POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE
Fakulta bezpečnostně právní
Katedra kriminalistiky

Metodika vyšetřování internetových podvodů – problémy teorie a praxe

Diplomová práce

Internet fraud investigation methodology – problems of theory and practice
Master thesis

VEDOUCÍ PRÁCE
doc. JUDr. Zdeněk KONRÁD, CSc.

AUTOR PRÁCE
Bc. Milan ZÁBOJNÍK

PRAHA
2024

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 5. 3. 2024

Bc. Milan ZÁBOJNÍK

Poděkování

Na tomto místě bych rád poděkoval všem, kteří mi pomohli v realizaci diplomové práce. Zejména děkuji vedoucímu práce doc. JUDr. Zdeňkovi Konrádovi, CSc., za odborné vedení a cenné rady. Rád bych poděkoval také své rodině, která mě při vytváření této práce podporovala.

ANOTACE

Diplomová práce se věnuje internetovým podvodům z kriminalistického hlediska, jejich charakteristice a metodice vyšetřování. Práce je rozdělena do čtyř kapitol. První kapitola je věnována teoretickému vymezení metodik vyšetřování za využití odborné literatury. Druhá kapitola vymezuje základní pojmy. Třetí kapitola popisuje realizovaný výzkum, kterým byla získána data ke kriminalistické charakteristice internetových podvodů, typickým stopám, zvláštnostem předmětu vyšetřování, typickým podnětům a počátečním vyšetřovacím situacím, zvláštnostem počátečních a následných úkonů. Čtvrtá kapitola je věnována metodice vyšetřování internetových podvodů, která byla zpracována na základě teoretických východisek a výsledků provedeného výzkumu.

KLÍČOVÁ SLOVA

internet * internetový podvod * typy podvodů * kyberprostor * kybernetická kriminalita * kriminalistická charakteristika * metodika vyšetřování

ANNOTATION

The diploma thesis is devoted to Internet fraud from a criminalistic point of view, their characteristics and investigation methodology. The work is divided into four chapters. The first chapter is devoted to the theoretical definition of investigation methodologies using professional literature. The second chapter defines basic concepts. The third chapter describes the research carried out, which revealed data on the criminalistic characteristics of Internet fraud, typical traces, special objects of investigation, typical stimuli and initial investigative situations, peculiarities of initial and subsequent actions. The fourth chapter is devoted to the methodology of internet fraud investigation, which was elaborated on the basis of theoretical starting points and the results of the conducted research.

KEYWORDS

internet * internet fraud * types of fraud * cyberspace * cybercrime * criminalistic characteristics * investigation methodology

Obsah

ÚVOD

Kriminalistika je samostatným interdisciplinárním vědním oborem, který členíme na úvodní, obecnou a zvláštní část. Metodiku vyšetřování řadíme do zvláštní části kriminalistické vědy. Jednotlivé metodiky vyšetřování se vytváří pro skupiny trestných činů páchaných obdobným způsobem, zanechávající obdobné stopy a vyšetřované obdobným způsobem. Takovou skupinu tvoří i internetové podvody.

Internetový podvod je ve své podstatě obecný podvod, jehož skutková podstata je vyjádřena v § 209 trestního zákoníku. Podvod je majetkovým trestným činem, jehož objektem ochrany je cizí majetek. Pro účely této práce je internetový podvod chápán jako podvod, který byl spáchán za využití informačních a komunikačních technologií. Nejedná se tedy jenom o skupinu trestných činů, které byly spáchány za využití propojené počítačové sítě internetu, jako prostředku ke spáchání podvodu, ale také za využití jiných komunikačních technologií, např. telefonní hovor.

Internet nebyl, není a nebude jenom prostředkem pro společensky prospěšnou činnost. Silné stránky internetu jako jeho globálnost, velké množství uživatelů, snadná dostupnost, rychlost a svoboda, jsou zároveň jeho slabinami, které využívají pachatelé při páchání trestné činnosti, čemuž jim napomáhá i anonymita internetu. Každý, kdo internet používá k prodeji, nákupům, komunikaci, vyhledávání informací, správě svých financí apod., se může stát cílem protiprávního jednání. Prostřednictvím internetu lze odkudkoliv zasáhnout komukoliv do života a ovlivnit jej pozitivně i negativně.

Kriminalita na internetu nezná hranic. Nejde pouze o internetové podvody, které jsou součástí velké rodiny kybernetické kriminality, ale např. i o útoky na počítačové sítě a její systémy, kritickou infrastrukturu, šíření dětské i jiné pornografie, šíření nenávistného obsahu. Jak pokračuje digitalizace společnosti, budou se objevovat nové způsoby páchání trestné činnosti, jako např. vzdálený zásah do autonomního řízení dopravních prostředků, zásah do inteligentní domácnosti apod.

Pokud nahlédneme do historie internetových podvodů v České republice zjistíme, že typickým internetovým podvodem bylo již od počátku jednání, při kterém pachatel nabízel k prodeji zboží, které po zaplacení nedodal. Následovaly útoky typu Ransomware. V prvních letech se jednalo o typ útoku, kdy škodlivý program zablokoval počítačový systém falešnou zprávou od policie a s odkazem na nevhodný obsah uloženy v počítači, požadoval zaplacení pokuty. Později již útoky typu

Ransomware byly propracovanější a docházelo při nich k šifrování dat uložených v počítačovém systému a byla požadována platba za jejich dešifrování. V roce 2014 následovala masivní kampaň s falešnou zprávou od exekučního úřadu, která byla zaslána e-mailovou zprávou a po otevření přílohy došlo ke spuštění škodlivého programu, který napadl počítač a monitoroval činnost uživatele při internetovém bankovnictví. Následně pod falešnou záminkou nutnosti zvýšení zabezpečení přiměl poškozeného k instalaci škodlivé aplikace do mobilního zařízení, a poté odčerpal finanční prostředky z účtu poškozeného. O vlně podvodných e-shopů se dá hovořit zejména v roce 2019. V době Covidu v letech 2019-2021 nastala kampaň „Ceo fraud“, kdy pachatelé využili situace omezených osobních kontaktů a celkové celosvětové situace a formou zaslané e-mailové zprávy s podvrhnutou hlavičkou odesílatele předstírali identitu jednatele, ředitele podniku či jiné odpovědné osoby a požadovali zaplacení falešné faktury. V těchto případech dosahovaly škody v jednotlivých případech řádu desítek miliónů.

Od roku 2022 se společnost potýká s obrovský nárustem kybernetické kriminality, především internetových podvodů, a jejím aktuálním stavem se zabývá tato diplomová práce.

Tak jak docházelo k rozmachu kybernetické kriminality a začal se zvětšovat její podíl na celkovém nápadu trestné činnosti, tak se musela přizpůsobovat i činnost policie. Zpočátku neexistovala na tento druh trestné činnosti žádná specializace a případy byly prověřovány na všech jejich organizačních článcích. V současné době je již vybudována struktura specializovaných pracovišť kybernetické kriminality.

Internetové podvody nemají zatím z kriminalistického hlediska zpracovanou metodiku vyšetřování. Existuje obecná metodika na podvody nebo metodika vyšetřování kybernetické kriminality. Internetové podvody však v sobě zahrnují problematiky obou těchto metodik.

Cílem této diplomové práce je popsat a stanovit typický model kriminalistické metodiky vyšetřování internetových podvodů.

K dosažení cíle jsem zvolil specifickou metodu kriminalistické vědy spočívající ve zevšeobecňování poznatků z policejní, vyšetřovací a soudní praxe. Jde o metodu, která spojuje kriminalistickou vědu s praxí.

Půjde o tvorbu metodiky nové, vytvořené na základě aktuálních požadavků kriminalistické praxe. Metodika bude vycházet z teoretických východisek a provedeného terénního šetření, při kterém byla provedena obsahová analýza vyšetřovacích spisů.

Práce je zpracována tak, aby odpovídala požadavkům kriminalistiky na tvorbu metodik vyšetřování, a proto je zvolena forma teoreticko-empirická a práce je rozdělena do čtyř kapitol.

První kapitola je věnována obecně teoretickým východiskům a je zde popsána teorie vyšetřování. Druhá kapitola nám přibližuje základní pojmy, které jsou důležité pro orientaci v práci a pochopení popisovaných jevů. Třetí kapitola je věnována provedenému výzkumu, je zde uveden výzkumný cíl, výzkumná strategie, metoda a použité postupy, výběr výzkumného souboru, realizace, zpracování dat a výsledky výzkumu, které jsou popsány a pro lepší přehlednost doplněny o grafy. Terénní šetření bylo provedeno u případů spáchaných na teritoriu Krajského ředitelství policie Zlínského kraje v roce 2022. Závěrečná kapitola naplňuje cíl práce a je věnována metodice vyšetřování internetových podvodů, která byla zpracována na základě výsledků provedeného výzkumu.

Téma diplomové práce „Metodika vyšetřování internetových podvodů – problémy teorie a praxe“ jsem si vybral, protože se touto problematikou profesně zabývám již od roku 2007 a měl jsem možnost sledovat její vývoj až do současné doby. Zaznamenal jsem, jak se v průběhu let měnil přístup k vyšetřování a jakými úskalími prochází policisté při jejím odhalování a vyšetřování. Využití internetu k páchání trestné činnosti nelze považovat za záležitost přechodného charakteru, ale naopak nad budoucností bychom měli přemýšlet tak, že tato forma se stane převládajícím způsobem páchání trestné činnosti.

Vzhledem k výše uvedenému se domnívám, že zpracování metodiky vyšetřování internetových podvodů může být přínosné, a to nejenom pro ty policisty, kteří tento druh trestné činnosti odhalují a vyšetřují, ale i pro ostatní, kteří se na rozvoji schopností policie prověřovat kybernetickou trestnou činnost podílejí.

1 TEORIE METODIKY VYŠETŘOVÁNÍ

1.1 Teoretická základy

„Teorie vyšetřování je jednou ze specifických teorií v systému kriminalistické vědy, která zkoumá zákonitosti vzniku, průběhu a projevů trestných činů v materiálním prostředí a ve vědomí lidí s cílem rozpracování optimálních modelů vyšetřovacích metod, metodik, technik, postupů a operací a jejich aplikace v procesu vyšetřování a prevence trestných činů.“[1]

Vědecké zkoumání vyšetřovací praxe přináší teoretickou úroveň poznání zákonitostí, formování a projevu kriminalistických rysů trestných činů i procesu vyšetřování. Vznikají tak poznatky a zobecněné informace o:

- nejcharakterističtějších zákonitostech,
- znacích různých trestných činů,
- zvláštnostech vznikajících při typických vyšetřovacích situacích,
- typových postupech vyšetřování,

které se využívají nejen k vypracování jednotlivých metodik vyšetřování trestných činů, ale i k prognózování možného rozvoje současné metodologie.[2]

Teorii vyšetřování můžeme rozdělit na část obecnou a zvláštní. V obecné části jsou rozpracovány základní teoretická východiska, pojmy a ostatní kategorie, které jsou společné pro všechny metodiky vyšetřování. Jednotlivé kategorie obecné části tedy vytvářejí základní osnovu pro každou dílčí metodiku vyšetřování, která potom tvoří zvláštní část teorie vyšetřování.[3]

1.2 Pojem a funkce metodiky vyšetřování

Metodika vyšetřování není kriminalistickou vědou chápána jako trestněprávní metodika přípravného řízení, ale jako: *„část kriminalistické vědy, která odhaluje a zkoumá zákonitosti vzniku stop a zvláštnosti postupů při vyhledávání, zajišťování*

---

[1] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4, str. 158.
[2] PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. aktualiz. a rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2, str. 829-830.
[3] STRAUS, Jiří, Viktor PORADA a kol. *Teorie, metody a metodologie kriminalistiky.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. ISBN 978-80-7380-666-8, str. 367.

a využívání stop, jiných soudních důkazů a kriminalisticky významných informací s ohledem na určitý typ trestného činu a předpokládanou typovou vyšetřovací situaci“[4] a má tedy úzkou vazbu na vyšetřovací praxi.

