočívá v sepsání úředního záznamu o podaném vysvětlení podle § 158 odst. 6 trestního řádu. Podání vysvětlení může být požadováno od osob, kterých se protiprávní jednání týká nebo, které svou výpovědí mohou přispět k zjištění doposud neznámých skutečností nebo informací vedoucí k osobě pachatele. Nejčastějšími osobami, kterých se podání vysvětlení týká, jsou v postavení poškozeného, svědka nebo prověřovaného (v závislosti na stádiu trestního řízení). Problém je zejména u osob v postavení prověřovaného, podezřelého či obviněného, které nemají povinnost mluvit pravdu a tudíž v častých případech policejnímu orgánu lžou. Zatímco svědci musí mluvit pravdu a nic nezamlčet, s tím, že jsou poučení o následcích křivého obvinění podle § 345 trestního zákoníku a křivé výpovědi podle § 346 trestního zákoníku. Problémem může být ovšem skutečnost, že pro kvalifikování křivého obvinění nebo křivé výpovědi by musel policejní orgán nashromáždit důkazní materiály, které by naplnění skutkové podstaty některého z trestných činů prokazovalo. Ne vždy je snadné prokázat takového jednání.

Podání vysvětlení předchází využití oprávnění policejního orgán a tedy vyzvat osobu podle ustanovení § 158 odst. 7 trestního řádu, aby se dostavila v konkrétní dobu a na konkrétní místo k podání vysvětlení. V případě, že se osoba na výzvu policejního orgánu bez dostatečné omluvy nedostaví, může být předvedena. Rovněž za nedostavení se, hrozí osobě pořádková pokuta až do výše 50.000,-Kč.

V případě zajištění potřebných důkazních materiálů, policejní orgán osobě pachatele sdělí podezření nebo obvinění a osobu jako podezřelou nebo obviněnou znovu vyslechne, a to na příslušný protokol.

9.7 Ustanovení § 158c trestního řádu

Pod ustanovením § 158c trestního řádu se skrývá předstíraný převod. *„Předstíraným převodem se rozumí předstírání koupě, prodeje nebo jiného způsobu převodu předmětu plnění včetně převodu věci,*

a) k jejímuž držení je třeba zvláštního povolení,

b) jejíž držení je nepřípustné,

c) která pochází z trestného činu, nebo

d) která je určena ke spáchání trestného činu.“ [14]

V oblasti kybernetické kriminality hovoříme o převodech různých dat, které je nezákonné a zároveň postižitelné zákonem č. 40/2009 Sb., trestním zákoníkem. Příkladem jsou třeba převody různých hesel. Pro využití daného oprávnění musí mít policejní orgán písemný souhlas od dozorujícího státního zástupce. To neplatí v případě, že věc nesnese odkladu. V takovém případě, policejní orgán je povinen si povolení zpětně vyžádat od státního zástupce. Je však limitován 48 hodinami. Pokud povolení do 48 hodin nezíská, musí úkony spojené s předstíraným převodem ukončit a nesmí získané skutečnosti v trestním řízení použít. Policejní orgán také musí sepsat záznam o předstíraném převodu a tento ve lhůtě 48 hodin předat státnímu zástupci. Cílem předstíraného převodu je získat důvěru pachatele a na základě toho i více důkazních materiálů pro trestní řízení. [14]

9.8 Ustanovení § 158d trestního řádu

Oprávnění sledování osob a věcí podle § 158d trestního řádu, je vymezeno v odstavci jedna. *„Sledováním osob a věcí (dále jen "sledování") se rozumí získávání poznatků o osobách a věcech prováděné utajovaným způsobem technickými nebo jinými prostředky. Pokud policejní orgán při sledování zjistí, že obviněný komunikuje se svým obhájcem, je povinen záznam s obsahem této komunikace zničit a poznatky, které se v této souvislosti dozvěděl, nijak nepoužít.“* [14]

V případě pouhého sledování, policejní orgán nepotřebuje žádné povolení. Jestliže policejní orgán má v plánu si sledování nahrávat nebo fotit, tak již potřebuje písemné povolení ze strany státního zástupce. Záznamy získané na základě daného povolení státního zástupce, je možné využít také u prověřování jiného úmyslného trestného činu nebo se souhlasem dané osoby. Ve třetím odstavci je pak uvedeno: *„Pokud má být sledováním zasahováno do nedotknutelnosti obydlí, do listovního tajemství nebo zjišťován obsah jiných písemností a záznamů uchovávaných v soukromí za použití technických prostředků, lze je uskutečnit jen na základě předchozího povolení soudce. Při vstupu do obydlí nesmějí být provedeny žádné jiné úkony než takové, které směřují k umístění technických prostředků“.* [14]

Žádost o povolení sledování musí být opodstatněna podezřením z konkrétního trestného činu. U známých totožností osob se uvádí jejich osobní údaje a rovněž se uvádí informace známé o věcích, u nichž je sledování prováděno. Povolení může být poskytnuto na dobu až šesti měsíců, která může být příslušným orgánem činným v trestním řízení znovu prodloužena až o šest měsíců. Rozdílem mezi sledováním na základě focení, nahrávání a sledování uvedeném ve třetím odstavci je tedy v osobě vydávající povolení. V prvním případě postačuje povolení státního zástupce, avšak v druhém případě již policejní orgán potřebuje povolení soudce. Dalším rozdílem je, že sledování v prvním případě může být zahájeno bez souhlasu státního zástupce, pokud věc nesnese odkladu. Platí zde to stejné jako u předstíraného převodu. Policejní orgán tedy musí do 48 hodin zpětně zažádat o povolení státního zástupce a zajistit si dané povolení. V případě zamítnutí ze strany státního zástupce, musí být sledování ukončeno a záznamy musí být zničeny a informace z nich nesmí být nijak využity. Není třeba povolení v prvním ani druhém případě, jestli máme souhlas od osoby, jejíž sledování je prováděno. Osoba může takový souhlas později odvolat. V takovém případě policejní orgán musí sledování ukončit. Aby mohly být záznamy ze sledování využity jako důkazní materiál, policejní orgán k nim musí sepsat protokol. V odstavci 9 se setkáváme se specifickým oprávněním: *„Provozovatelé telekomunikační činnosti, jejich zaměstnanci a jiné osoby, které se na provozování telekomunikační činnosti podílejí, jakož i pošta nebo osoba provádějící dopravu zásilek jsou povinny bezúplatně poskytovat policejnímu orgánu provádějícímu sledování podle jeho pokynů nezbytnou součinnost. Přitom se nelze dovolávat povinnosti mlčenlivosti stanovené zvláštními zákony“.* [14]

Devátá kapitola se zabývala oprávněním policejního orgánu při vyšetřování kybernetické kriminality. Byla zde zmíněna konkrétní právní ustanovení z trestního řádu využívaná k získání informací podstatných pro trestní řízení.

10 PŘÍPADOVÁ STUDIE NA VYBRANÉ PODVODNÉ JEDNÁNÍ PŘES POČÍTAČ

Před začátkem čtení případové studie bych chtěl dopředu uvést, že všechna jména osob fyzických i právnických, data narození, částky, data i adresy, včetně příběhu nejsou založeny na pravdě a jsou využity pouze pro lepší představu a orientaci.

10.1 Obsah oznámení

Dne 1. 1. 2020 panu Janu Novákovi narozenému 3. 3. 1980 (fiktivnímu jménu) na adresu předchozího bydliště Krátká 111, 220 11 Malá Ves, přišla výzva k úhradě neuhrazené splátky od společnosti „X“, s tím, že zastupuje společnost „Y“ jako společnost vymáhající dluhy. Pan Novák je v dopise informován o tom, že splátka jeho smlouvy o úvěru se společností „Y“ je již 15. den po splatnosti. Na to byl opakovaně upozorňován formou sms zpráv a emailů. Tímto dopisem je pan Jan Novák vyzván k uhrazení částky ve výši 11.899,-Kč na bankovní účet číslo 69855896226/0111, jinak bude zahájeno inkasní řízení s následným možným záznamem v registru dlužníků. V dopise je také psáno, že v den úhrady je nutné kontaktovat společnost „X“ ohledně výše dlužné částky, která stále narůstá. Dlužnou částku je možné zjistit i na jeho profilu v klientské zóně. V případě jakýchkoliv dotazů má společnost „X“ kontaktovat na telefonním čísle +420 886 659 636 nebo na emailu pohledavky@spolecnostx.cz, a to v době od 9 do 18 hodin. Úhradou bude záležitost ze strany společnosti „Y“ uzavřena.

10.2 Prvotní úkony

Dne 2. 1. 2020 v 15:30 hodin se pan Jan Novák pracující v hlavním městě Praha, dostaví na nejbližší policejní oddělení v blízkosti jeho zaměstnání. Tímto oddělením je Místní oddělení Lebeda. Dotazujícímu se policistovi oznamuje, že přišel na Místní oddělení Lebeda oznámit protiprávní jednání. Policista tedy pana Nováka pustí dovnitř budovy Policie ČR. Po vstoupení do budovy Policie ČR je pracovníkem dozorčí služby, vyzván k prokázání totožnosti a dotázán, jak mu může policista pomoci.

Pracovníkem dozorčí služby je policista, který odpovídá za zkompletované přijetí oznámení z hlediska policejních úkolů označovaných jako prvotní úkony. Většinou se jedná o zkušené policisty, kteří již za svou služební kariéru přijali od občanů stovky oznámení. Jsou tedy schopni rozumně a efektivně přijmout oznámení a provést prvotní a neopakovatelné úkony.

Dozorčí služba tedy odpovídá za celkovou prvotní kompletaci daného spisového materiálu. Odpovídá i za dílčí policejní dokumentaci hlídkových policistů, kteří jsou v danou chvíli jeho podřízení.

Jan Novák policistovi majícímu směnu v pozici dozorčí služby, popíše, jaký dopis mu přišel na adresu jeho trvalého pobytu. Policistovi také uvede, že nikdy nic se společností „Y" neuzavíral, tudíž s daným dopisem nemá nic společného. Adresu trvalého pobytu má již jinde, a to na adrese Jasmínová 623, 869 64 Velká Ves. Dopis pan Novák přinesl sebou a předává jej policistovi. Dále pan Novák uvádí, že nejprve volal na telefonní číslo společnosti „X", kde pracovníkovi infolinky rovněž popsal celou situaci. Pracovník infolinky mu na to odpověděl, aby věc oznámil na policii ČR a kopii podaného oznámení následně zaslal na email uvedený v dopise. Poté bude věc ze strany společnosti „X" dočasně zastavena než dojde k prověření daného oznámení ze strany policejního orgánu. Policista tedy začne dokumentovat samotné oznámení v policejním systému.

Po základní editaci v policejním systému se policista přesune k sepisování samotného oznámení. Před sepsáním samotného oznámení policista musí osobu poučit na základě příslušných poučení. Jedná se poučení o poskytování informací, poučení oběti trestného činu a poučení poškozeného v trestním řízení. V poučeních se nachází práva a povinnosti spojené s daným podáním vysvětlení a případné následky za porušení. Veškerá poučení policista vytiskne a vyzve oznamovatele a zároveň poškozeného k podpisu jednotlivých poučení. Tímto potvrdí své seznámení s danými poučeními a rovněž s postihy za jejich porušení.

Teprve poté je policistou sepisován úřední záznam o podaném vysvětlení podle § 158 odst. 6 zákona číslo 141/1961 Sb. trestního řádu. Úřední záznam o podaném vysvětlení podle trestního řádu je sepisován pouze u trestných činů. V případě přestupků je sepisován úřední záznam o podaném vysvětlení podle § 61 odst. 1 zákona č. 273/2009 Sb. o Policii ČR. Zde je vybrána osoba podávající vysvětlení a uvádí se zde i kontaktní údaje k dané osobě. Uvádí se zde telefonní kontakt, zaměstnání. Jméno, příjmení, datum narození, trvalý i přechodný pobyt se propíší z editace, kterou policista dříve provedl. Zde je poškozený dále poučen o svých právech a povinnostech týkajících se trestního řádu. Následuje sepsání celého oznámení od pana Jana Nováka ze strany vyslýchajícího policisty. Výslech je veden policistou, aby dané oznámení obsahovalo veškeré podstatné skutečnosti, ze kterých bude šetřící policista vycházet. Během sepisování podaného vysvětlení je pan Jan Novák ze strany policisty dotázán, zda v poslední době neztratil nebo mu nebyl odcizen jeho průkaz totožnosti. Jan Novák skutečně potvrzuje, že mu byla v průběhu prosince odcizena peněženka, ve které měl

i svůj občanský průkaz. Jelikož k odcizení došlo v pátek 11. 12. 2019 ve večerních hodinách, tak se pan Jan Novák rozhodl věc oznámit na Policii ČR až v pondělí 13. 12. 2019 po jeho pracovní době. Po sepsání úředního záznamu o podaném vysvětlení, policista úřední záznam vytiskne, sám podepíše a nechá jej rovněž podepsat oznamujícím panem Novákem. Dopis, který pan Novák policistovi při prvotním kontaktu předal, policista naskenuje. Naskenovaný dopis přiloží elektronicky ke spisovému materiálu a papírový dopis ke spisovému materiálu v papírové podobě.

Následně policista s panem Janem Novákem prvotní část oznámení ukončí a sdělí mu, že daným skutkem se bude zabývat některý z policistů z Místního oddělení Lebeda, s osmihodinovou pracovní dobou od pondělí do pátku. Pan Novák se policisty zeptá, zda se může případně přijít podívat na stav řízení u daného oznámení. Policista panu Novákovi odpoví, aby klidně třeba za měsíc telefonicky zavolal na zdejší oddělení a při telefonátu uvedl příslušné číslo jednací. Na základě konkrétního čísla jednacího, pracovník dozorčí služby zjistí, komu byl spisový materiál přidělen. Telefonát bude přepojen na příslušného zpracovatele, se kterým se pan Novák může dohodnout na termínu nahlédnutí do spisu. Pan Novák se ještě dotáže, kdy bude vědět, jak byla věc ukončena. Na to je dozorčí službou odpovězeno, že policejní orgán má na prošetření daného oznámení zákonnou lhůtu dva měsíce. Policejní orgán případně může státnímu zastupitelství zaslat žádost o prodloužení lhůty prověřování. Dozorující státní zástupce rozhodne, zda lhůtu prověřování policejnímu orgánu prodlouží či nikoliv. Státní zástupce při prodloužení lhůty uvede, do kdy je lhůta prověřování prodloužena. Po dané informaci již pan Novák opouští policejní stanici.

Dozorčí služba ještě sepíše záznam o zahájení úkonů trestního řízení podle § 158 odst. 3 trestního řádu. Záznam o zahájení úkonů trestního řízení musí obsahovat datum zahájení úkonů, na základě čeho byly úkony zahájeny, název evidovaného skutku, časové rozmezí skutku, pachatele skutku (pokud je znám), paragrafové znění protiprávního jednání, popis samotného skutku, výši škody a poškozeného v daném spisovém materiálu. V našem případě byly zahájeny úkony trestního řízení dne 1. 1. 2020 na základě oznámení pana Jana Nováka ve věci NP PODVOD SPOLEČNOST „Y“, neboť na podkladě zjištěných skutečností je dostatečně odůvodněn závěr, že v blíže nezjištěné době od 11. 12. 2019 do 1. 1. 2020, doposud neznámý pachatel se prostřednictvím internetu dopustil přečinu Podvod podle § 209 odst. 1 trestního zákoníku, a to tím, že uzavřel smlouvu o úvěru se společností „Y“ na jméno Jan Novák, které mu byly vyplaceny a do současné doby neuhradil žádnou splátku, čímž k dneš-

nímu dni způsobil škodu ve výši 11.899,-Kč ku škodě společnosti „Y“. Protože zjištěné skutečnosti nasvědčují tomu, že došlo ke spáchání trestného činu, byly k objasnění a prověření všech okolností zahájeny úkony trestního řízení.

Dne 2. 1. 2020 policista z dozorčí služby svému nadřízenému předává veškerá zpracovaná oznámení z předchozího dne, kdy je mezi nimi i výše uvedené oznámení. Po prostudování spisového materiálu zástupce vedoucího pro trestní řízení, napíše ke spisovému materiálu pokyny pro jeho budoucího zpracovatele a spisový materiál přidělí některému z policistů tzv. zpracovatelů, pracujících v osmihodinové pracovní době. Zástupce vedoucího pro trestní řízení předá oznámení v papírové podobě danému zpracovateli, aby mohl začít pracovat na prověřování daného oznámení.

10.3 Zajišťování důkazních materiálů

Zpracovatel přidělení daného oznámení zjistí tedy předáním v papírové podobě, ale i zobrazením v elektronické podobě v policejním systému. Po převzetí spisového materiálu zpracovatelem, si zpracovatel nejprve musí pročíst celý spisový materiál, aby zjistil: kdo, co, kdy, kde, jak, proč a čím se stalo. V našem případě se zpracovatel nejprve dozvídá pouze výši dlužné částky, název poškozené společnosti „Y“. Zpracovatel tedy využije svého zákonného oprávnění podle § 8 odst. 1 trestního řádu, kde je uvedeno: *„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. Státní orgány jsou dále povinny neprodleně oznamovat státnímu zástupci nebo policejním orgánům skutečnosti nasvědčující tomu, že byl spáchán trestný čin“.*

Prostřednictvím datové zprávy zašle společnosti „Y“ žádost o zaslání smlouvy s panem Janem Novákem a veškerých podkladů se smlouvou spojených. Zpracovatel musí vyčkat několik dní než od společnosti „Y“ přijde odpověď. Doposud nejsou známy žádné bližší podrobnosti k dané smlouvě, tudíž zatím nemůže být prováděno další šetření. Po doručení smlouvy a jejích podkladů si musí zpracovatel veškeré písemnosti řádně nastudovat. Zpracovatel zjišťuje, že smlouva o poskytnutí úvěru byla založena dne 20. 12. 2019 v 15:55 hodin přes internet z IP adresy: 90.172.112.168 a požadovaná částka 11.000,-Kč byla zaslána na bankovní účet číslo 76178234492/0222. Ke smlouvě byl přiložen naskenovaný občanský průkaz na jméno Jan Novák, narozen 3. 3. 1980.

Zpracovatel si začne ověřovat podklady a údaje ve smlouvě. Zjistí několik nesrovnalostí. Číslo odcizeného občanského průkazu pana Jana Nováka, odpovídá doloženému občanskému průkazu. Na doloženém občanském průkazu jsou úpravy, a to v koncovce rodného čísla Kromě změny v koncovce rodného čísla, je také uvedena adresa již bývalého bydliště pana Jana Nováka. Rovněž je ve smlouvě uvedena emailová adresa a telefonní číslo, které neodpovídají kontaktním údajům uvedeným panem Novákem v úředním záznamu o podaném vysvětlení podle § 158 odst. 6 trestního řádu sepsaným dne 1. 1. 2020.

V policejních systémech je zpracovatelem provedena kontrola kontaktních údajů, zda se dané údaje nenachází i v jiných spisových materiálech šetřených útvary v rámci Policie ČR. Také je provedeno šetření k vlastníkovi telefonního čísla 796 365 289, uvedeného ve smlouvě. Šetřením se podařilo zjistit, že telefonní číslo patří osobě Karel Novotný, narozen 16. 10. 1978. K emailové adrese jan.novak15@ceskyportal.cz zpracovatel využil oprávnění podle ustanovení § 8 odst. 1 trestního řádu a podařilo se mu zjistit informace týkající se konkrétní emailové adresy.

Zpracovatel využil své oprávnění podle § 88a odst. 1 trestního řádu, uplatnitelné mimo jiné pro trestný čin Podvod podle § 209 trestního zákoníku. Policista tedy sepíše žádost o vydání příkazu ke zjištění a postoupení záznamu uskutečněného telekomunikačního provozu podle § 88a odst. 1 trestního řádu k uživateli telekomunikačního provozu. Zpracovatel musí udělat i kopii celého spisového materiálu. Kopii spisového materiálu včetně jednoho originálu žádosti podle § 88a odst. 1 trestního řádu, zašle na příslušné Obvodní státní zastupitelství na Prahu 33, aby vytvořilo návrh na vydání příkazu k vyžádání údajů o telekomunikačním provozu podle § 88a odst. 1 trestního řádu a zaslalo ho na příslušný soud, v našem případě Obvodní soud pro Prahu 33. Příslušný soud zašle příslušné společnosti zprostředkovávající internetové služby, žádost k uživateli IP adresy, ve které rovněž uvede IP adresu, datum a čas k potřebnému zjištění. Z odpovědi společnosti poskytující internetové služby se podařilo zjistit, že adresa registrace je Pitkovická 56, 612 278 Větrolupy a uživatelem dané IP adresy je Karel Novotný, narozen 16. 10. 1978.