Metodika vyšetřování pokrývá tyto činnosti vyšetřovatele a policejních orgánů:

- **odhalování trestných činů** – aktivní vyhledávání informací o možném spáchání trestného činu; probíhá zpravidla v před procesním stadiu a řídí se policejním právem,
- **vyšetřování trestných činů** – procesní stadium upraveno trestním řádem,
- **kriminalistickou prevenci** – realizovaná převážně neprávními prostředky.[5]

Metodika vyšetřování jako součást kriminalistické vědy má tyto funkce:

- **poznávací funkci** plní metodika tak, že seskupuje trestné činy do stejnorodých skupin a podává popis jejich:
    - kriminalistické charakteristiky,
    - typických stop vznikajících při jejich páchání,
    - typických vyšetřovacích situací, které se utváří při jejich vyšetřování.
- **formativní funkci** plní metodika tak, že vytváří typové modely činností policejních orgánů v procesu poznání určité kategorie trestných činů. Jde o typové modely činnosti vyšetřovatele. Pro praxi jsou metodiky užitečné tím, že slouží jako návod pro sestavení plánu vyšetřování v konkrétním případě, který ulehčuje a zrychluje postup vyšetřovatele.
- **kontrolní funkci** plní metodika tak, že srovnává, zda dosud vypracovaná metodická doporučení jsou v praxi dostatečně efektivní a jsou v souladu se změnami způsobu páchání a změnami legislativními.[6]

[4] NĚMEC, Miroslav et. al. *Teorie a metodologie kriminalistiky pro magisterské studium – I. díl. Aktuální problémy kriminalistické teorie*. Praha: ABOOK, 2018. ISBN 978-80-906974-1-6, str. 62.
[5] MUSIL, Jan, Zdeněk KONRÁD a Jaroslav SUCHÁNEK. *Kriminalistika*. Praha: C. H. Beck, 2001. ISBN 80-7179-362-0, str. 370.
[6] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4, str. 161.

1.3 Systém a struktura metodik vyšetřování

Systém metodik vyšetřování není tvořen podle systemizace trestných činů uvedených ve zvláštní části trestního zákona, ale určujícím kritériem je typová kriminalistická charakteristika trestného činu. Podle této jsou vytvářeny stejnorodé skupiny trestných činů, které se páchají obdobným způsobem, zanechávají obdobné stopy a obdobným způsobem se vyšetřují. To znamená, že pro trestné činy, které mají shodné rozhodné prvky kriminalistické charakteristiky, spadají do jednoho typu trestných činů a mají vytvořený typový model činnosti – samostatná metodika.[7]

„Každý z typových modelů (metodik vyšetřování jednotlivých druhů trestných činů) představuje uspořádaný systém poznatků a doporučení s pevně stanovenou strukturou. Strukturu metodik vyšetřování jednotlivých druhů trestných činů představují následující komponenty:

1. *typová kriminalistická charakteristika dané skupiny trestných činů,*
2. *stopy typické pro daný typ trestných činů,*
3. *zvláštnosti předmětu vyšetřování,*
4. *typické podněty k vyšetřování a jejich zvláštnosti,*
5. *typické vyšetřovací situace vyskytující se při vyšetřování daného typu trestných činů,*
6. *typické počáteční úkony a jejich zvláštnosti,*
7. *typové vyšetřovací verze a zvláštnosti vytyčování vyšetřovacích verzí, plánování a organizace vyšetřování,*
8. *zvláštnosti následné etapy vyšetřování,*
9. *zvláštnosti zapojení veřejnosti do vyšetřování.“*[8]

[7] STRAUS, Jiří, Viktor PORADA a kol. *Teorie, metody a metodologie kriminalistiky.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. ISBN 978-80-7380-666-8, str. 371.

[8] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4, str. 162-163.

1.4 Typová kriminalistická charakteristika

„Kriminalistická charakteristika trestného činu je popisem kriminalisticky relevantních vlastností trestného činu, tj. takových vlastností, které ovlivňují proces tvorby stop a proces poznání trestného činu.“[9]

Struktura kriminalistické charakteristiky trestného činu spočívá v komponentách:

1. **Způsob páchání trestného činu**

Způsob, jakým byl trestný čin spáchán je základní součást kriminalistické charakteristiky, protože nejvíce ovlivňuje tvorbu stop a tím i možnost poznání trestného činu. Způsobem spáchání rozumíme vzájemně spjatý systém úkonů jednání pachatele a způsobů, jakými pachatel volí nebo využívá objektivní podmínky a prostředky při přípravě, páchání a utajování trestného činu.

2. **Kriminální situace**

Kriminální situací rozumíme situaci, za které byl trestný čin spáchán. K zásadním prvků kriminální situace řadíme: situační podmínky vnějšího prostředí, demografické podmínky, topografické podmínky, čas spáchání, meteorologické podmínky.

3. **Osobností rysy pachatele trestného činu**

Rozeznáváme tyto zásadní skupiny vlastností pachatelů: vlastnosti pachatelů určitých kategorií trestných činů; vlastnosti pachatelů, které ovlivňují průběh objasňování trestného činu; vlastnosti pachatelů, které ovlivňují vznik kriminalisticky relevantních informací.

4. **Osobnostní rysy oběti trestného činu**

Osobnostní rysy oběti jsou kriminalisticky relevantní především proto, že oběť je nositelem materiálních i paměťových stop, ale současně je i původcem stop, které zanechává na místě události, pachateli a předmětech. Kvalita paměťových stop je individuální a závisí na vnímání, uchovávání a reprodukci paměťových stop.

5. **Motiv činu**

Motiv činu je v některých případech trestných činů stále stejný (např. krádeže) a u jiných může být značně variabilní (např. u vraždy). Rozlišujeme tyto motivy: zištný, finanční, projevy žárlivosti, sexuální, emoce.[10]

---

[9] MUSIL, Jan, Zdeněk KONRÁD a Jaroslav SUCHÁNEK. *Kriminalistika*. 2. přeprac. a dopl. vyd. Praha: C. H. Beck, 2004. ISBN 80-7179-878-9, str. 31.

[10] STRAUS, Jiří, Viktor PORADA a kol. *Teorie, metody a metodologie kriminalistiky.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. ISBN 978-80-7380-666-8, str. 48-55.

1.5 Zásady metodik vyšetřování jednotlivých druhů trestných činů

Zásady metodik vyšetřování jednotlivých druhů trestných činů se dělí do dvou skupin:

1. Zásady tvorby metodik
2. Zásady aplikace metodik[11]

Pro tvorbu metodik platí tyto zásady:

- **vědeckost tvorby jednotlivých metodik** – základem musí být vědecké zobecnění kriminalistických aspektů vyšetřovací a soudní praxe a nelze stavět jen na zkušenosti jedné osoby,
- **závislost obsahu jednotlivých metodik na kriminalistické charakteristice daného trestného činu** – metodika musí svým obsahem odpovídat různorodosti kriminalisticky významných prvků určitého typu trestného činu,
- **systémový přístup k tvorbě jednotlivých metodik** – metodiky mají tvořit celistvý a strukturovaný systém,
- **dynamičnost tvorby jednotlivých metodik** – metodiky musí odrážet aktuální potřeby kriminalistické praxe.[12]

Při aplikaci jednotlivých druhů metodik v praxi platí:

- **zásada tvůrčího přizpůsobení metodiky konkrétním okolnostem trestného činu** – každý trestný čin je jedinečný, přestože vykazuje určité společné prvky, což vyžaduje tvůrčí aplikaci obecných doporučení na konkrétní okolnosti trestného činu,
- **zásada tvůrčího přizpůsobení metodických doporučení konkrétním vyšetřovacím situacím –** při vyšetřování dochází k jedinečným vyšetřovacím situacím, které nelze zobecňováním postihnout, proto je potřeba k řešení situací přistupovat tvůrčím způsobem.[13]

[11] MUSIL, Jan, Zdeněk KONRÁD a Jaroslav SUCHÁNEK. *Kriminalistika*. 2. přeprac. a dopl. vyd. Praha: C. H. Beck, 2004. ISBN 80-7179-878-9, str. 411.
[12] STRAUS, Jiří, Viktor PORADA a kol. *Teorie, metody a metodologie kriminalistiky.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. ISBN 978-80-7380-666-8, str. 376.
[13] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4, str. 166-167.

2 ZÁKLADNÍ POJMY

2.1 Kybernetický prostor

„Kybernetický prostor (Cyber Space) je globálně propojený prostor, který se skládá z Internetu a dalších počítačových sítí, digitálních zařízení, systémů, služeb a procesů na nich. Tím poskytuje globální infrastrukturu pro široké spektrum osobních, podnikatelských i správních aktivit a pro jejich propojení.“[14]

Základní charakteristika kyberprostoru:

1. **anonymita** – identita uživatele není jasně prokazatelná a garantovaná žádnou autoritou,
2. **asymetričnost** – bez ohledu na to, kdo činnost v kyberprostoru vyvinul, může mít jeho aktivita významný dopad na ostatní uživatele,
3. **neexistence hranic** – to co se v kyberprostoru děje není omezováno jurisdikcí, suverenitou, právním systémem či kulturou,
4. **okamžitos**t – akce provedená teď může mít okamžitý celosvětový dopad,
5. **volný vstup i ukončení pobytu v něm** – do kyberprostoru lze kdykoliv vstoupit i vystoupit,
6. **interakce** – uživatele se mohou vzájemně ovlivňovat.[15]

Podle Johna Barlowa, zakladatele Electronic Frontier Foundation, můžeme za kyberprostor považovat existující počítačové sítě a vlastně veškeré telekomunikační sítě. V kyberprostoru se tedy nalézáme, i když telefonujeme.[16]

2.2 Internet a IP adresa

Internet

„Globální systém propojených počítačových sítí, které používají standardní internetový protokol (TCP/IP). Internet slouží miliardám uživatelů po celém světě. Je to síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních

[14] DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4, str. 17.
[15] Tamtéž, str. 18-19.
[16] JIROVSKÝ, Václav. *Kybernetická kriminalita*. Praha: Grada Publishing, 2007. ISBN 978-80-247-1561- 2, str. 17.

a vládních sítí, s místním až globálním rozsahem, které jsou propojeny širokou škálou elektronických, bezdrátových a optických síťových technologií.“[17]

Počítačovou síť můžeme chápat: „*jako soubor (množinu) počítačových systémů, které jsou mezi sebou navzájem propojeny a mezi nimiž dochází k výměně dat či informací.“*[18]

Internet můžeme chápat jako komplexní vícevrstvý systém, ve kterém identifikujeme tyto 4 úrovně: technologická, komunikační, kulturní, organistická. První úroveň je systém počítačů, který prostřednictvím internetu přistupuje k informacím. Druhá úroveň nám umožňuje komunikovat celou řadu obsahů na velké vzdálenosti. Třetí úroveň chápeme v nejširším smyslu a obsahuje různé lidské ambice, záměry, hodnoty, produkty, plány. Vytváří také nový kulturní svět. A konečně je internet nezávislým organismem, který se vyvíjí stejně jako jakýkoliv jiný evoluční systém. Lidé jsou se svými myšlenkami, činy a ambicemi součástí tohoto organismu.[19]

IP adresa

„Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol) a slouží k rozlišení síťových rozhraní připojených k počítačové síti“.[20]

Pokud tedy chce počítačový systém komunikovat v rámci jakékoliv sítě, musí mít přidělenou IP adresu, která je v rámci koncové sítě jedinečná. IP adresa může být přidělována:

- **staticky** – počítačovému systému je „napevno“ manuálně přidělena IP adresa,
- **dynamicky** – při každém připojení počítačového systému k počítačové síti na základě MAC adresy je přidělena automaticky IP adresa nová.[21]

---

[17] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 5. dopl. a uprav. vyd. Praha: Česká pobočka AFCEA a Centrum kybernetické bezpečnosti, 2022. [cit. 28.10.2023]. ISBN: 978-80-908388-4-0, str. 83. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf.

[18] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 67.

[19] ABU-TAIEH, Evon, Abdelkrim El MOUATASIM a Issam H. AL HADID. *Cyberspace* [online]. Velká Británie: IntechOpen, 2020. [cit. 27.2.2024]. ISBN: 978-1-78985-858-7, str. 15. Dostupné z: https://www.google.cz/books/edition/Cyberspace/eqf8DwAAQBAJ?hl=cs&gbpv=1.

[20] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 5. dopl. a uprav. vyd. Praha: Česká pobočka AFCEA a Centrum kybernetické bezpečnosti, 2022. [cit. 28.10.2023]. ISBN: 978-80-908388-4-0, str. 85. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf.

[21] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 74.

Můžeme říct, že IP adresa je identifikátor, který nám směřuje k místu připojení. Zjistíme tedy místo připojení a účastníka smlouvy o připojení. IP adresa neidentifikuje konkrétní osobu, která v daném čase vykonávala určitou činnost. Výsledky šetření k IP adrese napomáhají ke zjištění takové osoby.