Policista uplatní i ustanovení § 8 odst. 2 trestního řádu k získání informací podléhající bankovnímu tajemství. Ustanovení § 8 odst. 2 trestního řádu, je využito k zjištění majitele bankovního účtu ze smlouvy, na který byla zaslána částka 11.000,-Kč. Policejní orgán udělá znovu kopii spisového materiálu a zašle návrh dozorujícímu státnímu zástupci Obvodního státního zastupitelství Praha 33, aby podle § 8 odst. 2 trestního řádu vyžádal informace podléhající bankovnímu tajemství u banky Moravská banka, s. r. o.. Dozorující státní zástupce

Obvodního státního zastupitelství Prahy 33 zašle žádost k danému účtu banky Moravská banka, s. r. o., kde mimo jiné uvede, že je třeba vyžádané bankovní informace neprodleně doručit na Místní oddělení Lebeda, k číslu jednacímu daného spisového materiálu a k rukám samotného zpracovatele. O dané skutečnosti dozorující státní zástupce písemně vyrozumí Místní oddělení Lebeda. Zpracovatel musí vyčkat na odpověď z Moravské banky, s. r. o. Po příchozí odpovědi z Moravské banky, s. r. o. na Místní oddělení Lebeda zpracovatel daného spisového materiálu zjišťuje, že majitelem bankovního účtu a jediným disponentem daného bankovního účtu je Karel Novotný, narozen 16. 10. 1978 a další informace týkající se bankovního účtu. Z výpisů z účtu se potvrzuje, že částka 11.000,-Kč od společnosti „Y“ byla skutečně připsána na daný bankovní účet.

10.4 Výslech pachatele

Veškeré vyžádané odpovědi si zpracovatel ve spisovém materiálu uspořádá a sepíše výzvu k podání vysvětlení podle § 158 odst. 7 trestního řádu. Zde uvede jméno, příjmení, datum narození a adresu bydliště předvolávaného. Ve výzvě zpracovatel uvede datum, čas a místo, kde se má předvolaný dostavit k podání vysvětlení. Předvolávaný je poučen o tom, aby se dostavil k podání vysvětlení s dokladem totožnosti. V případě, že by se předvolaný ve stanovenou dobu nemohl dostavit, je potřeba se omluvit. Kdyby se předvolávaný dostatečně neomluvil, mohl by být ze strany policejního orgánu předveden nebo mu může být uložena pořádková pokuta až do výše 50.000,-Kč. Výzva se zašle poštovní obálkou, kde příjemce při doručení vypíše své jméno a příjmení. Uvede datum převzetí a vše potvrdí svým podpisem. Když předvolávaný vlastní datovou schránku, je mu výzva zaslána pomocí datové zprávy, kde si vyžádá zaslání informace o doručení.

Po dostavení se prověřovaného k podání vysvětlení na policejní oddělení, zpracovatel nejprve ověří totožnost předvolaného na základě předložení dokladu totožnosti a ověření totožnosti v informačních systémech policie ČR. Následně policista osobu poučí o svých právech a povinnostech v rámci probíhajícího trestního řízení.

Po výše uvedených poučeních, policista s předvolaným Karlem Novotným sepíše úřední záznam o podaném vysvětlení podle § 158 odst. 6 trestního řádu. Při sepisování úředního záznamu o podaném vysvětlení se policista předvolaného dotazuje na celý průběh daného skutku. Od počátečního obecného dotazování, policista postupně směřuje na detailní stránku konkrétního protiprávního jednání. Novotný se k protiprávnímu jednání doznává v plné

míře, kdy popisuje celý průběh svého jednání. Při podání vysvětlení se prověřovaný sám rozpovídá. Uvádí, že jednoho dne po cestě domů z práce na zemi v některé z ulic města Prahy nalezl občanský průkaz na jméno „Jan Novák“. Poté přemýšlel, co by s nalezeným občanským průkazem provedl. Odevzdání nalezeného občanského průkazu na Policii ČR nebo Městský úřad vůbec nezvažoval. Při přemýšlení jej napadlo, že by si mohl půjčit nějaké peníze na jméno osoby uvedené na nalezeném občanském průkazu. Po příchodu domů si ve svém domě v ulici Velká čp. 4698 v Praze v části Stará Hrana, na své tiskárně naskenoval nalezený občanský průkaz. Spustil si svůj počítač, kde do internetového vyhledávače zadal „rychlá půjčka“. Hned jako první odkaz mu byla nabídnuta společnost „Y“. Otevřel tedy hned první odkaz a v nabídce společnosti „Y“ mimo jiné našel poskytnutí půjčky do výše 20.000,-Kč s nutností splatit půjčenou částku do 30ti dní od uzavření smlouvy. Novotnému se taková nabídka zamlouvala, proto tedy na svém počítači zvolil možnost uzavření takovéto půjčky. V elektronické žádosti o úvěr uvedl veškeré údaje k osobě Jana Nováka narozeného 3. 3. 1980 s adresou trvalého bydliště Krátká 111, 220 11 Malá Ves z nalezeného občanského průkazu. Dále v žádosti uvedl telefonního číslo 796 365 289 a emailovou adresu jan.novak15@ceskyportal.cz. Emailová adresa byla povinná pro nutnost následného potvrzení úvěru přes odkaz zaslaný na emailovou adresu uvedenou v žádosti o půjčku. Jako požadovanou částku zadal 11.000,-Kč s vyplacením na bankovní účet č. 76178234492/0222 u banky Moravská banka, s. r. o.. Do příloh žádosti přiložil naskenovaný občanský průkaz pana Jana Nového a žádost o půjčku elektronicky odeslal. Přibližně za hodinu mu mělo na emailovou adresu jan.novak15@ceskyportal.cz přijít předběžné schválení půjčky od společnosti „Y“. V emailu bylo také napsáno, že v případě nežádání majitele emailu o půjčku, je potřeba neprodleně kontaktovat Moravskou banku, s. r. o. na telefonním čísle uvedeném v email. Pokud se jedná o žadatele o půjčku, tak má otevřít odkaz uvedený v emailu a po otevření odkazu zvolit možnost uzavření půjčky. Po zvolení půjčky je prováděn další proces prověření osoby uzavírající úvěr. Žadateli je na telefonní číslo uvedené v žádosti o úvěr zaslán kód, který je nutné vložit do otevřeného odkazu z emailu. Novotný tedy doručený kód vložil do kolonky na dané internetové stránce a stiskl tlačítko potvrdit uzavření půjčky. Tímto byla půjčka uzavřena. Přibližně za 5 hodiny mu na bankovní účet č. 76178234492/0222 byla převedena částka 11.000,-Kč od banky Moravská banka, s. r. o.. Po připsání částky na účet odešel z domu k nejbližší popelnici nacházející se u jeho domu a občanský průkaz pana Jana Nováka zde vyhodil. Dále již nic neřešil a částku neuhradil. S bankou Moravská banka, s. r. o. již z jeho strany nekomunikoval. Na závěr uvedl, že svého jednání lituje.

Vzhledem k tomu, že se policejnímu orgánu podařilo provést veškeré výše popsané úkony do tří týdnů od oznámení, policista ještě téhož dne pana Janu Novákovi předá záznam o sdělení podezření na základě ustanovení § 179b odst. 3 trestního řádu. Záznam o sdělení podezření bude obsahovat podrobný popis skutku, s uvedením: kdy a kde k danému protiprávnímu jednání došlo, jakým způsobem spáchal protiprávní jednání a jakého trestného činu se dopustil. Jednu verzi záznamu o sdělení podezření, vyslýchající policista předá panu Novotnému. Po sdělení podezření policista osobu znovu vyslechne, a to na protokol o výslechu podezřelého podle ve smyslu § 179b odstavce 3 trestního řádu. Při sepisováním protokolu o výslechu podezřelého, policejní orgán znovu osobu poučí příslušnými poučeními.

Oproti podání vysvětlení podle § 158 odst. 6 trestního řádu, policejní orgán od již podezřelého také zjišťuje informace ohledně členů rodiny, jeho vzdělání, o majetkových poměrech, a zda již byl někdy vyslýchán pro nějaký trestný čin, případně kolikrát a pro jaké trestné činy. Je třeba osobu poučit o následcích Křivého obvinění podle ustanovení § 345 zákona č. 40/2009 Sb. trestního zákoníku. Podezřelý je dotázán, jestli si volí obhájce či nikoliv. Podle ustanovení § 33 odst. 1 trestního řádu je podezřelý poučen o možnosti nevypovídat a následně dotázán zda bude vypovídat. V tomto případě si pan Novotný obhájce nezvolil a rozhodl se vypovídat. Při sepisování protokolu o výslechu osoby podezřelé se policista znovu pana Novotného dotáže na celý průběh spáchání trestného činu. Není možné pouze uvést, že se osoba odkazuje na podání vysvětlení podle § 158 odst. 6 trestního řádu. Podání vysvětlení podle § 158 odst. 6 trestního řádu nemá u soudu právní váhu. Podstatné je, co je uvedené v protokolu o výslechu podezřelého.

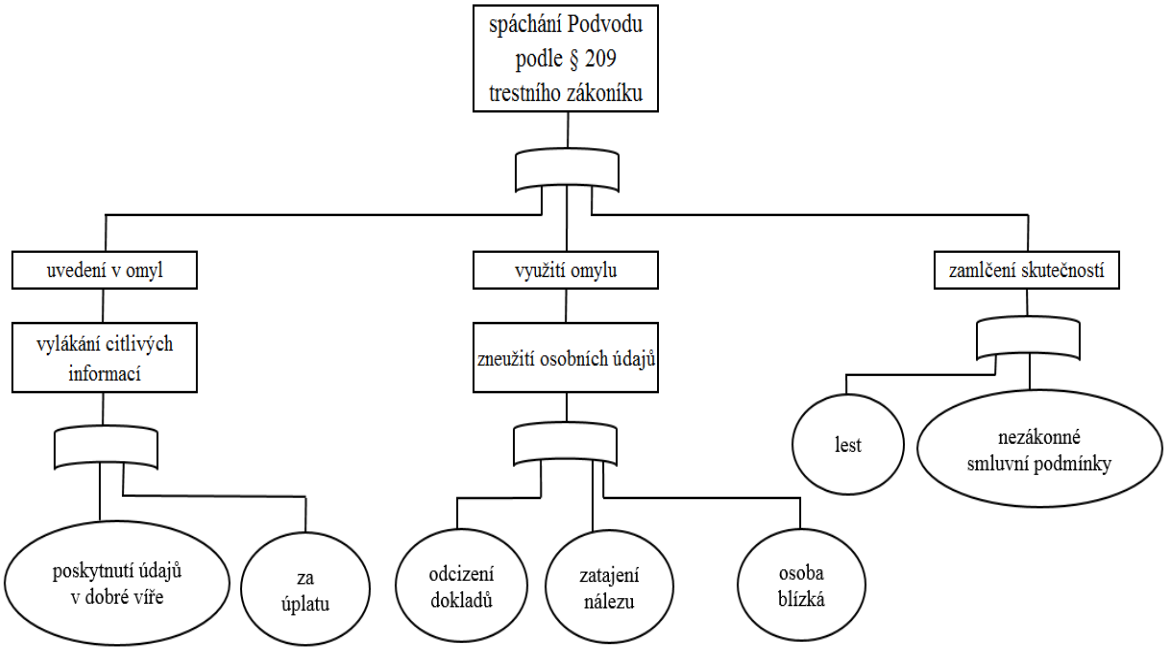
10.5 Závěrečné úkony

Po ukončení výslechu si policista ještě zajistí podklady o chování a způsobu života osoby podezřelé. Následně policista setřídí celý spisový materiál. Vytvoří dvě kopie uspořádaného originálu spisového materiálu. Originál a jedna kopie spisového materiálu je zaslána dozorovému státnímu zástupci na příslušné státní zastupitelství. Originál spisového materiálu dále putuje k soudu a zaslaná kopie spisu zůstává u státního zástupce jako dozorový spis. Druhá kopie spisovému materiálu se ukládá na útvaru Policie ČR, který skutek řešil. Tímto končí úkony policejního orgánu v dané věci. Panu Novotnému za jeho protiprávní jednání hrozí trest odnětí svobody až na dva roky.

Pro podvodné jednání přes počítač byl zvolen vytvořený případ kvalifikovaný jako Podvod podle § 209 trestního zákoníku. Byl zde popsán celý postup policejního orgánu od přijetí oznámení až po předání kompletního spisového materiálu dozorujícímu státnímu zástupci. Jedná se o skutek, který se policejnímu orgánu podařilo objasnit a ztotožnit tedy osobu pachatele trestného činu.

11 ANALÝZA RIZIK U PODVODNÉHO JEDNÁNÍ

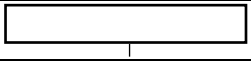
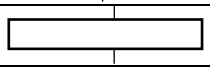
V návaznosti na případovou studii bude provedena analýza rizik spojených s podvodným jednáním podle ustanovení § 209 trestního zákoníku. K zobrazení rizik byla zvolena metoda FTA. Metoda FTA spočívá ve vytyčení hlavního problému, jehož dílčí příčiny jsou následně ve stromové struktuře rozvětvovány. Metoda FTA využívá hradel pro další členění jednotlivých oblastí. Ve spodní části stromové struktury jsou uvedeny prvotní příčiny celého jednání (Obr. 1: Podvod ve stromové struktuře).



Obr. 1: Podvod ve stromové struktuře [vlastní zpracování]

Legenda k podvodnému jednání bude znázorněna v tabulce (Tab. 1: Legenda k metodě FTA).

Tab. 1: Legenda k metodě FTA [vlastní zpracování]

Symbol	Popis symbolu
	vrcholová událost skrývající hlavní problém
	událost vedoucí k vrcholové události
	hradlo znázorňující možnost nebo
	základní událost bez dalšího rozvoje

11.1 Uvedení v omyl

Skutková podstata Podvodu podle § 209 trestního zákoníku může být naplněna několika způsoby. Prvním z nich je uvedení někoho v omyl. V omyl lze někoho uvést vylákáním citlivých informací. Za citlivé informace jsou považovány osobní údaje k osobě či osobám nebo interní informace určité společnosti. Hlavním problémem bývá vylákání citlivých informací, kdy budoucí oběť své osobní údaje poskytne někomu jiné v dobré víře, že je druhá strana skutečně potřebuje a vhodně využije. V dobré víře je myšleno dobrovolně bez nátlaku jiné osoby s předpokladem, že nedojde ke zneužití. Příkladem je uvedení svých osobních údajů neověřenému žadateli a bez zjištění důvodu sdělení těchto informací. Za základní protiopatření lze považovat nezadávání a nevyplňování svých osobních údajů v prostředí internetu a samozřejmě je nikomu jen tak nesdělovat ani mimo síť internet. To platí i v případě požádání o sdělení citlivých informací svému kamarádovi či známému. V budoucnu takový člověk může naše osobní údaje kdykoliv zneužít. Člověk také může někomu sdělit své osobní údaje například v různém dotazníku na ulici a neuvědomuje si, že jeho údaje mohou býti zneužity. Proto je třeba se vždy a neustále dotazovat, proč někdo potřebuje znát mé osobní údaje. Zejména v případech, kdy jsou údaje vyžadovány zcela neúměrně k dané situaci. Je třeba využít elementárních znalostí a logického, střízlivého uvažování, které nám pomůže odlišit situace, v nichž je třeba údaje sdělovat a při kterých naopak nikoli. Také je vhodné sledovat hromadné sdělovací prostředky, kde jsou někdy uváděna různá podvodná jednání, která se na území ČR odehrála a vzít si z nich poučení.

Získání osobních údajů za úplatu je dalším z rizik. S tímto problémem se často setkávají policisté při vyšetřování podvodných jednání, kdy vše směřuje k osobě žijící na ulici. Lidé na ulici často bojují o své přežití a starost, komu sdělí své osobní údaje je pro ně druhotnou. Pachatelé tak na ulici přijdou za osobou žijící bez domova, kdy jí pod záštitou fiktivního příběhu nabídnou finanční částku. Pachatelé požadují založení bankovního účtu osobou bez domova a následné předání bankovní karty a přihlašovacích údajů. Za to osobě bez domova dají určitou finanční částku a obě strany jsou spokojeny. Osoba bez domova si za peníze může zakoupit jídlo a pití potřebné k přežití a pachatel jednoduše získá osobu tzv. bílého koně. Jedinou šancí jak tomuto častému jevu zabránit je zlepšení úrovně životní úrovně osob bez domova. Zlepšení životní úrovně může spočívat v nabídnutí levnějších pronájmů bytů především ze strany měst a snaha státu o jejich začlenění se získáním zaměstnání byť s nižší úrovní produktivity za nižší finanční výdělky.

11.2 Využití omylu

Druhý způsob spáchání Podvodu je využití omylu. Zde můžeme zařadit odcizení dokladu, zatajení nálezu anebo využití omylu za úplatu. Výsledek všech těchto případů může býti stejný, avšak něčím se liší.

V případě odcizení dokladu a zatajení nálezu se bavíme o podobném problému, avšak u odcizení je větší pravděpodobnost rychlejšího zneužití než u zatajení nálezu. Rozdíl spočívá v tom, že může trvat určitou dobu, než doklad totožnosti někdo nalezne. Doklad může nalézt i slušný člověk. Zatímco u odcizení kabelky nebo peněženky s osobním dokladem je protiprávní jednání úmyslné ze strany pachatele. Tím může mít pachatel více času ke zneužití dokladu totožnosti, než poškozený přijde na odcizení svých věcí. Opatřením před odcizením či ztrátou dokladů je nosit svou peněženku s doklady nejlépe v uzavřené kapse nebo v případě žen například v uzavřené kabelce. U obou případů by člověk měl mít svou peněženku na očích. Je tím myšleno mít doklady pozici před tělem nikoliv za tělem. Tedy v předních kapsách od kalhot nebo kapsách od bundy. Vhodné je mít peněženku doléhající na tělo, aby člověk cítil dotyk dané peněženky na části těla. V kapse od bundy, kde má člověk několik dalších věcí, tak nemusí ani cítit, že by mu peněženka byla odcizena nebo mu vypadla. Zvýšenou pozornost by měl člověk věnovat svým věcem na místech s větší fluktuací osob, jakými jsou například prostředky městské hromadné dopravy nebo náměstí ve větších městech. V případě odcizení osobního dokladu je nutné danou skutečnost co nejdříve oznámit na Policii ČR pro případ jeho dalšího zneužití. Při ztrátě dokladu totožnosti, je vhodné věc oznámit na příslušný úřad. V sobotu a neděli, kdy jsou úřady zavřeny, bych doporučil i ztrátu oznámit na Policii ČR. Policie ČR osobě při ztrátě ani dočasný doklad osobě nevydá, avšak o daném oznámení bude zmínka v policejních systémech pro případné zneužití daného dokladu.

Zneužít osobní údaje může také osoba nám blízká, i když je to smutné. Pravděpodobnost takového jednání je nižší než při výše uvedených případech, ale také se stávají. Těmto případům se těžko předchází, zejména u rodin, kde není zjištěný žádný závadový člen. Za závadového člena lze označit osobu s problémovým, trvale nezřízeným či nezákonným stylem života. Jediné opatření spočívá v možnosti mít své doklady stále na dohled, případně je nosit při sobě.

11.3 Zamlčení skutečností

V případě zamlčení skutečností se budeme bavit o lsti a nezákonných smluvních podmínkách. Lstí mohou být zasílány podvodné emaily s cílem útočníků získání finančních prostředků od své oběti. V těchto případech bych doporučil vůbec neotevírat emaily z neznámých emailových adres. Ve chvíli již otevřeného emailu od neznámé osoby, na tento email nereagovat a rozhodně nezasílat peníze, které mohou být požadovány. Není nic jednoduššího než si telefonicky nebo pomocí emailu ověřit pravdivost požadavku od společnosti, za kterou se může někdo jen vydávat.

Za další problém považuji nezákonné smluvní podmínky. Jedná se o smlouvy, které směřují proti základním právům zákazníka nebo obsahují dodatky, které mohou zákazníkovi způsobit problémy. Každý prodávající bude svůj produkt vychvalovat. Jako opatření bych doporučil si každou smlouvu důkladně pročíst a nepodepisovat ji jen na základě ústně sdělených výhod ze strany nabízejícího. Jako nejvhodnější variantu vidím v možnosti nechat si smlouvu zkontrolovat od nezávislé osoby s právním vzděláním. Právně vzdělaná osoba nás tak může upozornit na nevýhodné smluvní podmínky a doporučit nám neuzavření takovéto smlouvy.

V tabulce (Tab. 2: Návrhy na opatření v bodech) budou uvedeny návrhy na opatření zjednodušeně v bodech.

Tab. 2: Návrhy na opatření v bodech [vlastní zpracování]

Poskytnutí údajů v dobré víře	**Poskytnutí údajů za úplatu**
• Nezadávat a nevyplňovat své osobní údaje • Nikomu nesdělovat osobní údaje • Dotazovat se na důvod požadavku • Logické zvážení potřeby údajů druhou stranou • Poučit se z případů z hromadných sdělovacích prostředků	• Zlepšení životní úrovně lidí bez domova: - nabídnutím levnějších pronájmů bytu ze strany měst - pomoc se získáním zaměstnání ze strany měst
Odcizení dokladů a zatajení nálezu	**Osoba blízká**

• Nošení peněženky v uzavřené kapse nebo kabelce • Mít svou peněženku v kapsách před tělem • Mít peněženku doléhající na tělo bez dalších věcí • Zvýšená pozornost v místech s větší fluktuací osob	• Mít své doklady stále na dohled • Nosit doklady při sobě
Lest	**Nezákonné smluvní podmínky**
• Neotevírat zprávy od neznámého adresáta • Nereagovat na zprávy a nezasílat finanční prostředky • Telefonicky nebo pomocí emailu si ověřit pravdivost požadavku	• Důkladně si přečíst smlouvu • Nepodepisovat smlouvu jen na základě ústních sdělení • Nechat si smlouvu zkontrolovat od právně vzdělané osoby

Jedenáctá kapitola navazuje na případovou studii a rozvíjí oblast podvodného jednání. Obsahem jsou rovněž doporučení pro jednotlivá rizika.