MAC adresa

Adresa MAC je jedinečný identifikátor, který přiřadil výrobce konkrétnímu síťovému hardwaru (jako jsou karty Wi-Fi nebo Ethernet) a jednoznačně identifikuje konkrétní zařízení. Na Mac adresu se však nelze 100 % spolehnout, protože ji lze změnit.[22]

Někteří poskytovatelé internetových služeb mohou například požadovat použití konkrétní adresy MAC pro přístup k jejich zařízení. Když se pokazí síťová karta a je vyměněna za jinou, přestanou jejich služby fungovat. Tehdy lze podvrhnout původní adresu MAC.[23]

IP adresa společně s MAC adresou může pomoci určit konkrétní místo a zařízení, ze kterého pachatel komunikoval, prováděl určitou činnost. Pokud si je pachatel těchto okolností vědom, může anonymizovat nejenom připojení k internetu, ale i zařízení ze kterého se připojuje.

2.3 Digitální stopa

Široká odborná veřejnost doma i v zahraničí digitální stopu definuje podle znění, které v roce 1999 navrhla pracovní skupina SWGDE – Scientific Working Group on Digital Evidence (Vědecká pracovní skupina pro digitální důkazy):

„Digitální stopa je jakákoliv informace s vypovídající hodnotou pro danou relevantní událost, uložená nebo přenášená v digitální podobě.“[24]

Jedná se o definici, která je otevřená jakékoliv digitální technologii. Pokrývá jak oblast počítačů a počítačové komunikace, tak i oblast digitálních přenosů (mobilní telefony, digitální TV), videa, audia, digitální fotografie, data uzavřených kamerových systémů,

---

[22] ABC LINUXU, 2005. *MAC adresa* [online]. [cit. 15.02.2024]. Dostupné z: https://www.abclinuxu.cz/slovnik/mac-adresa.

[23] GNOME HELP. *Co je MAC adresa?* [online]. [cit. 15.02.2024]. Dostupné z: https://help.gnome.org/users/gnome-help/stable/net-macaddress.html.cs

[24] RAK, Roman a Viktor PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství* [online]. 2005, roč. 16, č. 4. [cit. 19.11.2023]. Dostupné z: https://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf.

data systémů elektronických, zabezpečovacích a dalších technologií potencionálně spojených s páchaním trestné činnosti.[25]

Digitální stopa a její místo v klasické teorii stop

„Podstatou kriminalistických stop je exaktně zjištěná skutečnost formulovaná v obecné filozofické teorii vzájemného působení: „Působí-li na sebe současně dva nebo více objektů, dochází ke vzájemnému předávání informací o jednotlivých objektech navzájem.“[26]

Výsledkem vzájemného působení a předávání informací je tzv. **odraz**, který je považován za stopu za splnění tří podmínek:

1. **Odraz (změna) musí být v souvislosti s kriminalisticky relevantní událostí, abychom hovořili o kriminalistické stopě** – využití digitálních zařízení, výpočetní techniky zanechávají velké množství záznamů, které dokumentují aktivity uživatelů a užitého zařízení. O kriminalistických digitálních stopách v kriminalistickém pojetí hovoříme v souvislosti s počítačovou nebo kybernetickou kriminalitou, nebo s kriminalitou počítačově či kyberneticky související.
2. **Odraz (změna) musí existovat alespoň od svého vzniku do zjištění** – důraz na objektivní, nepopiratelnou dokumentaci digitálních stop.
3. **Odraz (změna) musí být vyhodnotitelný současnými metodami a prostředky** – pokud nelze získat z nalezených a zjištěných změn potřebné informace, nemá taková změna praktický upotřebitelný význam. Podmínka, která se přímo vztahuje na znaleckou činnost.[27]

V souvislosti s obecnou teorií stop, kde stopy jsou výsledkem odrazu, hovoříme o odrážených objektech, prostředcích odrazu a odrážejících objektech a subjektech. **Odrážený objekt** – v našem případě to jsou uživatelé výpočetní a digitální techniky a tato technika samotná. **Prostředek odrazu** – vlastnosti odrážených objektů

[25] RAK, Roman a Viktor PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství* [online]. 2005, roč. 16, č. 4. [cit. 19.11.2023]. Dostupné z: https://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf.

[26] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Teorie, metodologie a metody kriminalistické techniky*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-869-3, str. 55.

[27] RAK, Roman a Viktor PORADA. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2005, roč. 16, č. 1. [cit. 19.11.2023]. Dostupné z: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf.

a objektivní okolnosti. U osob to jsou obecně jejich psychologické vlastnosti, znalosti a dovednosti, které se odrážejí výběrem softwaru nebo zařízení pro svou činnost, úrovní jeho ovládání či využití. **Odrážející objekty a subjekty** – vnější materiální prostředí a vědomí lidí, na které odrážené objekty za pomoci prostředků odrazu působí. Technologie v konečném důsledku působí na záznamové médium, na které se ukládají data. Kromě tohoto materiálního prostředí jsou stopy o aktivitách odraženy i ve vědomí lidí. Tyto stopy jsou nemateriálního charakteru a v teorii kriminalistických stop je obecně nazýváme paměťovými stopami.[28]

Digitální stopy z pohledu kriminalistické kategorizace stop

Podle definice digitální stopy jde o informaci, která jako taková je nehmotná. V čase jejího ukládání se zhmotňuje v prostředí paměťového média, které je technologického charakteru. Abychom mohli přenášenou informaci přečíst a analyzovat, musíme ji nejprve technologicky zachytit a následně opět trvale nebo dočasně uložit na paměťové médium. Digitální stopa je:

- hmotného, materiálního charakteru,
- stopou vnitřní stavby odráženého objektu,
- převážně mikrostopou – k jejímu zviditelnění jsou nutná technologická zařízení a potřebný software,
- digitální stopu zařazujeme převážně mezi fyzikální stopy technologického charakteru.[29]

Zdroje digitálních stop

- **otevřené počítačové systémy** – počítač a jeho bezprostřední periférie,
- **komunikační systémy** – klasické pevné telefony, bezdrátové telekomunikační systémy, počítačové sítě a internet (např. e-mail a jeho obsah a logovací soubory serverů při přenosu jsou digitální stopou),
- **zařízení s integrovaným počítačovým čipem** – mobilní telefony, osobní digitální asistenti (PDA), čipové platební karty a mnoho dalších zařízení s počítačovým čipem (např. zařízení GPS).[30]

---

[28] PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. aktualiz. a rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2, str. 189-190.

[29] RAK, Roman a Viktor PORADA. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2005, roč. 16, č. 1. [cit. 19.11.2023]. Dostupné z: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf.

[30] PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. aktualiz. a rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2, str. 192-193.

Místo trestného činu a digitální stopy

Rozeznáváme 4 typické oblasti, kde je nutné hledat digitální stopy, které se v některých případech mohou mezi sebou překrývat, splývat:

1. **oblast zájmu** – obvykle cíl útoku,
2. **oblast podpory zájmu** – okolní prostředí, bezprostředně hraničící s oblastí zájmu (např. servery, komunikační cesty, spolupachatelé apod.),
3. **oblast pachatele** – místo, ze kterého pachatel organizuje, koordinuje aktivity směřované do oblasti zájmu,
4. **oblast zázemí pachatele** – jestliže pachatel svůj útok připravuje, obvykle přemýšlí, kam skrýt hodnoty získané z útoku.[31]

Vlastnosti a specifika digitálních stop

Aktivita uživatelů digitálních informačních a komunikačních technologií se odráží ve specifických vlastnostech digitálních stop, mezi které řadíme (bez nároku na úplnost):

- nehmotnost digitálních stop,
- latentnost digitálních stop,
- manipulovatelnost s časem v počítačových systémech,
- způsob uchovávání záznamů,
- dynamika činnosti počítačových systémů,
- komplexnost prostředí,
- vysoký stupeň interní a externí interakce probíhajících procesů,
- velký geografický rozsah prostoru s digitálními stopami.[32]

Digitální stopu řadíme pohledem trestního práva procesního mezi věcné a listinné důkazy, které jsou upraveny v § 112 zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád).

---

[31] RAK, Roman a Viktor PORADA. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2005, roč. 16, č. 1. [cit. 19.11.2023]. Dostupné z: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf.

[32] NĚMEC, Miroslav et. al. *Teorie a metodologie kriminalistiky pro magisterské studium – II. díl. Aktuální problémy kriminalistické praxe*. Praha: ABOOK, 2019. ISBN 978-80-906974-2-3, str. 312.
PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. aktualiz. a rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2, str. 196.

2.4 Kybernetická kriminalita

Kybernetická trestná činnost se odehrává v prostředí počítačových sítích, v kyberprostoru a představuje jakousi množinu pro veškerou trestnou činnost, ke které zde dochází. Velmi často je sem přenášena „klasická trestná činnost“, neboť zde je možné páchat ji efektivněji a rychleji (např. podvody). Vedle této trestné činnosti zde dochází k útokům novým, mnohdy dosud právem neřešeným.[33]

Kybernetickou trestnou činnost můžeme kumulativně definovat jako:

- trestný čin ohrožující informační a komunikační technologie,
- trestný čin využívající informační a komunikační technologie ke spáchání tradičních trestných činů,
- trestný čin vztahující se k obsahu, např. dětská pornografie, pomluva, porušení práv k duševnímu vlastnictví.[34]

Policie České republiky dělí kybernetickou kriminalitu na dvě části, které definuje takto:

1. *„Kriminalita, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí, kdy hlavním objektem útoku je samotná oblast informačních a komunikačních technologií a v nich obsažená data.“*
2. *„Kriminalita páchaná za výrazného využití informačních a komunikačních technologií, přičemž hlavním objektem útoku je zejména život, zdraví, majetek, svoboda, lidská důstojnost a mravnost.“*[35]

Podle tohoto dělení, řadíme internetové podvody do druhé skupiny kybernetické kriminality.

Britská národní kriminální agentura a její jednotka kybernetického zločinu dělí kybernetickou kriminalitu podle role, kterou při jejím páchání hraje technologie na:

1. počítačem podporované zločiny – zločiny, které byly i před internetem, ale s ním nabývají nového života jako např. podvody, pornografie, nenávistné projevy apod.,

[33] KOLOUCH, Jan, Pavel BAŠTA a kol. *Cybersecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34- 8, str. 83.
[34] GŘIVNA, Tomáš, Radim POLČÁK et al. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4, str. 35.
[35] POKYN policejního prezidenta č. 103/2013, *o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení* v posledním znění.

2. zločiny zaměřené na počítač – zločiny, které se objevily v tandemu se zřízením internetu a nemohly by bez něj existovat, např. hacking, virové útoky, znehodnocení webových stránek apod.[36]

Informační a komunikační technologie

Za informační a komunikační technologie se považuje: *„veškerá technika, která se zabývá zpracováním a přenosem informací, tj. zejména výpočetní a komunikační technika a její programové vybavení.“*[37]

2.5 Podvod

Skutková podstata trestného činu podvod je vyjádřena v § 209 trestního zákoníku takto:

„(1) Kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.

(2) Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a byl-li za takový čin v posledních třech letech odsouzen nebo potrestán.

(3) Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 větší škodu.

(4) Odnětím svobody na dvě léta až osm let bude pachatel potrestán,

a) spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,
b) spáchá-li takový čin jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,

---

[36] YAR Majid a Kevin F. Steinmetz. *Cybercrime and Society* [online]. Velká Británie: SAGE Publications, 2019. [cit. 27.2.2024]. ISBN: 9781526481658, kap. 1.4. Dostupné z: https://www.google.cz/books/edition/Cybercrime_and_Society/_nN7DwAAQBAJ?hl=cs&gbpv=1.

[37] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 5. dopl. a uprav. vyd. Praha: Česká pobočka AFCEA a Centrum kybernetické bezpečnosti, 2022. [cit. 28.10.2023]. ISBN: 978-80-908388-4-0, str. 77-78. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf.

c) spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo

d) způsobí-li takovým činem značnou škodu.

(5) Odnětím svobody na pět až deset let bude pachatel potrestán,

a) způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo

b) spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání teroristického trestného činu, trestného činu financování terorismu (§ 312d) nebo vyhrožování teroristickým trestným činem (§ 312f).

(6) Příprava je trestná.“[38]

U podvodu se jedná o trestněprávní ochranu majetkových zájmů před jednáním podvodného charakteru a objektem trestného činu podvodu je tedy cizí majetek.
Objektivní stránka spočívá v tom, že pachatel:

- uvede někoho v omyl,
- využije něčího omylu, nebo
- zamlčí podstatné skutečnosti,

v důsledku čehož oklamaná osoba provede majetkovou dispozici a tím:

- vznikne na cizím majetku škoda nikoliv nepatrná a
- zároveň se tím pachatel nebo jiná osoba obohatí.[39]

Abychom mohly skutek kvalifikovat, jako trestný čin podvod musí být činem způsobena **škoda nikoli nepatrná**, což je škoda dosahující částky nejméně 10.000 Kč.[40]

Pokud není způsobena škoda v uvedené výši, přichází v úvahu kvalifikovat podvodné jednání pachatele, jako přestupek proti majetku:

- u fyzických osob podle § 8 odst. 1 písm. a) bod 3 nebo
- u právnických nebo podnikajících fyzických osob podle § 8 odst. 2 písm. a) bod 3 zákona č. 251/2016., o některých přestupcích.

Zde je nutno zmínit, že škody u internetových podvodů často nedosahují škody nikoliv nepatrné a jsou kvalifikovány jako přestupky proti majetku. U každého takového

---

[38] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění, § 209.
[39] JELÍNEK, Jiří a kolektiv. *Trestní právo hmotné. Obecná část. Zvláštní část*. 8. aktualiz. vyd. Praha: Nakladatelství Leges, 2022. ISBN 978-80-7502-576-0, str. 683-684.
[40] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění, § 138.

jednání je nutné se zabývat otázkou, zda se nejedná o pokračování v přestupku nebo o pokračování v trestném činu. Škody způsobené pokračováním se sčítají, a tudíž správnou detekcí pokračování v trestném činu můžeme zmařit záměr pachatele vyhnout se trestnímu postihu tím, že bude páchat pouze skutky s přestupkovými škodami.

„Pokračováním v přestupku se rozumí takové jednání, jehož jednotlivé dílčí útoky vedené jednotným záměrem naplňují skutkovou podstatu stejného přestupku, jsou spojeny stejným nebo podobným způsobem provedení, blízkou souvislostí časovou a souvislostí v předmětu útoku.“[41]

„Pokračováním v trestném činu se rozumí takové jednání, jehož jednotlivé dílčí útoky vedené jednotným záměrem naplňují, byť i v souhrnu, skutkovou podstatu stejného trestného činu, jsou spojeny stejným nebo podobným způsobem provedení a blízkou souvislostí časovou a souvislostí v předmětu útoku.“[42]

Pokračování v trestném činu je splněno za těchto podmínek:

a) jednotný záměr – můžeme volněji chápat jako opakování trestného činu při stejné příležitosti,
b) stejný nebo obdobný způsob provedení – je splněn i v případě, kdy některé dílčí útoky mají znaky dokonaného trestného činu, jiné mají znaky pokusu nebo přípravy. Dílčí útoky mohou mít různý rozsah i způsobenou škodu,
c) blízká časová souvislost – je nutno brát ohled i na čas potřebný k přípravě na další útok,
d) jednotlivé útoky, byť v souhrnu naplňují skutkovou podstatu stejného trestného činu.[43]

Omyl je rozpor mezi představou a skutečností. O omyl se jedná i v případě, kdy podváděná osoba nemá o důležité okolnosti žádnou představu nebo se domnívá, že se nemá čeho obávat. **Uvedením v omyl** chápeme jednání, kterým pachatel předstírá okolnosti, které nejsou v souladu se skutečným stavem věcí. **Podstatné skutečnosti zamlčí** ten pachatel, který při svém podvodném jednání neuvede jakékoliv skutečnosti,

[41] Zákon č. 250/2016 Sb., *o odpovědnosti za přestupky a řízení o nich* v posledním znění, § 7.
[42] Zákon č. 40/2009 Sb., *trestní zákoník v posledním znění*, § 116.
[43] NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo hmotné*. 3. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-291-2, str. 97-98.

které jsou rozhodující nebo zásadní pro rozhodnutí poškozeného, popř. jiné podváděné osoby.[44]

Zavinění u podvodu je vyžadováno úmyslné, přičemž podvodný úmysl musí být již v době jednání pachatele vůči poškozenému. Samotný fakt nedodání zboží nebo nezaplacení kupní ceny automaticky neznamená, že se taková osoba dopustila podvodu. Pro posouzení subjektivní stránky je potřeba zvažovat všechny okolnosti případu. U internetových podvodů spojených s nabídkou zboží, které nebylo po zaplacení dodáno, je velmi důležité zjistit celkový objem obchodů, tedy aktivně vyhledávat další kupující s cílem zjistit, zda jim zboží bylo či nebylo dodáno. Častým trikem podvodníků je vybudovat si dobré renomé prodejem levných produktů a následně nabídnout produkty s vyšší prodejní cenou a ty již nedodat.

2.6 Internetové podvody

Pojem internetový podvod není odbornou veřejností přesněji definován, ale můžeme se setkat s definicí **počítačového podvodu**: „*Podvod spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený*.“[45] Nejobecněji je možné **internetový podvod** definovat jako: podvod probíhající online v kyberprostoru.

Jak již bylo uvedeno za kyberprostor považujeme veškeré počítačové a telekomunikační sítě, a proto do internetových podvodů řadíme nejenom typy podvodů, které mají spojitost s internetem, ale i ty které k jeho spáchání využívají telefonní hovor.

Internetový podvod tedy není speciálním typem podvodu, jako je tomu například u pojistných podvodů a nemá ve zvláštní části trestního zákoníku vyjádřenou samostatnou skutkovou podstatu, protože se jedná o obecný podvod podle § 209 trestního zákoníku.

Informační a komunikační technologie pachatelé zneužívají u podvodných praktik nejenom jako nástroj ke spáchání trestného činu, ale v některých případech přímo

[44] ŠÁMAL, Pavel, Tomáš GŘIVNA, Lukáš BOHUSLAV, Oto NOVOTNÝ, Jiří HERCEG et al. *Trestní právo hmotné*. 9. vyd. Praha: Wolters Kluwer ČR, 2022. ISBN 978-80-7598-764-8, str. 766-767.

[45] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 5. dopl. a uprav. vyd. Praha: Česká pobočka AFCEA a Centrum kybernetické bezpečnosti, 2022. [cit. 28.10.2023]. ISBN: 978-80-908388-4-0, str. 127. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf.

útočí na informační a komunikační technologie (např. internetbanking, smartbanking, vzdálená správa počítače).

Typy internetových podvodů se mění nejenom v čase, ale i podle zemí, kde jsou páchány. Pachatelé vždy reagují na nastalou hospodářskou, sociální a politickou situaci, kterou využívají pro svoji trestnou činnost.

2.6.1 Sociální inženýrství (Sociotechnika)

„Sociotechnika je ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá a kterou si vytvořil pro potřeby manipulace. Díky tomu je sociotechnik schopný využívat lidi, se kterými hovoří, případně dodatečné technologické prostředky, aby získal hledané informace.“[46]

Sociální inženýrství je tedy způsob, kterým pachatel manipuluje své oběti s cílem je přimět k určité činnosti, či s úmyslem získat požadované informace. Útoky sociotechnika jsou zpravidla vedeny těmito 3 způsoby, které se můžou i vzájemně kombinovat:

1. sběr volně (veřejně) dostupných dat o cíli útoku,
2. fyzický útok – útočník se snaží svou fyzickou přítomností, kdy se vydává např. za pracovníka servisní společnosti (pracovník údržby), získat co nejvíce informací,
3. psychologický útok.[47]

Útočníci využívají toho, že se v on-line prostředí chováme tak, jako by byli všichni lidé dobří a poctiví, a to přestože si uvědomujeme, že ne všichni takový jsou. Sociotechnik musí být okouzlující, zdvořilý, přesvědčivý a je snadné si ho oblíbit, což je potřebné k tomu, aby mohl získat porozumění a důvěru jiných. Sociotechnika je vlastně takové řemeslo, které umožňuje schopnému sociotechnikovi získat přístup prakticky ke každé informaci, či přimět jiného k určité činnosti.[48]

---

[46] MITNICK, Kevin a William SIMON. *Umění klamu*. Gliwice: Nakladatelství Helion, 2002. ISBN 83-7361-210-6, str.4.
[47] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 187-188.
[48] MITNICK, Kevin a William SIMON. *Umění klamu*. Gliwice: Nakladatelství Helion, 2002. ISBN 83-7361-210-6, str.24-25.

2.6.2 Phishing, Vishing, Spoofing, Smishing

Phishing

Jedná se o podvodnou metodu jejíž cílem je zcizování digitální identity uživatele, jeho citlivých informací, jako jsou jeho osobní údaje, přihlašovací jména, hesla, čísla bankovních účtů a karet apod., za účelem jejich následného zneužití (výběr finančních prostředků z bankovního účtu, neoprávněný přístup k datům apod.). Zmíněné informace se snaží útočník vylákat např. zasláním falešné, ale věrohodné zprávy, kde se maskuje za identitu věrohodného odesílatele. Může jít například o padělaný dotaz banky, kterou uživatel používá, s žádostí o aktualizaci svých přihlašovacích údajů (použití URL odkazu, který oběť nasměřuje na útočníkovy stránky) nebo vytvořením podvodné stránky banky, která se zobrazí v internetovém vyhledavači po zadání názvu banky, kdy po jejím otevření jsou opět požadovány přihlašovací údaje do internetového bankovnictví.[49]

Speciálním druhem phishingu je „**Spear phishing**“, kdy jsou využívány předem získané informace o uživateli, na kterého je útok zaměřen. Jedná se o přesně cílený útok na konkrétní skupinu, organizaci, jednotlivce.[50]

Vishing

Je ve své podstatě vishing (voice-hlas a phishing) za využití telefonického hovoru, při kterém využívá útočník technik sociálního inženýrství a snaží volaného přimět k určité činnosti nebo od něj získat citlivé informace, jako jsou osobní údaje, přihlašovací jména, hesla, čísla bankovních účtů a karet apod., za účelem jejich následného zneužití. Z důvodu co největší věrohodnosti útočníci, často předstírají identitu, bankéřů, policistů, případně jiných zástupců věrohodných institucí, společností.[51]

Tuto techniku dotáhli téměř k dokonalosti provozovatelé falešných call center. Během hovoru je vytvořena představa řádně fungujícího call centra a to tak, že operátor vystupuje profesionálně, v pozadí je slyšet okolní ruch, klient je přepojen na jiné kolegy

[49] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 5. dopl. a uprav. vyd. Praha: Česká pobočka AFCEA a Centrum kybernetické bezpečnosti, 2022. [cit. 28.10.2023]. ISBN: 978-80-908388-4-0, str. 122. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf.
[50] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, str. 264.
[51] Tamtéž, str. 265.

a komunikace probíhá tak dlouho, dokud falešní operátoři od poškozeného nezískají potřebné informace.[52]

Spoofing

V kybernetické kriminalitě znamená spoofing předstírání identity, za účelem získání důvěry a s cílem přimět oběť udělat to, co si útočník přeje. U vishingových útoků pachatelé falšují telefonní číslo volajícího pomocí technologie VoIP (volání přes internet), která jim umožňuje vytvoření čísla volajícího dle vlastního výběru (např. banky, policie).[53]

Smishing

Smishing (sms a phishing) je stejně jako phishing a vishing podvodná technika, při které se útočník snaží získat citlivé informace, jako jsou osobní údaje, přihlašovací jména, hesla, čísla bankovních účtů a karet apod., za účelem jejich následného zneužití. Útočník tedy zašle oběti SMS zprávu, ve které svou identitu maskuje za důvěryhodného odesílatele, jako je např. banka, různá ministerstva apod., a v této zprávě příjemce informuje např. o poskytnutí příspěvku, aktualizaci bankovních údajů apod., což má učinit tak, že klikne na přiložený URL odkaz, který směřuje na podvodné stránky útočníka.[54]

2.6.3 Reverzní inzertní podvod

Podvodná technika, při které pachatel předstírá zájem o zboží inzerované poškozeným na některém z inzertních portálů. Během následně vedené komunikace zašle poškozenému odkaz na platební bránu, kde si může vyzvednout peníze za zaplacené zboží. Platební brána však slouží zejména k získání přihlašovacích údajů do internetového bankovnictví (případně k získání identifikátorů platební karty), které následně pachatel použije pro vstup do internetového bankovnictví, k čemuž využije součinnost poškozeného, který mu po vhodné manipulaci přístup sám autorizuje.

---

[52] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozš a aktualiz. vyd. Plzeň: Nakladatelství a vydavatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5, str. 227.
[53] Kaspersky Lab. *What is Spoofing – Definition and Explanation* [online]. [cit. 20.2.2024]. Dostupné z: https://usa.kaspersky.com/resource-center/definitions/spoofing.
[54] Kaspersky Lab. *What is Smishing and How to Defend Against it?* [online]. [cit. 20.2.2024]. Dostupné z: https://usa.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it.