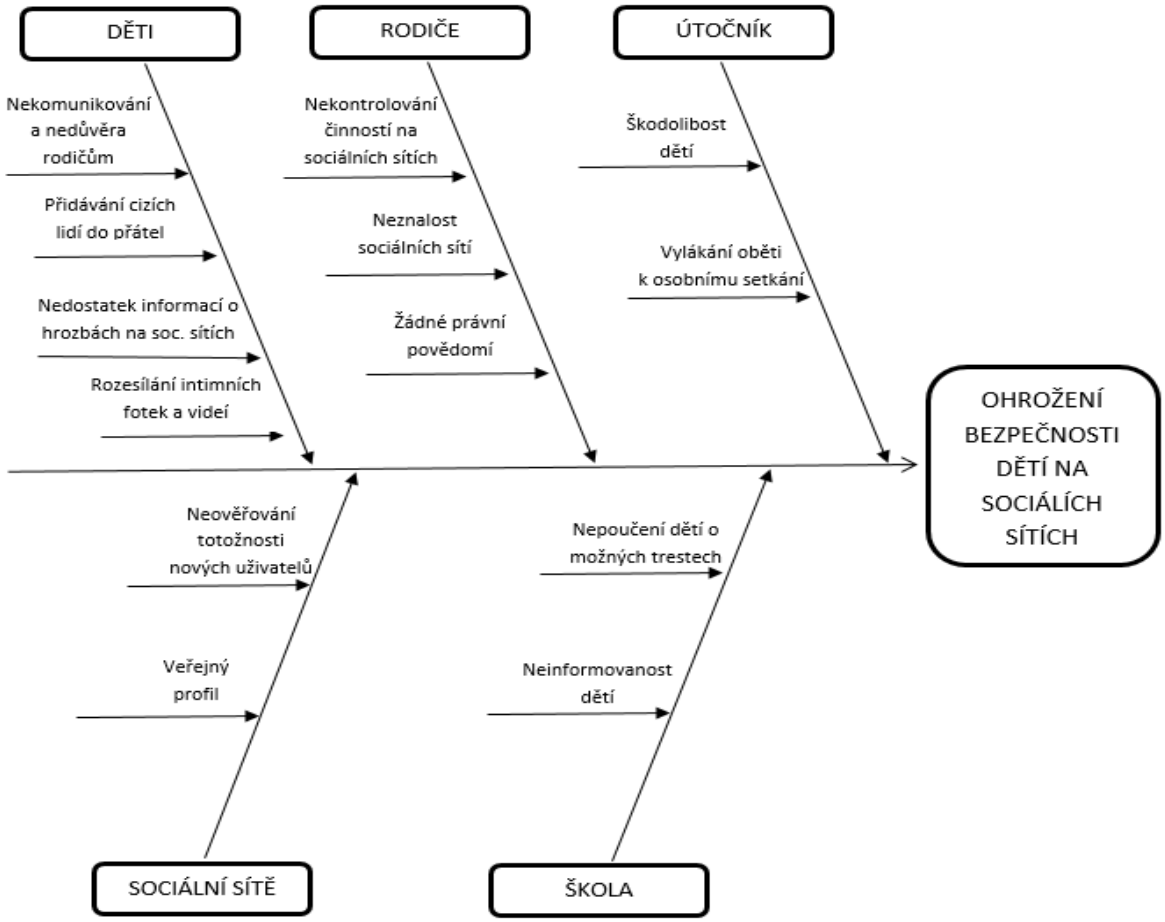
12 ANALÝZA RIZIK BEZPEČNOSTI DĚTÍ NA SOCIÁLNÍCH SÍTÍCH

Pro analýzu rizik byla také zvolena oblast bezpečnosti dětí na sociálních sítích. Důvodem výběru odlišné oblasti než je oblast v případě případové studie, bylo ukázat čtenáři více oblastí protiprávního jednání, ke kterým dochází mimo jiné i v kyberprostoru. Analýza rizik se bude skládat z Ishikawa diagramu, pomocí kterého budou stanoveny rizikové faktory v obrazovém znázornění. Ishikawa diagram je diagram příčin a důsledků, který přehledně graficky znázorňuje rizikové faktory ve tvaru rybí kosti.

Dále bude využita metoda PNH, pomocí které budou rizikové faktory ohodnoceny. Rizikové faktory budou vyhodnoceny a na závěr budou k jednotlivým rizikům navržena opatření pro jejich snížení. Metoda PNH je semi-kvantitativní metodou složenou ze tří oblastí. Jedná se o oblast pravděpodobnosti vzniku, závažnosti následků a názoru hodnotitelů, následným součinem přiřazených hodnot dostáváme hodnotu celkového rizika. Bližší informace k metodě PNH budou uvedeny při ohodnocení rizikových faktorů.

12.1 Identifikace rizik pomocí Ishikawa diagram

Bylo vytyčeno 5 rizikových oblastí, které mají určitý vliv na ohrožení bezpečnosti dětí na sociálních sítích. Jedná se o oblast dětí, rodičů, útočníků, sociálních sítí a školy. K jednotlivým rizikovým oblastem budou uvedeny rizikové faktory. Znázornění pomocí Ishikawa diagramu je provedeno na níže uvedeném obrázku (Obr. 2: Znázornění Ishikawa diagramu).



Obr. 2: Znázornění Ishikawa diagramu [vlastní zpracování]

12.2 Ohodnocení rizik metodou PNH

Z Ishikawa diagramu budou nejprve vypsány jednotlivé rizikové faktory do tabulky (Tab. 3: Rizikové faktory), které budou dále ohodnoceny metodou PNH.

Tab. 3: Rizikové faktory [vlastní zpracování]

Pořadí	Název rizikového faktoru
1.	Nekomunikování a nedůvěra rodičům
2.	Přidávání cizích lidí do přátel
3.	Nedostatek informací dítěti o hrozbách na sociálních sítích
4.	Rozesílání intimních fotek a videí
5.	Nekontrolování činností dětí na sociálních sítích
6.	Neznalost sociálních sítí ze strany rodičů
7.	Žádné právní povědomí ze strany rodičů
8.	Škodolibost dětí
9.	Vylákání oběti k osobnímu setkání
10.	Neověření totožnosti nových uživatelů
11.	Veřejný profil
12.	Nepoučení dětí o možných trestech ze strany školy
13.	Neinformovanost dětí ze strany školy

Ohodnocení rizik vychází z pravděpodobnosti vzniku, závažnosti následků a názoru hodnotitelů. Pravděpodobnost vzniku, závažnost následků a názor hodnotitelů u rizikových faktorů budou ohodnoceny v rozmezí hodnot od 1 do 5. Ve všech případech hodnota 1 znamená nejnižší hodnotu a hodnota 5 tvoří hodnotu nejvyšší. V tabulkách 4, 5 a 6 budou uvedeny podklady pro hodnocení (Tab. 4: Pravděpodobnost vzniku, Tab. 5: Závažnost následků a Tab. 6: Názor hodnotitelů).

Tab. 4: Pravděpodobnost vzniku [vlastní zpracování]

Hodnoty	Pravděpodobnost vzniku – P
1	Nahodilost
2	Nepravděpodobnost
3	Malá míra pravděpodobnosti
4	Větší míra pravděpodobnosti
5	Trvalé riziko

Tab. 5: Závažnost následků [vlastní zpracování]

Hodnoty	Závažnost následků – N
1	Změny v chování dítěte
2	Snížená sebedůvěra dítěte
3	Dočasná psychická újma vyžadující psychologickou pomoc
4	Psychická újma s trvalými následky
5	Smrtelný následek

Tab. 6: Názor hodnotitelů [vlastní zpracování]

Hodnoty	Názor hodnotitelů – H
1	Zanedbatelný vliv na bezpečnost dětí
2	Malý vliv na bezpečnost dětí
3	Nezanedbatelný vliv na bezpečnost dětí
4	Významný vliv na bezpečnost dětí
5	Velmi významný vliv na bezpečnost dětí

Hodnoty z tabulek výše uvedených tabulek budou přiřazeny k jednotlivým rizikovým faktorům. Následným vynásobením hodnot P, N a H vznikne hodnota R neboli hodnota celkového rizika. Celková hodnota rizikového faktoru bude zařazena do příslušného stupně rizikovosti podle tabulky (Tab. 7: Hodnotící tabulka).

Tab. 7: Hodnotící tabulka [vlastní zpracování]

Stupeň	Hodnota rizika	Slovní vyjádření rizika
1.	101 a víc	Nepřijatelné
2.	51 - 100	Nežádoucí
3.	11 - 50	Mírné riziko
4.	4 - 10	Přijatelné
5.	0-3	Bezvýznamné

Nyní bude provedeno ohodnocení rizik, které bude znázorněno v tabulce (Tab. 8: Ohodnocení rizik), a to včetně příslušných hodnot se stanovením celkové hodnoty rizika. Celková hodnota rizika bude pod písmenem R.

Tab. 8: Ohodnocení rizik [vlastní zpracování]

Rizikový faktor	P	N	H	R
Nekomunikování a nedůvěra rodičům	4	2	4	32
Přidávání cizích lidí do přátel	3	4	4	48
Nedostatek informací dítěti o hrozbách na sociálních sítích	4	4	5	80
Rozesílání intimních fotek a videí	3	4	5	60
Nekontrolování činností dětí na sociálních sítích	4	2	4	32
Neznalost sociálních sítí ze strany rodičů	2	2	4	16
Žádné právní povědomí ze strany rodičů	2	3	4	24
Škodolibost dětí	3	2	3	18
Vylákání oběti k osobnímu setkání	3	5	5	75
Neověření totožnosti nových uživatelů	4	3	4	48
Veřejný profil	4	3	4	48
Nepoučení dětí o možných trestech ze strany školy	3	1	3	9
Neinformovanost dětí ze strany školy	4	4	5	80

Z výsledných hodnot jednotlivých rizikových faktorů je viditelné, že do prvního a pátého stupně rizik nespadá žádný z uvedených rizikových faktorů. Do přijatelných rizik patří riziko spočívající v nepoučení dětí o možných trestech ze strany školy. Za mírná rizika jsou považována: neznalost sociálních sítí ze strany rodičů, škodolibost dětí, žádné právní povědomí ze strany rodičů, nekontrolování činností dětí na sociálních sítích, nekomunikování a nedůvěra rodičům, přidávání cizích lidí do přátel, neověření totožnosti nových uživatelů a veřejný profil. Nežádoucími riziky jsou: rozesílání intimních fotek a videí, vylákání oběti k osobnímu setkání, nedostatek informací dítěti o hrozbách na sociálních sítích a neinformovanost dětí ze strany školy.