Následně pachatel provede převod všech dostupných finančních prostředků z účtu poškozeného a případně ještě odčerpá i finanční prostředky z předschváleného úvěru.

2.6.4 Inzertní podvod

Podvodná technika, při které pachatel umístí na internetový inzertní portál nabídku na prodej zboží. Často se jedná o nabídku na žádané zboží s podbízivou cenou. Může se ale také jednat v dané době a lokalitě o zboží nedostatkové a zde již cena může odpovídat ceně obvyklé. Po navázání kontaktu se vyhýbá osobnímu předání, uvádí vzdálenou lokalitu od místa pobytu kupce a preferuje platbu předem. Ve většině případů po provedení platby zboží buď nedodá nebo dodá věc jinou bezcennou či neodpovídající deklarovaným vlastnostem při prodeji.

2.6.5 Investiční podvody

Podvodná technika, při které pachatelé v první fázi umisťují na internetu reklamy, kterými lákají své oběti na lukrativní, neodolatelnou nabídku na zhodnocení finančních prostředků, a to investicí do kryptoměn, zejména Bitcoinů. Výhodnost investice je umocňována rozhovory se známými osobnostmi, které ji doporučují a potvrzují. Zájemci o investici vyplní elektronický formulář, ve kterém sdělí své osobní údaje včetně kontaktů.

Ve druhé fázi jsou tito zájemci telefonicky kontaktováni údajnými zástupci investičních společností a jsou manipulováni tak, aby zaslali oskenované nebo vyfocené své osobní doklady, které pachatelé využívají k registraci u legitimních obchodníků s kryptoměnou a dále jsou přesvědčeni k prvotní investici, která je použita jako vklad ve prospěch bitcoinové peněženky, ke které však poškozený nemá přístup. Tento vklad se zobrazuje poškozenému v podvodné investiční platformě a ten se mylně domnívá, že tyto prostředky stále drží a může s nimi disponovat.

Ve třetí fázi je poškozený pod legendou ověření funkčnosti investičního systému a z důvodu seznámení se s jeho fungováním zmanipulován tak, aby si nainstaloval program, který umožnuje vzdálenou správu zařízení přes internet a aby provedl přihlášení do svého internetového bankovnictví.

Čtvrtá fáze spočívá v převodu všech dostupných finančních prostředků z účtu poškozeného, a to buď za přímé součinnosti poškozeného, který se mylně domnívá, že převody finančních prostředků slouží k jejich investování, a proto je autorizuje nebo tyto převody po ovládnutí bankovního účtu provádí pachatel bez vědomí jeho majitele. Jestli je k účtu veden i předschválený úvěr žádá pachatel o jeho čerpání.

V některých případech je oběť zmanipulována tak, že v dobré víře svolí k tomu, aby byl její bankovní účet používán k převodu peněz od domnělých finančních partnerů, kteří jsou však jinými poškozenými, což však oběti není známo. Takto ovládané účty potom slouží k legalizaci výnosů z trestné činnosti.

2.6.6 Výplata falešného zisku

Podvod při výplatě údajného výnosu z investice do kryptoměny. Jedná se o obdobnou podvodnou techniku jako u podvodných investic. V první fázi pachatel telefonicky kontaktuje oběť a informuje ji, že na její jméno jsou vedeny zhodnocené finanční prostředky, zejména z investic do kryptoměny. V další fází nabídne poškozenému pomoc při jejich vyplacení a manipuluje ho tak, aby si nainstaloval program, který umožnuje vzdálenou správu zařízení přes internet a aby provedl přihlášení do svého internetového bankovnictví. Poslední fáze spočívá v převodu všech dostupných finančních prostředků z účtu poškozeného, a to buď za přímé součinnosti poškozeného, který se mylně domnívá, že převody finančních prostředků slouží k výplatě peněz, a proto je autorizuje nebo tyto převody po ovládnutí bankovního účtu provádí pachatel bez vědomí jeho majitele. Jestli je k účtu veden i předschválený úvěr žádá pachatel o jeho čerpání. Oběti poskytují potřebnou součinnost i v případech, kdy do kryptoměn neinvestovali, ale jsou zlákání vidinou rychlého obohacení.

2.6.7 Scam 419

Jedná se v podstatě o klasický podvod, k jehož páchání jsou využity prostředky internetu, jako jsou e-mailové zprávy či jiné způsoby navázání a vedení komunikace, a to zejména v její psané podobě. V době, kdy ještě nebyl internet, se k navazování kontaktů používalo rozesílání dopisů. Jedná se o manipulativní techniku, jejímž cílem je přimět oběť k zaslání peněz, a to zejména pod těmito legendami:

- milostný příběh – pachatel pod falešnou identitou předstírá lásku k oběti a tím ji přiměje k zaslání finančních prostředků,
- dědictví – pachatel pod falešnou záminkou získání dědictví přiměje pod různými záminkami oběť k zaslání finančních prostředků,
- neočekávaná výhra – pachatel pod falešnou záminkou vyplacení výhry přiměje pod různými záminkami oběť k zaslání finančních prostředků.

A proč název Scam 419? Původ názvu pochází z 80. let 20. století, kdy se ještě v písemné podobě začaly objevovat dopisy odesílané například údajným ředitelem Nigerijské Národní Petrolejářské Korporace s nabídkou převodu 20 milionů dolarů se slíbeným podílem 30 %. Následně byla i řada jiných „nigerijských" variant, a protože v nigérijském trestním řádu, který popisuje tento způsob finančních podvodů, je ustanoven v § 419, zdomácněl název podvod 419 – Scam 419.[55]

2.6.8 Falešný bankéř

Podvodná technika, při které pachatel telefonicky kontaktuje svou potencionální oběť a vydává se za pracovníka banky případně i policistu a pod legendou napadení, ohrožení bankovního účtu např. počítačovým virem, požadavkem na změnu autorizačního telefonního čísla, falešnou informací o požadavku o půjčku, manipuluje svou oběť tak, aby činila určité kroky k záchraně svých finančních prostředků.

Takovým krokem může být převod veškerých finančních prostředků na jiný bezpečný účet, a to včetně finančních prostředků získaných z předschváleného úvěru nebo výběrem veškerých finančních prostředků a jejich následným vložením do záchranného bankomatu banky. Takovým záchranným bankomatem jsou však vkladomaty na virtuální měnu, kde jsou vložené finanční prostředky připisovány na krypto peněženky pachatele, ke kterým nemá poškozený přístup.

Tato technika je nebezpečná v tom, že pachatel zná některé důvěrné informace o oběti, které mohl získat předchozím zdánlivě neškodným telefonátem, z volných zdrojů, uniklých databází, či cestou předchozího phishingového útoku, který poškozený nerozeznal. Útočníci dále používají techniku tzv. **spoofingu**, což je

[55] KLOZOVÁ Miroslava, 2021. Podvod 419 alias "SCAM 419"– 2021. In: *INTERNETEM BEZPEČNĚ* [online]. [cit. 13.12.2023]. Dostupné z: https://www.internetembezpecne.cz/podvod-419-alias-scam-419/.

v obecné rovině činnost jejímž cílem je oklamat uživatele pomocí předstírané/podvržené falešné identity. U spoofingu se jedná o využití takových technických prostředků, které dokážou napodobit jakékoliv telefonní číslo volajícího, což činí útok velmi nebezpečný. Pokud si oběť telefonní číslo vyhledá, ale neprovede zpětný hovor tak zjistí, že zobrazené číslo opravdu patří instituci, za kterou se pachatel vydává a úkony, které po něm pachatel požaduje, provádí v mylné představě oprávněného požadavku.

3 VÝZKUM

3.1 Výzkumný cíl

Hlavním cílem výzkumu bylo zjistit a vymezit kriminalistickou charakteristiku internetových podvodů, tedy: způsob spáchání, kriminální situace, osobnostní rysy pachatele a oběti trestného činu, motiv činu.

Dílčími cíli výzkumu pak jsou:

1) Zjistit typické stopy a jiné soudní důkazy u internetových podvodů.
2) Zjistit zvláštnosti předmětu vyšetřování u internetových podvodů.
3) Zjistit typické podněty a jejich zvláštnosti u internetových podvodů.
4) Zjistit typické počáteční vyšetřovací situace u internetových podvodů.
5) Zjistit zvláštnosti počátečních úkonů a opatření u internetových podvodů.
6) Zjistit zvláštnosti následných úkonů u internetových podvodů.

Splnění vytyčených výzkumných cílů nám umožní dosáhnou cíle této diplomové práce, tedy popsat a stanovit typický model kriminalistické metodiky vyšetřování internetových podvodů.

3.2 Výzkumná strategie, metoda a použité postupy

K dosažení cíle práce jsem zvolil specifickou metodu kriminalistické vědy spočívající ve zevšeobecňování poznatků z policejní, vyšetřovací a soudní praxe.

Za výzkumnou strategii jsem zvolil kvantitativní výzkum a pro získání potřebných informací jsem provedl tyto postupy:

- zajištění výzkumného souboru,
- stanovení výzkumných otázek k dosažení zvolených cílů (Příloha 1),
- sběr dat provedený metodou obsahové analýzy vyšetřovacích spisů (terénní šetření),
- analýza získaných dat za využití statistických metod a jejich interpretace,
    - výsledky zjištění jsem seskupil do jednotlivých oddílů tak, aby odrážely stanovené výzkumné cíle,
- vytvoření metodiky vyšetřování internetových podvodů.

3.3. Výzkumný soubor

Výzkumným souborem je množina trestných činů spáchaných na teritoriu Krajského ředitelství policie Zlínského kraje v období od 1.1.2022 do 31.12.2022, kvalifikovaných jako trestný čin podvod podle § 209 trestního zákoníku a spáchaných v prostředí internetu.

K zajištění výzkumného souboru byl použit informační systém Policie ČR, konkrétně pak informační systém ETŘ (elektronické trestní řízení), ve kterém byl definován dotaz splňující tyto atributy:

1. oznámení případu od 1.1.2022 do 31.12.2022,
2. místní příslušnost v působnosti Krajského ředitelství policie Zlínského kraje,
3. trestný čin podvod,
4. sledovaná událost "IT kriminalita“.

Bylo zjištěno, že zadaná kritéria splňuje celkem 654 případů.

Z tohoto souboru byly vyloučeny případy, které byly k datu 5. 12. 2023 ukončeny odložením podle § 159a odst. 1 trestního řádu, protože ve věcech nešlo o podezření z trestného činu. Soubor poté čítal 647 případů.

Tento soubor (647 případů) byl vyhodnocen za účelem zjištění nejčastějších způsobů jednání pachatele při páchání internetových podvodů, viz níže otázka č. 1.

Samostatný způsob byl kategorizován, pokud tímto jednáním bylo provedeno alespoň 20 případů.

Dále byl výzkumný soubor o 647 případech zúžen tak, aby zahrnoval:

5. ukončené případy, popř. vyšetřování k datu 5. 12. 2023 (celkem 340 případů),
6. pro každý zjištěný způsob spáchání byl vybrán vzorek 10 případů, které vždy zahrnovaly objasněné případy a případy ve vyšetřování (celkem 24 z 340 případů),
7. pokud nebyl zajištěn vzorek 10 případů, podle kritéria 6, byl vzorek doplněn o ukončené, ale neobjasněné případy.

Tímto způsobem byl získán výzkumný soubor o 80 případech.

Poněkud komplikovanější přístup k zajištění výzkumného souboru byl zvolen z důvodu získání komplexní informace o jednotlivých způsobech jednání pachatele při páchání internetových podvodů.

Další údaje k výzkumnému souboru

Prvotní kritéria splňovalo 654 případů. Celkem 7 případů bylo ukončeno odložením podle § 159a odst. 1 trestního řádu.
Na Krajském ředitelství policie Zlínského kraje bylo ke dni 5. 12. 2023, kdy byla získána výzkumná data, ukončeno (nebo je ve vyšetřování) 340 případů a z toho bylo 24 (7 %) objasněno. Mezi objasněné jsou zahrnuty případy, u kterých byl zjištěn pachatel (zkrácené přípravné řízení, návrh na podání obžaloby, jiné ukončení s pachatelem) nebo jsou ve vyšetřování.
Způsob evidování zbylých 307 případů neumožňuje bez analýzy konkrétního spisu určit, zda je stále v prověřování na organizačním článku Krajského ředitelství policie Zlínského kraje nebo byl postoupen na jiný útvar, kde je v prověřování, vyšetřování nebo jakým způsobem byl ukončen.

3.4 Realizace výzkumu

Realizace výzkumu proběhla podle připraveného časového plánu v měsíci prosinci 2023. Výzkumný soubor byl získán k datu 5. prosince 2023. Následně bylo provedeno terénní šetření a obsahovou analýzou vyšetřovacích spisů byly zjištěny odpovědi na výzkumné otázky. Terénní šetření bylo provedeno po přechozím souhlasu oprávněného služebního funkcionáře.

3.5 Zpracování dat

Zjištěné odpovědi na výzkumné otázky byly zpracovávány v programu Microsoft Excel. Data byla strukturovaně rozřazena, zjištěna četnost a vyjádřena jejich procentuální hodnota. Data byla pro lepší přehlednost vizualizována do grafické podoby (grafy) a doplněna slovním popisem. U jednoznačných výsledků nebylo grafické znázornění použito. Vizualizace pomocí grafu, byla použita i u zjištění s velkým počtem údajů z důvodu přehledného znázornění převažujících hodnot. Tabulková vizualizace by pro tento účel byla méně přehledná.

3.6 Výsledky výzkumu

Informace zjištěné výzkumem jsou prezentovány v jednotlivých bodech tak, aby se v nich odrážely stanovené výzkumné cíle.

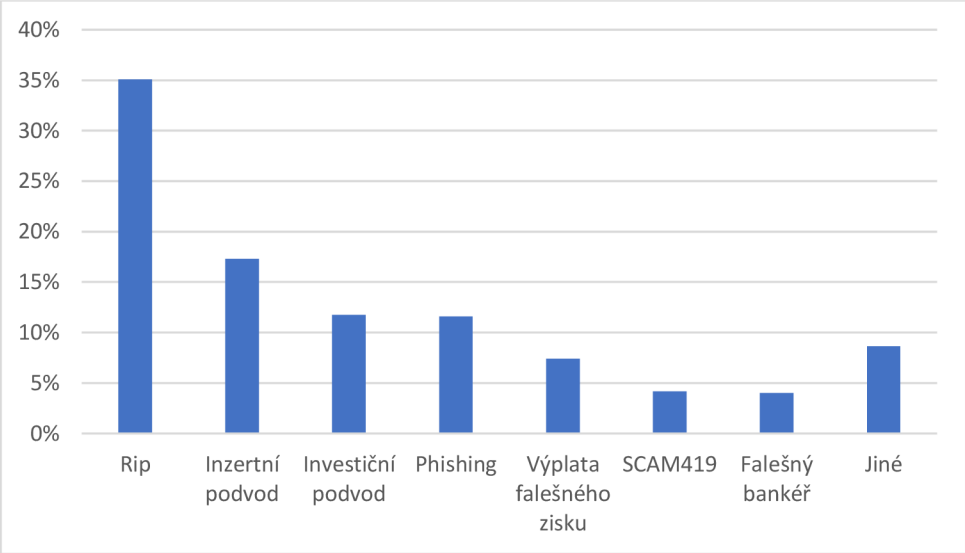
3.6.1 Výsledky k hlavnímu cíli

Hlavním cílem bylo zjistit, jaká je typová kriminalistická charakteristika trestného činu podvodu spáchaného v prostředí internetu na teritoriu Krajského ředitelství policie Zlínského kraje v roce 2022.

3.6.1.1 Způsob páchání

Otázka č. 1 byla zaměřena na zjištění, jaké jsou nejčastější způsoby jednání pachatele.

Výzkumný soubor obsahoval 647 případů. Bylo zjištěno 227 (35 %) případů reverzních inzertních podvodů, 112 (17 %) případů inzertních podvodů, 76 (12 %) případů investičních podvodů, 75 (12 %) případů phishingu, 48 (7 %) případů při výplatě falešného zisku, 27 (4 %) případů SCAM419, 26 (4 %) případů falešného bankéře a 56 (9 %) případů jiných podvodných jednání. Za jiné podvodné jednání lze považovat např. podvody s falešnými fakturami, podvodné pronájmy bytů, podvodné sázky, podvodný odběr služeb pod falešnou identitou apod.



Graf 1: Způsob jednání pachatele.

Zdroj: Vlastní zpracování

Otázka č. 2 byla zaměřena na zjištění, jaký komunikační prostředek pachatel použil.

Výzkumný soubor obsahoval 80 případů. Během jednání pachatele s poškozeným mohlo být použito více prostředků komunikace, např. prvotní kontakt voláním a následné instrukce zaslány e-mailem. Tato informace má na procentuální vyjádření ten význam, že součet procent u jednotlivých způsobů jednání pachatele a využitých komunikačních prostředků není roven 100 %.

Jako „jiné“ byly kategorizovány ty případy, kdy komunikace proběhla méně častým způsobem jako je komunikace formou chatu v prodejní platformě (např. Vinded), prostřednictvím Facebooku, Instagramu, telegramu, jiných komunikátorů apod.

Jako nejčastější způsob byl zjištěn kontakt e-mailem a to v 38 (48 %) případech, volání ve 34 (43 %) případech, jiný způsob komunikace ve 24 (30 %) případech, WhatsApp v 15 (19 %) případech, Messenger ve 13 (16 %) případech a SMS v 9 (11 %) případech.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – nejčastěji byl využit WhatsApp 6 (60 %) případů, e-mail 5 (50 %) případů, „jiné“ 4 (40 %) případy, sms 1 (10 %) případ. Volání a messenger nebyly využity.

Inzertní podvod – nejčastěji byl využit Messenger 5 (50 %) případů a e-mail 5 (50 %) případů, volání 4 (40 %) případy, „jiné“ 3 (30 %) případy, SMS 1 (10 %) případ, WhatsApp 1 (10 %) případ.

Investiční podvod – nejčastěji bylo využito volání 10 (100 %) případů, WhatApp 5 (50 %) případů, e-mail 4 (40 %) případy. SMS, Messenger a „jiné“ nebyly využity.

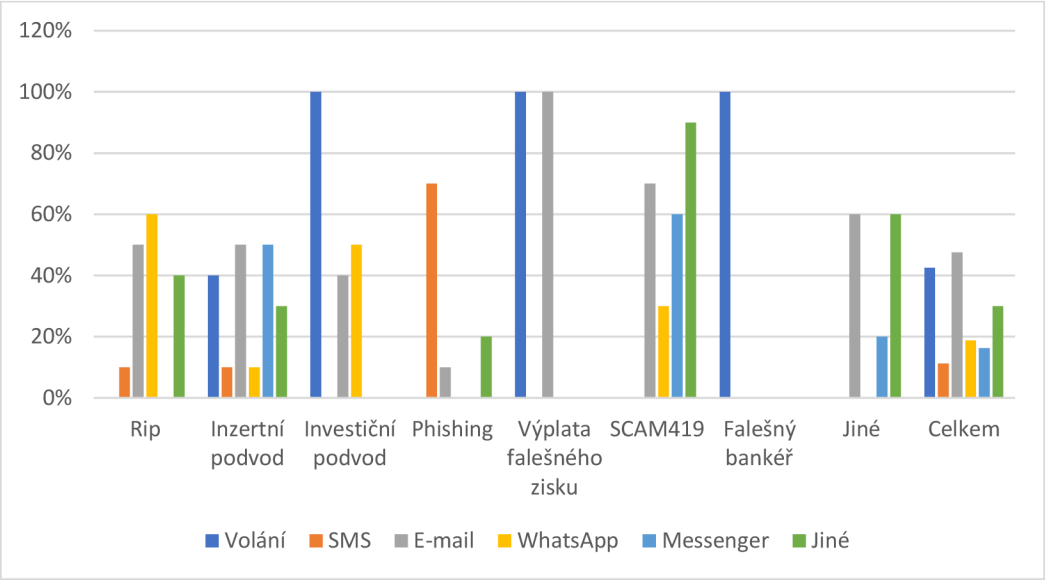
Phishing – nejčastěji byla využita SMS v 7 (70 %) případech, jiné 2 (20 %) případy, e- mail 1 (10 %) případ. Volání, WhatsApp a Messenger nebyly využity.

Výplata falešného zisku – nejčastěji bylo využito volání 10 (100 %) případů a e-mail 10 (100 %) případů. SMS, WhatsApp, Messenger a „jiné“ nebyly využity.

SCAM419 – nejčastěji byl využit jiný způsob komunikace a to v 9 (90 %) případech, e – mail 7 (70 %) případů, Messenger 6 (60 %) případů, WhatsApp 3 (30 %) případy. Volaní a SMS nebyly využity.

Falešný bankéř – pouze volání 10 (100 %) případů. Ostatní způsoby nebyly využity.

Jiné – nejčastěji byl využit e-mail 6 (60 %) případů, jiné 6 (60 %) případů, Messenger 2 (20 %) případy. Volání, SMS a WhatsApp nebyly využity.



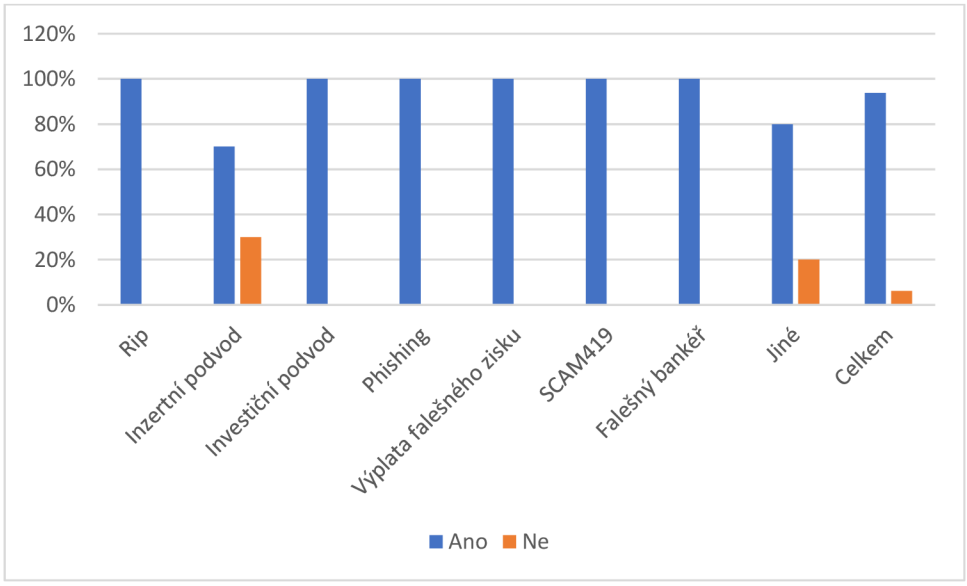
Graf 2: Komunikační prostředek.

Zdroj: Vlastní zpracování

Otázka č. 3 byla zaměřena na zjištění, jestli pachatel skrýval svou identitu, nebo jednal vlastním jménem.

Výzkumný soubor obsahoval 80 případů. Pachatel skrýval identitu v 75 (94 %) případech a v 5 (6 %) případech vystupoval pod vlastním jménem. U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – ve všech případech (100 %) skrytá identita. **Inzertní podvod** – v 7 (70 %) případech skrytá identita a ve 3 (30 %) případech vlastní jméno. **Jiné** – v 8 (80 %) případech skrytá identita a ve 2 (20 %) případech vlastní jméno.



Graf 3: Skrytá identita.

Zdroj: Vlastní zpracování

Otázka č. 4 byla zaměřena na zjištění, zda pachatel využil technických prostředků anonymizace komunikace.

Výzkumný soubor obsahoval 80 případů. Během jednání pachatele s poškozeným mohlo být použito více prostředků komunikace, a tedy více technických prostředků její anonymizace. Tato informace má na procentuální vyjádření ten význam, že součet procent u jednotlivých způsobů jednání pachatele a využitých prostředků anonymizace není roven 100 %. Pachatel použil technických prostředků anonymizace komunikace celkem v 63 (79 %) případech, v 5 (6 %) případech je nevyužil a ve 12 (15 %) případech to nebylo zjišťováno. Celkem v 50 (63 %) případech se jednalo o využití anonymizované IP adresy, ve 34 (43 %) případech o zneužití telefonního čísla a ve 13 (16 %) případech o spoofing.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – anonymizace komunikace celkem v 9 (90 %) případech a v 1 (10 %) případu to nebylo zjišťováno. Celkem v 9 (90 %) případech se jednalo o využití anonymizované IP adresy, v 6 (60 %) případech o zneužití telefonního čísla, ostatní možnosti nebyly využity.