Dvanáctou kapitolu tvoří Ishikawa diagram identifikující rizika spojená s ohrožením bezpečnosti dětí na sociálních sítích a o ohodnocení rizik pomocí metody PNH.

13 NÁVRHY OPATŘENÍ PRO JEDNOTLIVÁ RIZIKA

Každá analýza rizik musí obsahovat návrhy opatření ke snížení rizik na přijatelnou úroveň. K jednotlivým rizikovým faktorům budou uvedeny doporučení k předcházení a snížení rizik.

13.1 Rizika z oblasti dětí

Nekomunikování dítěte s rodiči je problémem, který může být způsoben například nezájmem rodičů o samotné dítě. Čím delší dobu se rodiče o své dítě nezajímají, tím se dítě více uzavírá a nemá potřebu s rodiči nic probírat. Rodiče tedy nemusí ani poznat, že jejich dítě může být v nesnázích. Takový problém může skočit tím, že dítě bude obětí nějakého protiprávního jednání a rodiče to ani nezjistí. Nekomunikování s trápícím se dítětem může přinejhorším vést až sebevraždě dítěte. Rodiče by se tedy měli zajímat o své děti a bavit se s nimi. V případě podezření na nějaký problém se snažit dítěte citlivě dotázat, zde se mu něco stalo a zjistit tak co nejvíce informací k danému problému, aby mohl být vhodnou formou řešen. Důvěra dětí rodičům je základem úspěšného rodinného soužití. Důvěra se těžko získává, ale velice snadno ztrácí. Důvěra může být zásadní v oblasti ohrožení bezpečnosti dětí na sociálních sítích. Vycházení rodičů s dětmi může zabránit nepříjemnostem pro jejich děti ve světě internetu. Dítě důvěřující svému rodiči může mámě nebo tátovi dobrovolně nebo prořeknutím sdělit, kdo mu dopisuje na sociálních sítí, a že od něj například požadoval svléknutí se během video rozhovoru na Facebooku. Rodiče mohou pomoci dalšímu jednání pachatele zabránit již v prvopočátku. Kdyby jim dítě nedůvěřovalo, tak se danou informaci nemusí nikdy dozvědět a jejich dítě se stane obětí trestného činu. Rodiče by se měli zaměřit na dobrý vztah se svými dětmi, ale to platí pro více oblastí nejen pro oblast využívání sociálních sítí.

Děti si často na sociálních sítích přidávají do přátel cizí lidi, aniž by je znaly. Důvodem někdy bývá jen soupeření se svými kamarády, kdo má více „přátel“. Některé děti si neuvědomují, že v prostředí sociálních sítí se nachází i lidé, kteří mohou jiným škodit. Důvody tak nemusí mít příliš rafinovaný podtext, napomoci může i prostá dětská naivita. Děti by si vždy měly ověřit, zda ví, o koho se jedná, než si jej přidají do přátel. Ověření druhé strany je možné provést například dotazem, odkud se znají. Dotaz by měl dále směřovat k ověření situace, kde se měly s osobou setkat a toto si dále ověřovat. Další možným ověřením osoby je podívání se, zda má osoba nějaké společné přátele. V případě, že ano, tak napsat danému kamarádovi nebo kamarádce, zda danou osobu znají. Když jim kamarád odpoví, že osobu

nikdy neviděl a neví, o koho jde, tak by si osobu rozhodně nemělo dítě přidávat do svých přátel. Jsou to příklady možností, kterými děti předejdou zbytečným problémům.

Nedostatek informací o hrozbách na sociálních sítích způsobuje, že děti neví, s čím se mohou ve světě internetu setkat. Myslí si, že se jim nic nemůže stát a proto k tomu tak přistupují. Prostor internetu znají jako místo, které slouží jako prostředek k zábavě, kde hrají hry, tráví svůj volný čas a mnohdy si nepřipouštějí, že by se mohlo jednat o nebezpečné prostředí. Je třeba se zaměřit na osvětu dětí ohledně nástrah nejen na sociálních sítích, ale celkově na internetu. Děti se musí o hrozbách na sociálních dozvídat na internetu, ve škole i od rodičů. Snahy některých rodičů chránit děti tím, že se nebudou dozvídat o „ošklivých věcech", které se na internetu dějí, jim tím poskytují spíše medvědí službu. Bez takových informací děti nebudou vědět, jak se mají zachovat a pachatelé jejich nevědomosti často využívají. Je tedy potřeba s dětmi hovořit a informovat je o případném způsobu řešení. Děti by měly být informovány také o institucích jako je Dětské krizové centrum, Linka bezpečí, Pražská linka důvěry, Rodičovská linka, Modrá linka, ebezpečí.cz či Bílý kruh bezpečí. Některé děti se stydí nepříjemnou situaci sdělit rodičům, proto by měly vědět o dalších alternativách pomoci.

Děti by neměly nikomu rozesílat intimní fotografie a videa na sociálních sítí. Děti si musí uvědomit, že jednou zveřejněná osobní fotografie nebo video, mohou být kdykoliv v budoucnu zneužity. V tomto případě se nejedná pouze zaslání dané fotografie nebo videa cizí osobě, ale i kamarádovi nebo svému příteli. Po rozchodu s přítelem nebo pohádání se se svým kamarádem, může takový člověk daný soubor například zveřejnit nebo rozeslat svým známým a to by přece nikdo nechtěl. Nejlepší je tedy takovou fotografii nebo video nikdy nikomu nezasílat. V případě zaslání musí být člověk srozuměn i s možnými následky. V případě pachatelů může být zaslání jedné fotografie nebo videa donucovací prostředek pro vyžádání si zaslání dalšího takového souboru. Dítěti je pak pohrozeno, že v případě nezaslání dalšího souboru, bude takový soubor zveřejněn. Dítě se tak ocitá v začarovaném kruhu. Kdyby se již taková situace skutečně stala a dítě bylo někým vydíráno pohrůžkou sdílením jeho intimního materiálu, mělo by dítě věc nejprve probrat s rodiči a poté oznámit na Policii ČR. S osobou pachatele je potřeba určitým způsobem udržovat kontakt i po odhalení nezákonného jednání, aby policejní orgán mohl zajistit co nejvíce důkazních prostředků pro rozhodnutí ve věci. V takovém případě, by neměli rodiče ani děti mazat dříve zaslanou komunikaci, profily ani účty na sociální síti, neboť takové informace pak mohou sloužit jako důkazní materiál.

13.2 Rizika z oblasti rodičů

Nekontrolování činnosti dětí na sociálních sítí je dalším rizikovým faktorem. Rodiče by měli dítěti nastavit určitá pravidla pro používání počítače. Mohou dítěti stanovit určitý počet hodin strávených na internetu. Dále by rodiče měli mít přehled o pohybu jejich dětí na internetu, kde můžeme zahrnout i sociální sítě. Samozřejmě není vhodné děti špehovat, ale někdy se podívat s kým si dítě dopisuje, nemusí být na škodu. Třeba ve chvíli, kdy si dítě odskočí na záchod nebo na jídlo. I tímto způsobem mohou rodiče narazit například na kyberšikanu, o které se dítě samo nezmínilo. Opatřením také může být stanovení dítěti dobu strávenou na počítači pro každý den. Přihlášení dítěte do sportovního nebo jiného kroužku může rovněž pomoci s prevencí předcházení protiprávního jednání na sociálních sítích. Dítě by mělo náplň po školní docházce a nenudilo se doma u počítače. Rodiče by také měli sledovat informace svých dětí zveřejněné na jejich sociálních sítích. Jedná se o osobní údaje, ale také o celkový sdílený materiál a reakce jeho navázaných kontaktů. Tímto rodiče mohou narazit na zbytečné množství zveřejněných osobních údajů, anebo nevhodné reakce jeho přátel na sociálních sítích a daný problém s dítětem konzultovat.

Někteří rodiče nepoužívají sociální sítě a tím pádem neznají, jak fungují ani neví o hrozbách v tomto prostoru. Bez znalosti o používání sociálních sítí, nemohou rodiče děti poučit o nástrahách na sociálních sítích. Většina rodičů v dnešní době již sociální sítě používá, ale samozřejmě najdou se i výjimky. Někteří z rodičů odmítají používání sociálních sítí. To je v pořádku, jelikož každý se má právo rozhodnout, zda bude chtít používat svět online či nikoliv. Nic to nemění na tom, že by rodiče alespoň měli vědět o nástrahách na sociálních sítích, aby o tom mohli hovořit se svými dětmi. Informace o sociálních sítích mohou rodiče získat i třeba jen díky rozhovoru se svými kolegy v práci aniž by sami sociální sítě používali. Vítanou možností je zapojit do procesu vzdělávání rodiče i vlastní dítě, jistě si velmi nerado nechá utéct příležitost, poučovat svého rodiče o věcech, které nezná.

Každý z nás by měl mít určité právní povědomí o tom, co je správné a čím se již někdo dopouští protiprávního jednání. Rodiče, kteří nemají představu o postižitelnosti nesprávných jednání, nebudou věc dále řešit kvůli své neznalosti. Tím je myšleno, že například v případě dopisování dospělé osoby s dítětem, někteří rodiče zakáží dítěti si s danou osobou dopisovat a tím to považují za ukončené. Dítě může být s tímto závěrem spokojené a rodiče třeba si poslechne, ale nezabráníme tím, aby se daná osoba o protiprávní jednání pokoušela u jiných dětí. Ideální způsobem je prozatím vzájemnou komunikaci neukončovat a jít věc oznámit na

Policii ČR. Policistům to může pomoci k získání potřebných důkazných materiálů a vedoucí k budoucímu potrestání pachatele na základě rozsudku soudu.

13.3 Rizika z oblasti útočníků

K častým problémům ve světě dětí bývá jejich škodolibost. Jedním z příkladů může být, že chlapec chodí s dívkou a kamarád chlapce mu dívku závidí. Proto si vytvoří například facebookový profil s dívčím jménem, ke kterému přiloží někde na internetu stažené fotografie hezké slečny. Potom během společné komunikace chlapce s „vytvořenou dívkou“ dopisuje, až z něj „kamarád“ získá intimní fotografie nebo videa a potom jej začne vydírat. Tohle je jen jedním z příkladů. Škodolibosti dětí lze předejít správnou výchovou ze strany rodičů a někdy i potřebnou tvrdou rukou ze strany otce či matky. V tomto případě považuji za zásadní výchovu ze strany rodičů již od útlého věku. Při zjištění rodiče útočníka, že jejich dítě se chová nevhodně k jinému dítěti, tak by mu měli důrazně slovně vyčinit s uvedením trestu, který by jej čekal, kdyby se jeho chování opakovalo. Chování vlastního dítěte však nejsme schopni ovlivnit vždy a se stoprocentním výsledkem. Člověk se rodí s určitým geneticky daným balíčkem vlastností, charakterových a povahových rysů, které nelze zcela změnit. Závist, pomstychtivost a další podobné vlastnosti jsou bohužel přirozeným a častým jevem v lidské osobnosti.