Inzertní podvod – anonymizace komunikace celkem v 5 (50 %) případech, ve 3 (30 %) případech nevyužita a ve 2 (20 %) případech to nebylo zjišťováno. Celkem v 5 (50 %) případech zneužití telefonního čísla, ostatní možnosti nebyly využity.

Investiční podvod – anonymizace komunikace celkem v 8 (80 %) případech a ve 2 (20 %) případech to nebylo zjišťováno. Celkem v 8 (80 %) případech se jednalo o využití anonymizované IP adresy, v 7 (70 %) případech o zneužití telefonního čísla a v 1 (10 %) případě o spoofing, ostatní možnosti nebyly využity.

Phishing – anonymizace komunikace celkem v 9 (90 %) případech a v 1 (10 %) případu to nebylo zjišťováno. Celkem v 9 (90 %) případech se jednalo o využití anonymizované IP adresy, v 7 (70 %) případech o zneužití telefonního čísla, ostatní možnosti nebyly využity.

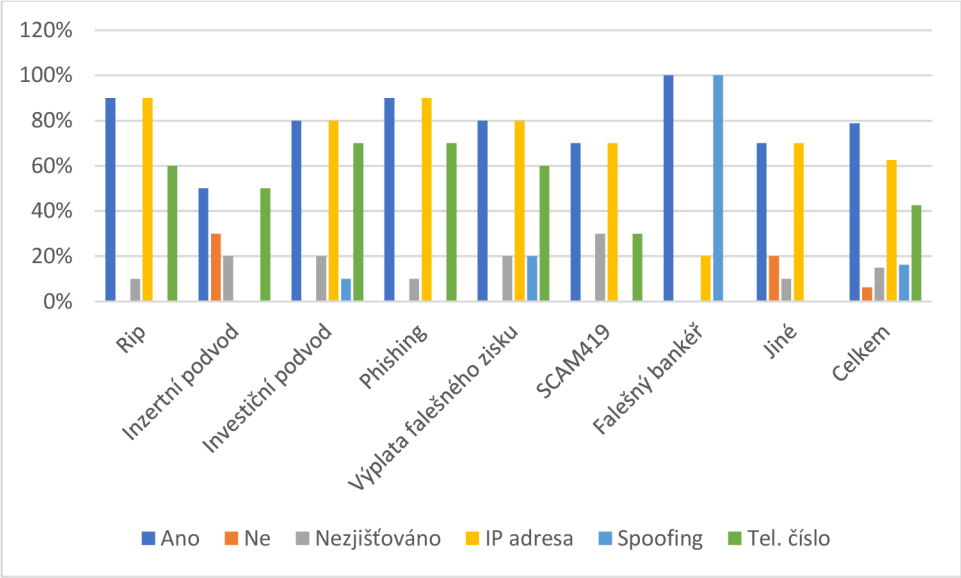
Výplata falešného zisku – anonymizace komunikace celkem v 8 (80 %) a ve 2 (20 %) případech to nebylo zjišťováno. Celkem v 8 (80 %) případech se jednalo o využití anonymizované IP adresy, v 6 (60 %) případech o zneužití telefonního čísla a ve 2 (20 %) případech o spoofing, ostatní možnosti nebyly využity.

SCAM419 – anonymizace komunikace celkem v 7 (70 %) případech a ve 3 (30 %) případech to nebylo zjišťováno. Celkem v 7 (70 %) případech se jednalo o využití

anonymizované IP adresy, ve 3 (30 %) případech o zneužití telefonního čísla, ostatní možnosti nebyly využity.

Falešný bankéř – anonymizace komunikace celkem v 10 (100 %) případech. Celkem ve 2 (20 %) případech se jednalo o využití anonymizované IP adresy a v 10 (100 %) případech o spoofing, ostatní možnosti nebyly využity.

Jiné – anonymizace komunikace celkem v 7 (70 %) případech, ve 2 (20 %) případech nevyužita a v 1 (10 %) případu to nebylo zjišťováno. Celkem v 7 (70 %) případech se jednalo o využití anonymizované IP adresy.



Graf 4: Technické prostředky anonymizace komunikace.

Zdroj: Vlastní zpracování

Otázka č. 5 byla zaměřena na zjištění, jaký byl vztah pachatele k použité technice.

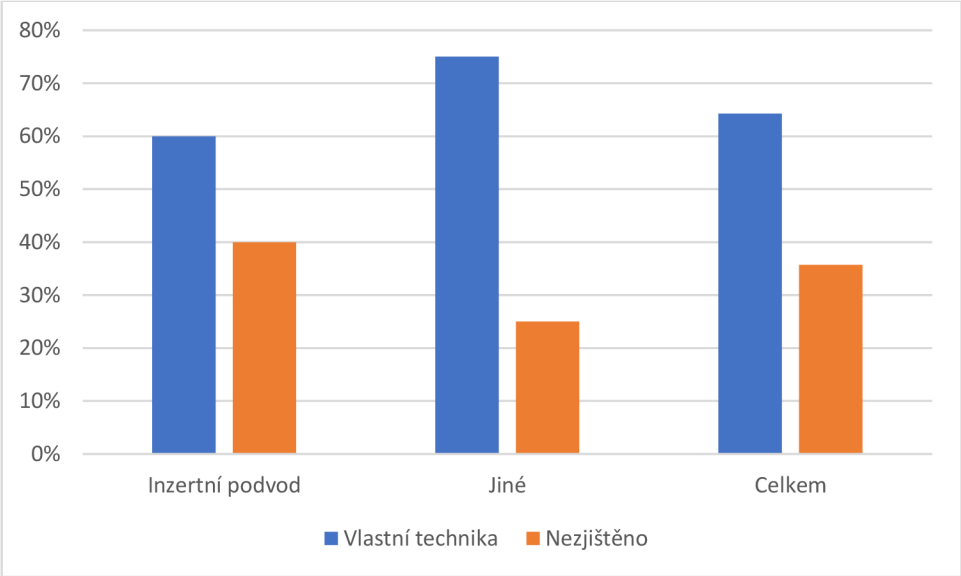
Z výzkumného souboru o 80 případech se jednalo o 14 objasněných případů, u který se dala tato informace zjistit: inzertní podvod, jiné. Celkem v 9 (64 %) případech bylo zjištěno, že pachatel použil vlastní techniku a v 5 (36 %) případech to nebylo zjišťováno.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – nebylo zjišťováno.

Inzertní podvod – informace byla zjišťována u všech 10 objasněných případů a bylo zjištěno, že v 6 (60 %) případech pachatel použil vlastní techniku a ve 4 (40 %) případech to nebylo zjišťováno.

Jiné – informace byla zjišťována u 4 objasněných případů a bylo zjištěno, že ve 3 (75 %) případech pachatel použil vlastní techniku a v 1 (25 %) případu to nebylo zjišťováno.



Graf 5: Vztah pachatele k použité technice.

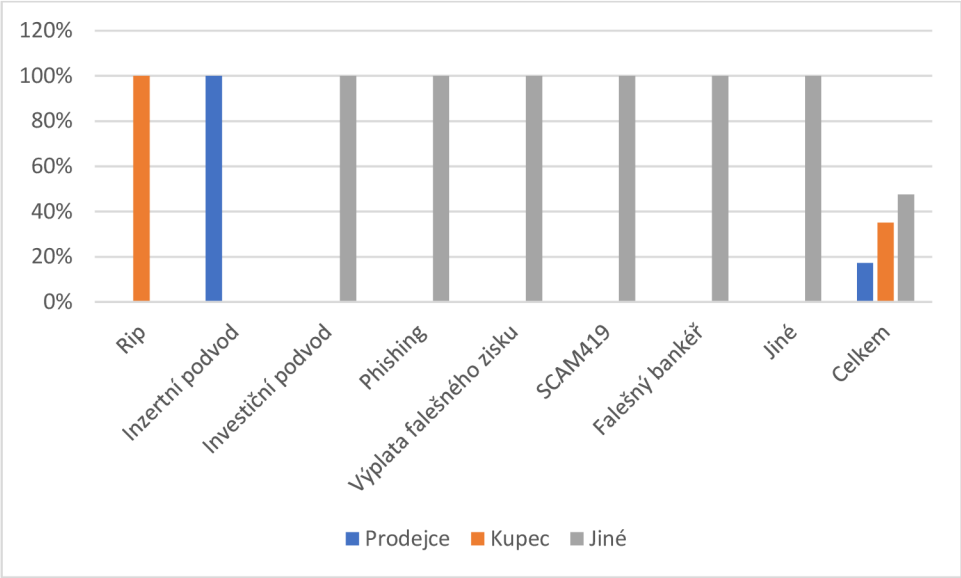
Zdroj: Vlastní zpracování

Otázka č. 6 byla zaměřena na zjištění, jaké bylo při podvodu postavení pachatele, zda se jednalo o kupce nebo prodejce.

Výzkumný soubor obsahoval 647 případů. Celkem ve 112 (17 %) případech byl pachatel v postavení prodejce, ve 227 (35 %) případech měl postavení kupce a ve 308 (48 %) případech měl jiné postavení jako např. investiční poradce, falešný bankéř, falešný lékař, podvodné sázky, pronájmy bytů apod.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – ve všech 227 (100 %) případech se jednalo o postavení kupce.
Inzertní podvod – ve všech 112 (100 %) případech se jednalo o postavení prodejce.
Investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř, jiné – ve všech případech (100 %) se jednalo o jiné postavení.



Graf 6: Postavení pachatele při obchodu.

Zdroj: Vlastní zpracování

Otázka č. 7 byla zaměřena na zjištění, v kolika případech zaslal pachatel zásilku.

Z výzkumného souboru o 80 případech se jednalo o 10 případů (inzertní podvod), u kterých pachatel vystupoval jako prodejce. Zásilka byla zaslána ve 2 (20 %) případech a v 8 (80 %) případech zaslána nebyla. Grafické znázornění nebylo použito.

Otázka č. 8 byla zaměřena na zjištění, jaký způsob platby nebo převodu peněz pachatel využil.

Výzkumný soubor obsahoval 80 případů. V jednotlivých případech mohlo dojít k vícenásobnému převodu peněz, a to různými způsoby. Tato informace má na procentuální vyjádření ten význam, že součet procent u jednotlivých způsobů jednání pachatele a způsobů plateb nebo převodů peněz není roven 100 %. Bankovní účet byl použit v 65 (81 %) případech, služby převodu peněz v 17 (21 %) případech, bankomat ve 2 (3 %) případech, bitcoinmat ve 2 (3 %) případech, platební karta ve 13 (16 %) případech, kryptoměna v 18 (23 %) případech.

U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod – bankovní účet byl použit v 7 (70 %) případech, služby převodu peněz ve 3 (30 %) případech, bankomat ve 2 (20 %) případech, bitcoinmat nebyl použit, platební karta ve 3 (30 %) případech, kryptoměna v 1 (10 %) případu.
Inzertní podvod – bankovní účet byl použit v 10 (100 %) případech, ostatní možnosti nebyly využity.

Investiční podvod – bankovní účet byl použit v 9 (90 %) případech, služby převodu peněz ve 4 (40 %) případech, kryptoměna v 7 (70 %) případech, ostatní možnosti nebyly využity.

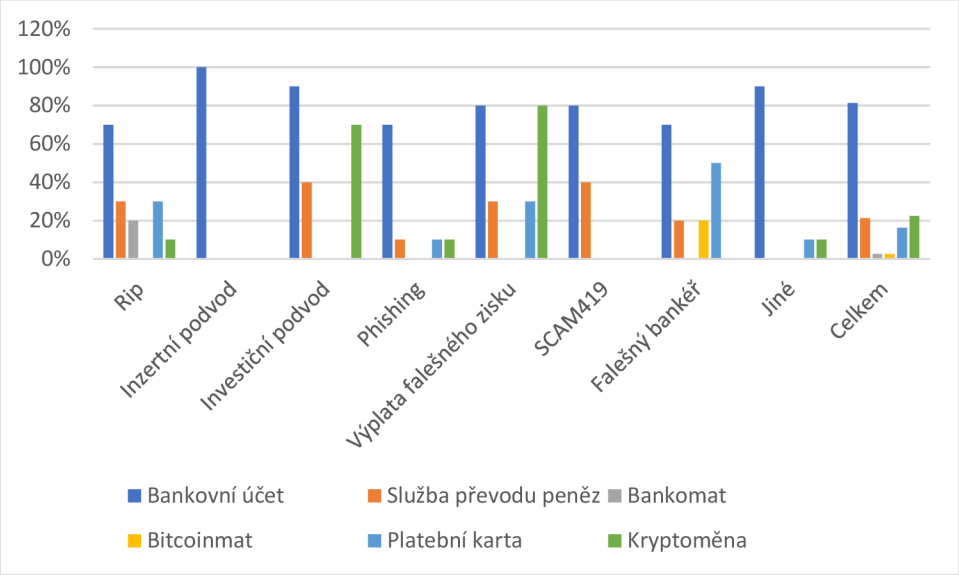
Phishing – bankovní účet byl použit v 7 (70 %) případech, služby převodu peněz v 1 (10 %) případu, platební karta v 1 (10 %) případu, kryptoměna v 1 (10 %) případu, ostatní možnosti nebyly využity.