Vylákání oběti ze strany útočníka k osobnímu setkání, je již tou nejhorší situací, se kterou se dítě může setkat. Na místě setkání dítě bude dítě jen složitě hledat způsob, jak pachateli uniknout. Většinou se jedná o odlehlá místa nebo místa s menší fluktuací osob. Dítě by se rozhodně nemělo domlouvat s cizí osobou na osobním setkání, zejména pokud osobu doposud osobně nikdy nevidělo. Znovu zde platí ověření si u svých přátel, zda člověka znají. V případě, že osobu nikdo nezná a nemá ji nikdo známý ve svých přátelích, tak by dítě nemělo osobě věřit a nejlépe již v zárodku ukončit konverzaci. Můžeme zde také opět zařadit prevenci ze strany rodičů. Kdyby se dítě rozhodlo s neznámou osobou setkat, tak by se mělo jednat o místo s větší fluktuací osob, aby si případně mohlo přivolat někoho na pomoc. Je vhodné, aby dítě disponovalo mobilním telefonem, znalostí základních telefonických čísel, pro přivolání pomoci. V dnešní době je již možnost využít aplikaci, která umožňuje sledovat pohyb dítěte pomocí GPS souřadnic a mapových souborů. Tato varianta se může zdát jako krajní řešení, které může narušovat soukromí a osobní život dítěte. Bude-li rodiči využívána a nikoliv zneužívána, může být velmi nápomocná. Poslední z variant, kterou vidím jako velmi účelnou, je naučit dítě se bránit. Nemůžeme očekávat, že každé dítě bude mít

zájem navštěvovat zájmový kroužek zabývající se takovou problematikou. Jistým řešením je vložení základů sebeobrany do osnov tělesné výchovy pro základní školy.

13.4 Rizika z oblasti sociálních sítí

Neověření totožnosti nových uživatelů sociálních sítí nahrává osobám pachatelů. Pachatelé si založí tolik profilů, kolik budou chtít. Je to ráj pro pachatele. Zakládání dalších profilů není žádným způsobem limitováno. Totožnost osoby není nijak ověřována. Limitováno by mohlo být například registrování několika osob se stejnou IP adresou během určitého časového rozmezí. Při registraci by sociální síť mohla požadovat rozpoznání obličeje. Požadavkem pro dokončení registrace by mohlo být zaslání fotografie své osoby s papírem, na kterém bude napsaný určitý text. Požadovaný text by byl vygenerovaný systémem dané sociální sítě a osoba by takovou fotografii musela zaslat do 5 minut od vyžádání. V případě nezaslání dané fotografie by byla registrace zamítnuta. Sociální sítě by musely mít osobu, která bude ověřování fotografií s osobami provádět. Jde o náklady navíc, ale mohlo by tím ubýt určité množství falešných profilů.

Možnost mít veřejný profil na sociálních sítí může vést k velkému problému. Problémem mimo jiné je, že někteří lidé se chtějí pochlubit svými fotografiemi, vzděláním a podobně. Na jednu stranu je pro děti potěšující, když jsou pochváleni, že jim to sluší. Netuší však, že na sociálních sítích se pohybují lidé, kteří využívají veřejné profily k vyhlídnutí budoucí oběti. Veřejně dostupné informace na profilech dětí (fotografie, obrázky, informace o koníčcích), mohou napomoci ke zvolení vhodného tématu či námětu k započetí komunikace a rozhovoru útočníka s obětí. Sociální sítě již nabízí možnost soukromého profilu u Instagramu nebo u Facebooku možností omezení přístupu na základě vlastního nastavení. Děti by tedy měly na své profily zveřejňovat co nejméně informací ke své osobě. V případě potřeby zveřejnit nějaké informace o sobě, je třeba si alespoň nastavit viditelnost osobních informací pouze pro lidi, které mají v přátelích. S tím dále souvisí obezřetnost a důslednost při výběru lidí, koho si dítě přidá do přátel a koho nikoliv. Kdyby dítě mělo pouze omezenou viditelnost osobních informací pro lidi mimo přátele, ale přidávaly si každého druhého, kdo jim pošle žádost o přátelství, tak by jakákoliv opatření byla k ničemu.

13.5 Rizika z oblasti školství

Oblast školství je dalším místem, se kterým lze spojovat ohrožení bezpečnosti dětí na sociálních sítí. Děti ve škole stráví přes 20 dní v měsíci. Jde o hodně času z jejich života. Škola

je také určitým druhem výchovy, se kterým se děti setkávají. Škola by se tedy také měla zaměřit na prevenci na internetu a děti o možných hrozbách informovat. Může to být prováděno například nějakými školními projekty nebo vyčleněním jednoho školního dne v roce pro pozvání osoby zabývající se bezpečností na internetu a sdělení dětem podstatných informací o dané problematice. Ve škole by mohla být i tzv. schránka důvěry, kdy by ředitel školy vybral vhodného empatického pedagoga, který by napomáhal dětem v řešení osobních problémů. Mnoho školních zařízení dnes disponuje svým interním psychologem, který do školy buď pravidelně dochází, případně je zde zaměstnán a poskytuje své služby každý den. V takových případech, je dobré děti i rodiče seznámit s možností bezplatného využívání psychologických služeb. Seznamovat děti s psychologem, tak aby k němu měli větší důvěru. Psycholog může být rovněž součástí poskytovaných přednášek a projektů, kdy bude schopen dětem adekvátně k jejich věku, vysvětlit možné následky a pravidla chování.

Škola by se také měla zamyslet nad tresty a nápravnými opatřeními, kterými by byly děti postihovány například u kyberšikany. Následně děti o daných trestech pravidelně informovat, což by mohlo odradit některé z dětí od takovýchto jednání. Příkladem je zhoršená známka z chování nebo podmínečné vyloučení ze školy.

V níže uvedené tabulce (Tab. 9: Návrhy na opatření v bodech) budou v bodech uvedeny jednotlivá opatření a doporučení.

Tab. 9: Návrhy na opatření v bodech [vlastní zpracování]

Nekomunikování a nedůvěra rodičům	**Přidávání cizích lidí do přátel**
• Zajímat se o své dítě a jeho zájmy	• Ověření si druhé strany: - dotazem odkud se znají - dotazem na místo setkání - zda jiný kamarád má osobu v přátelích a zeptat se na ni
Nedostatek informací dítěti o hrozbách na sociálních sítích	**Rozesílání intimních fotek a videí**
• Zvýšená informovanost dětí na internetu, ve škole i od rodičů • Informovat děti o institucích jako: - Dětské krizové centrum	• Nikomu nezasílat žádné intimní fotografie ani videa

- Linka bezpečí - Pražská linka důvěry - Rodičovská linka - Modrá linka - Ebezpečí.cz - Bílý kruh bezpečí	• V případě zaslání a následném vyhrožování neukončovat, nemazat komunikaci a věc oznámit na PČR
Nekontrolování činností dětí na sociálních sítích	**Neznalost sociálních sítí ze strany rodičů**
• Stanovení dítěti množství času stráveného u počítače • Občasná kontrola s kým si dítě dopisuje • Sledování příspěvků dítěte a reakcí jeho okolí • Přihlášení dítěte do nějakého kroužku	• Získání informací o hrozbách od kolegů v práci • Dát možnost dítěti poučit rodiče o fungování sociálních sítí
Žádné právní povědomí ze strany rodičů	**Škodolibost dětí**
• Samo vzdělávání se rodičů	• Řádná výchova dítěte od útlého věku • Úměrné tresty za nevhodné chování dítěte
Vylákání oběti k osobnímu setkání	**Neověření totožnosti nových uživatelů**
• Nedomlouvání se na osobním setkání s neznámou osobou • Nesouhlasit s místem schůzky na odlehlém místě • Mít u sebe mobilní telefon s aplikací ukazující místo výskytu • Znalost dítěte základů sebeobrany	• Limitování opakované registrace ze stejné IP adresy během určitého časového období • Při registraci požadavek rozpoznání obličeje

Veřejný profil	Nepoučení dětí o možných trestech ze strany školy
• Nastavit si soukromý profil • Zveřejňování co nejméně informací o své osobě • Obezřetnost při výběru lidí do přátel	• Hrozba zhoršené známky z chování • Hrozba podmínečným vyloučením ze školy
Neinformovanost dětí ze strany školy	
• Školní projekty zaměřené na sociální sítě • Vyčlenění školního dne na přednášku dětem • Schránka důvěry ve škole • Seznámení s možností bezplatného využívání psychologických služeb	

Třináctá a zároveň poslední kapitola obsahuje návrhy na opatření k jednotlivým rizikům dle dříve definovaných aspektů pomocí Ishikawa diagramu.

Shrnutí praktické části diplomové práce

Praktická část je složena ze tří kapitol. Jedná se o oprávnění Policie ČR při vyšetřování kybernetické kriminality, případovou studii na podvodné jednání přes počítač a analýzu rizik ohrožujících bezpečnost dětí na sociálních sítích.

První z kapitol obsahuje zákonná ustanovení, která policisté využívají pro zajišťování potřebných důkazních materiálů. Policisté musí při dokazování postupovat v souladu se zákony. V jiném případě takový důkazní prostředek není možné použít u soudu.

Následuje kapitola s případovou studií. Případová studie je popsána z pohledu policisty takovou formou, aby si laik i člověk znalý v trestném řízení přišel na své. Na případovou studii navazuje definování rizik u podvodných jednání, pomocí metody FTA. K rizikům jsou uvedena doporučení pro jejich snížení.

Poslední částí práce je zpracovaná analýza rizik ohledně bezpečností dětí na sociálních sítích. Při výběru oblasti pro analýzu rizik byla zohledněna aktuálnost probíraného tématu médii i veřejností. Děti bývají ve světě internetu a sociálních sítích pro pachatele snadnější obětí než dospělí, proto je potřebné se zabývat jejich prevencí. Zpracovanou analýzu rizik tvoří Ishikawa diagram, metoda PNH a návrhy na opatření.

ZÁVĚR

Kybernetická kriminalita je v současnosti nejvíce rostoucí kriminalitou v České republice. Postupně se dostává do většiny oblastí kriminality odpovídající trestnímu zákoníku.

Cílem práce bylo zpracování literární rešerše kybernetické kriminality, následně zpracování případové studie na protiprávní jednání přes počítač a zpracování analýzy rizik u vybraných rizik z vybrané oblasti kybernetické kriminality. Cíl práce byl zcela naplněn.

Literární rešerší ohledně kybernetické kriminality a kybernetické bezpečnosti se zabývala zejména teoretická část diplomové práce. V praktické části jsou vymezena oprávnění policejního orgánu při vyšetřování kybernetické kriminality. Jedná se zejména o paragrafová znění, aby nedošlo k úniku interních informací důležitých pro policejní orgán.

Následně byla zpracována případová studie na podvodné uzavření půjčky na nalezený občanský průkaz. Popis průběhu úkonů ze strany policejního orgánu představuje ukázku výčtu úkonů, které musí policejní orgán provést, aby dospěl k úspěšnému konci. Za úspěšný konec je považováno nejen odhalení pachatele protiprávního jednání, ale především prokázání jeho viny. Pro prokázání viny zajišťuje policejní orgán přímé a nepřímé důkazy. Přímé důkazy jsou důkazy potvrzující nebo vyvracející informace související s prověřovaným oznámením. Za přímý důkaz v našem případě považujeme doznání pachatele. Nepřímé důkazy potvrzují nebo vyvrací skutečnost na základě další skutečnosti. Jeden nepřímý důkaz většinou nestačí. Když je objasňování skutečností založeno pouze na nepřímých důkazech, tak by se mělo jednat o vícero nepřímých důkazu a ty musí vést ke stejné osobě pachatele. V případu popsaném v praktické části lze za nepřímý důkaz považovat zjištěnou IP adresu. Případová studie rovněž může čtenáři posloužit pro uvědomění si, jaké problémy by mohla způsobit ztráta osobního dokladu a proto se jej pečlivě střežit. V případě zjištění ztráty dokladu, dané zjištění nejlépe ihned oznámit příslušnému úřadu. O víkendu, kdy jsou úřady zavřené, je vhodné ztrátu oznámit na Policii ČR.

K případové studii byla stanovena širší oblast rizik spojených s podvodným jednáním. Využita byla metoda FTA, pomocí které byla jednotlivá rizika obrazově znázorněna. Dále byla uvedena doporučení pro snížení pravděpodobnosti vzniku podvodného jednání.

Pro analýzu rizik byla vybrána oblast bezpečnosti dětí na sociálních sítích v návaznosti na aktuálnost tématu uvedeného v teoretické části práce. Nejprve byly pomocí diagramu příčin a důsledků znázorněny rizikové oblasti a konkrétní rizikové faktory. Rizikové faktory

byly ohodnoceny pomocí metody PNH. Výsledné hodnoty rizikových faktorů byly okomentovány a následně uvedeny možná opatření pro jejich snížení.

SEZNAM POUŽITÉ LITERATURY

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

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

[3] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.

[4] HRŮZA, Petr. *Kybernetická bezpečnost*. Brno: Univerzita obrany, 2012. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7231-914-5.

[5] KOLOUCH, Jan a Petr VOLEVECKÝ. *Trestněprávní ochrana před kybernetickou kriminalitou: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Policejní akademie České republiky v Praze, 2013. ISBN 978-80-7251-402-1.

[6] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[7] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0.

[8] Co je IP adresa. *Správa sítě* [online]. Správa sítě, 2016 [cit. 2020-01-27]. Dostupné z: https://www.sprava-site.eu/ip-adresa/

[9] IP adresa. *Síťové prvky, IP adresa* [online]. Síťové prvky, IP adresa, 2019 [cit. 2020-01-27]. Dostupné z: https://informatika-sz.estranky.cz/clanky/ip-adresa.html

[10] ŠULC, Vladimír. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7380-737-5.

[11] AWAN, Imran; BLAKEMORE, Brian (eds.). *Policing cyber hate, cyber threats and cyber terrorism*. 1. vyd. Farnham: Ashgate, 2012. ISBN 978-1-4094-38168-8.

[12] MACEK, Jakub. Kyberprostor. *Revue pro média č. 5: Média a digitalizace* [online]. Brno: Spolek přátel pro vydávání časopisu Host, 2003 [cit. 2020-01-30]. Dostupné z: http://rpm.fss.muni.cz/Revue/Heslar/kyberprostor.htm

[13] Zákon o obětech trestných činů. *Zákony pro lidi* [online]. Zákony pro lidi, 2019 [cit. 2020-01-31]. Dostupné z: https://www.zakonyprolidi.cz/cs/2013-45

[14] Trestní řád. *Zákony pro lidi* [online]. Zákony pro lidi, 2019 [cit. 2020-01-31]. Dostupné z: https://www.zakonyprolidi.cz/cs/1961-141

[15] PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování počítačové kriminality*. Praha: Policejní akademie České republiky, 1998. Právní monografie (Wolters Kluwer ČR). ISBN 80-859-8175-0.

[16] VIKTORYOVÁ, J., Jiří STRAUS, D. BANGO, J. PALAREC, J. BLATNICKÝ, Š. KOČAN a L. VAJZER. *Vyšetrovanie*. 3. vyd. Bratislava: Akadémia policajného zboru v Bratislave - Katedra Vyšetrovania, 2015. ISBN 978-80-8054-643-4.

[17] MUSIL, Jan a Zdeněk KONRÁD. *Kriminalistika: vybrané problémy teorie a metodologie*. Praha: Policejní akademie České republiky, 2001. Právní monografie (Wolters Kluwer ČR). ISBN 80-7251-080-0.

[18] PORADA, Viktor a Roman RAK. *Kriminalita související s informačními a komunikačními technologiemi a identifikace osob na základě projevu lokomoce člověka: (vybrané problémové okruhy výzkumu)*. Praha: Vysoká škola Karlovy Vary, 2007. ISBN 978-80-254-0797-4.

[19] SMEJKAL, Vladimír a Zdeněk KONRÁD. *Internet a §§§*. Praha: Grada, 2001. Právní monografie (Wolters Kluwer ČR). ISBN 80-247-0058-1.

[20] Trestní zákoník. *Zákony pro lidi* [online]. Zákony pro lidi, 2019 [cit. 2020-01-31]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40

[21] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity: vybrané problémy teorie a metodologie*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7

[22] Strategie prevence kriminality v České republice na léta 2016 až 2020 (po aktualizaci v roce 2018). *Prevence kriminality v České republice* [online]. Ministerstvo vnitra ČR, 2018 [cit. 2020-02-05]. Dostupné z: https://prevencekriminality.cz/wp-content/uploads/2019/03/Strategie-prevence-kriminality-v-České-republice-na-léta-2016-až-2020.pdf

[23] Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. *Prevence kriminality v České republice* [online]. Národní bezpečnostní úřad, 2014 [cit. 2020-02-05]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

[24] Audit národní bezpečnosti. *Vláda České republiky* [online]. Ministerstvo vnitra ČR, 2016 [cit. 2020-02-06]. Dostupné z: https://www.vlada.cz/assets/media-centrum/aktualne/Audit-narodni-bezpecnosti-20161201.pdf

[25] NÚKYB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Národní úřad pro kybernetickou a informační bezpečnost, 2019 [cit. 2020-02-06]. Dostupné z: https://www.nukib.cz/cs/o-nukib/

[26] O úřadu. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Národní úřad pro kybernetickou a informační bezpečnost, 2019 [cit. 2020-02-07]. Dostupné z: https://www.nukib.cz/cs/o-nukib/o-uradu/

[27] ŠMAHAJ, Jan. *Kyberšikana jako společenský problém: Cyberbullying as a social problem*. Olomouc: Univerzita Palackého v Olomouci, 2014. ISBN 978-80-244-4227-3.

[28] SZOTKOWSKI, René a Kamil KOPECKÝ. *Kyberšikana a další druhy online agrese zaměřené na učitele: theory, research, applications*. Olomouc: Univerzita Palackého v Olomouci, 2018. ISBN 978-80-244-5334-7.

[29] Jak lidé šmírují své blízké? Stalkerware je využíván stále častěji. *Novinky.cz* [online]. Novinky, 2019 [cit. 2020-02-07]. Dostupné z: https://www.novinky.cz/internet-a-pc/bezpecnost/clanek/jak-lide-smiruji-sve-blizke-stalkerware-je-vyuzivan-stale-casteji-40298950

[30] KOPECKÝ, Kamil. *Kybergrooming - nebezpečí kyberprostoru*. 1. vyd. Olomouc: Net University Ltd, 2010. ISBN 978-80-254-7573-7.

[31] Trestná činnost spojená s internetovou kriminalitou. *Projekt E-bezpečí* [online]. *VLACHOVÁ, Marta*, 2009. [cit. 2020-02-07]. Dostupné z https://www.e-bezpeci.cz/index.php/temata/dali-rizika/148-226

[32] SHINDER, Debra Littlejohn, TITTEL, Ed. *Scene of the cybercrime*. Rockland, MA: Syngress Pub, 2002. ISBN 1-931836-65-5.

[33] PORADA, Viktor a Zdeněk KONRÁD. *Metodika vyšetřování počítačové kriminality: redakční uzávěrka.* Praha: Policejní akademie České republiky, 1998. ISBN 80-859-8175-0.

[34] SMEJKAL, Vladimír, Luděk NOVÁK a Josef POŽÁR. *Kybernetická kriminalita: Cyber security glossary*. 2., aktualiz. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. Pro praxi. ISBN 978-80-7380-501-2.

[35] ŠIŠULÁK, Stanislav, VAJZER, Ladislav. *Vybrané problémy objasňovania trestnej činnosti páchanej prostredníctvom informačno-komunikačných technológií*. 1. vyd. - Bratislava: Akadémia Policajného zboru, 2017. ISBN 978-80-244-4227-3.

[36] PORADA, Viktor a Peter POLÁK. *Kriminalistika: technické, forenzní a kybernetické aspekty*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2016. ISBN 978-80-7380-589-0.

[37] PORADA, Viktor a Peter POLÁK. *Kriminalistika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. ISBN 978-80-7380-558-6.

[38] PORADA, Viktor. *Kriminalistika*. Brno: CERM, 2001. ISBN 80-720-4194-0.

[39] GŘIVNA, Tomáš a Radim POLČÁK, ed. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

[40] STRAUS, Jiří. *Kriminalistická metodika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006. ISBN 80-86898-66-0.

[41] CHMELÍK, Jan. *Místo činu a znalecké dokazování*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-868-9842-3.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CERT Computer Emergency Response Team (Tým pro reakci na nouzové situace počítačů)

CSIRT Computer Security Incident Response (Tým pro reakci na bezpečnostní incidenty počítačů)

ČR Česká republika

FTA Analýza stromu poruch

IP Internetový protokol

IT Informační technologie

NATO Severoatlantická aliance

SWOT Silné stránky, slabé stránky, příležitosti a hrozby

SEZNAM OBRÁZKŮ

SEZNAM TABULEK