Výplata falešného zisku – bankovní účet byl použit v 8 (80 %) případech, služby převodu peněz ve 3 (30 %) případech, platební karta ve 3 (30 %) případech, kryptoměna v 8 (80 %) případech, ostatní možnosti nebyly využity.

SCAM419 – bankovní účet byl použit v 8 (80 %) případech, služby převodu peněz ve 4 (40 %) případech, ostatní možnosti nebyly využity.

Falešný bankéř – bankovní účet byl použit v 7 (70 %) případech, služby převodu peněz ve 2 (20 %) případech, bitcoinmat ve 2 (20 %) případech, platební karta v 5 (50 %) případech, ostatní možnosti nebyly využity.

Jiné – Bankovní účet byl použit v 9 (90 %) případech, platební karta v 1 (10 %) případu, kryptoměna v 1 (10 %) případu, ostatní možnosti nebyly využity.



Graf 7: Způsob platby nebo převodu peněz.

Zdroj: Vlastní zpracování

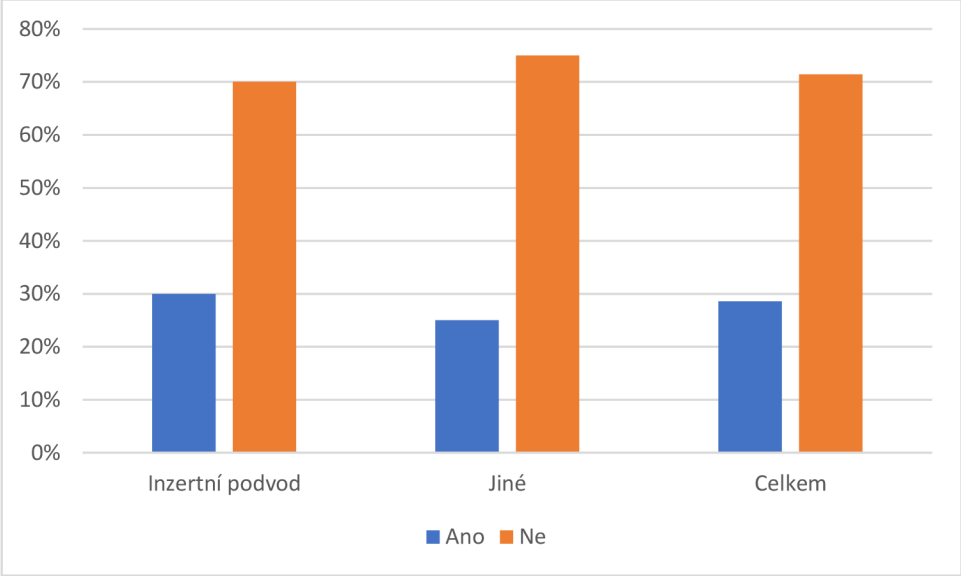
Otázka č. 9 byla zaměřena na zjištění, jaký byl vztah oběti a pachatele.

Výzkumný soubor obsahoval 80 případů. Ve všech případech 80 (100 %) případech se jednalo o cizí osobu. Grafické znázornění nebylo použito.

Otázka č. 10 byla zaměřena na zjištění, jaký počet případů byl spáchán ve spolupachatelství.

Z výzkumného souboru o 80 případech se jednalo o 14 objasněných případů, a to u způsobu jednání: inzertní podvod a jiné. Celkem 4 (29 %) případy byly spáchány ve spolupachatelství a 10 (71 %) případů bylo spácháno jedním pachatelem.

U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – pachatelé nebyli zjištěni.
Inzertní podvod – celkem z 10 případů byly 3 (30 %) spáchány ve spolupachatelství a 7 (70 %) případů bylo spácháno jedním pachatelem.
Jiné – celkem ze 4 případů byl 1 (25 %) spáchán ve spolupachatelství a 3 (75 %) případy byly spáchány jedním pachatelem.



Graf 8: Spolupachatelství.

Zdroj: Vlastní zpracování

3.6.1.2 Kriminální situace

Otázka č. 11 byla zaměřena na zjištění, jaký počet případů má zahraniční přesah.

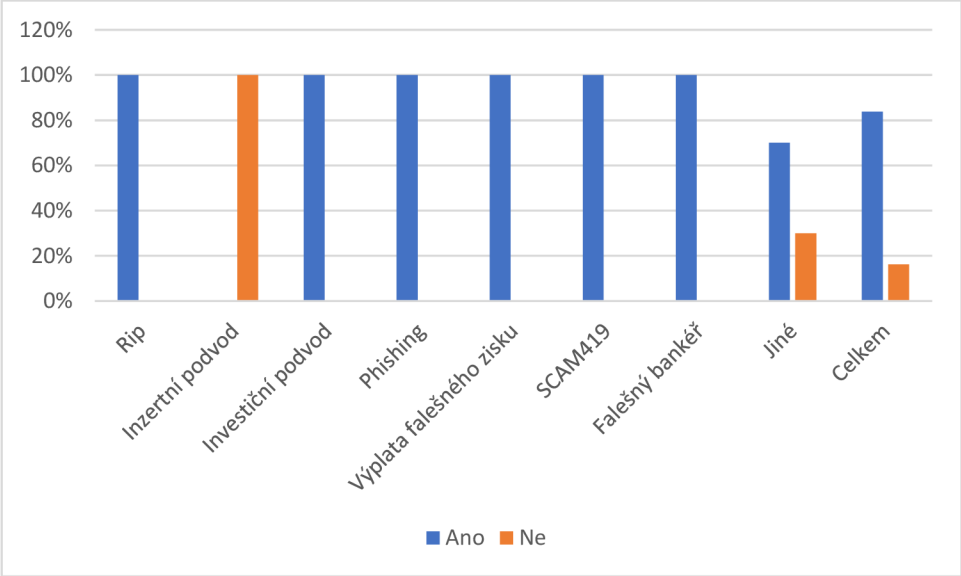
Výzkumný soubor obsahoval 80 případů. Celkem v 67 (84 %) případech byl zjištěn zahraniční přesah a ve 13 (16 %) případech nebyl.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – ve všech případech (100 %) byl zjištěn zahraniční přesah.

Inzertní podvod – ve všech 10 (100 %) případech nebyl zjištěn zahraniční přesah.

Jiné – v 7 (70 %) případech byl zjištěn zahraniční přesah a ve 3 (30 %) případech nebyl.



Graf 9: Zahraniční přesah.

Zdroj: Vlastní zpracování

Otázka č. 12 byla zaměřena na zjištění, jaká je objasněnost u všech ukončených případů.

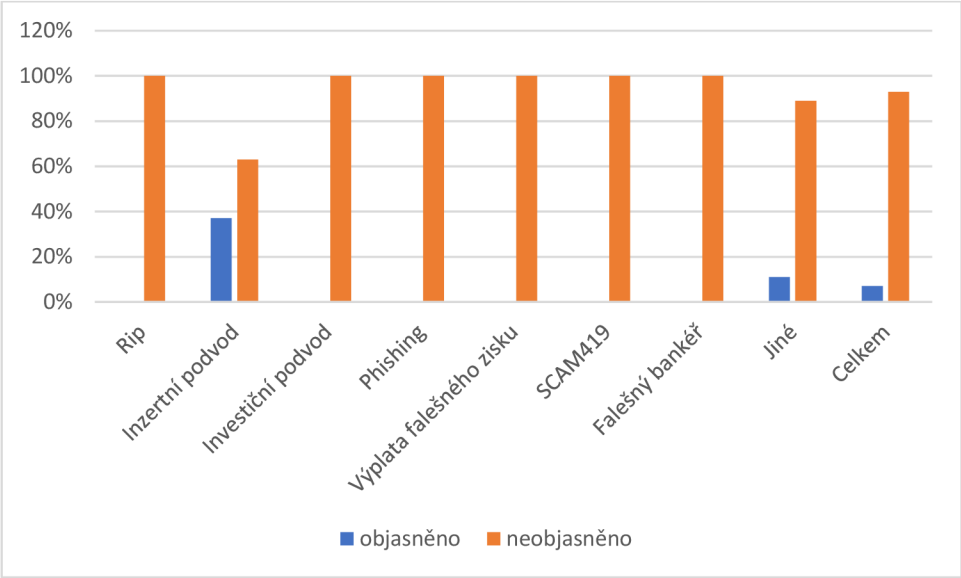
Výzkumný soubor obsahoval 340 ukončených případů. Celkem 24 (7 %) případů bylo objasněno, a to u způsobu jednání: inzertní podvod, jiné. Celkem 316 (93 %) případů nebylo objasněno.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – z celkového počtu 248 případů nebylo objasněno 248 (100 %) případů.

Inzertní podvod – z celkového počtu 54 případů bylo 20 (37 %) případů objasněno a 34 (63 %) nebylo objasněno.

Jiné – z celkového počtu 38 případů byly 4 (11 %) případy objasněny a 34 (89 %) nebylo objasněno.



Graf 10: Objasněnost.

Zdroj: Vlastní zpracování

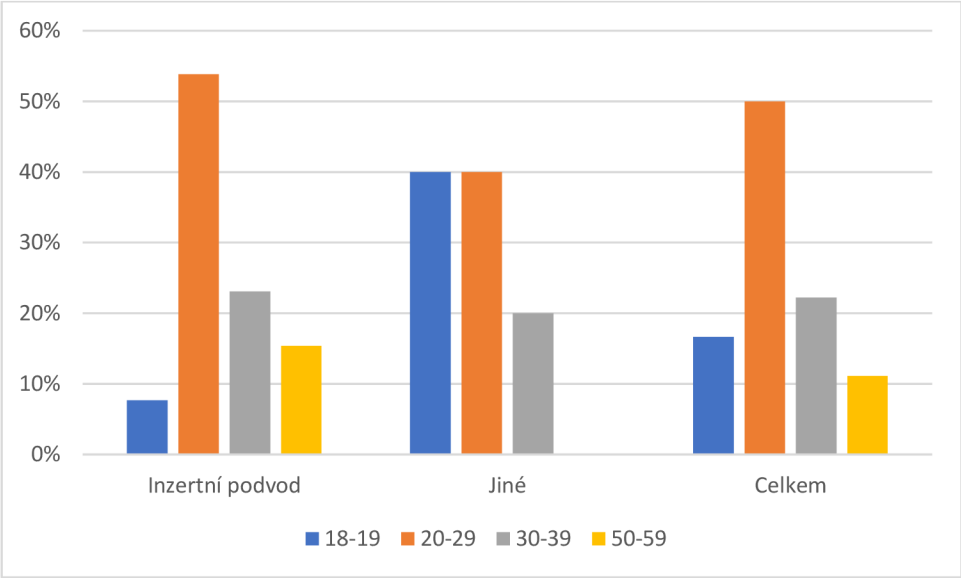
3.6.1.3 Osobnostní rysy pachatele trestného činu

Otázka č. 13 byla zaměřena na zjištění, jaký je věk pachatele.

Z výzkumného souboru o 80 případech se jednalo o 14 objasněných případů a celkem 18 pachatelů. 3 (17 %) pachatelé byli ve věku 18-19 let, 9 (50 %) pachatelů bylo ve věku 20-29 let, 4 (22 %) pachatelé měli 30-39 let a 2 (11 %) pachatelé měli 50-59 let.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – pachatelé nebyli zjištěni.
Inzertní podvod – celkem z 13 pachatelů byl 1 (8 %) pachatel ve věku 18-19 let, 7 (54 %) pachatelů bylo ve věku 20-29 let, 3 (23 %) pachatelé byli ve věku 30-39 let a 2 (15 %) pachatelé byli ve věku 50-59 let.
Jiné – celkem z 5 pachatelů měli 2 (40 %) pachatelé 18-19 let, 2 (40 %) pachatelé měli 20-29 let a 1 (20 %) pachatel měl 30-39 let.



Graf 11: Věk pachatele.

Zdroj: Vlastní zpracování

Otázka č. 14 byla zaměřena na zjištění, jaké je pohlaví pachatele.

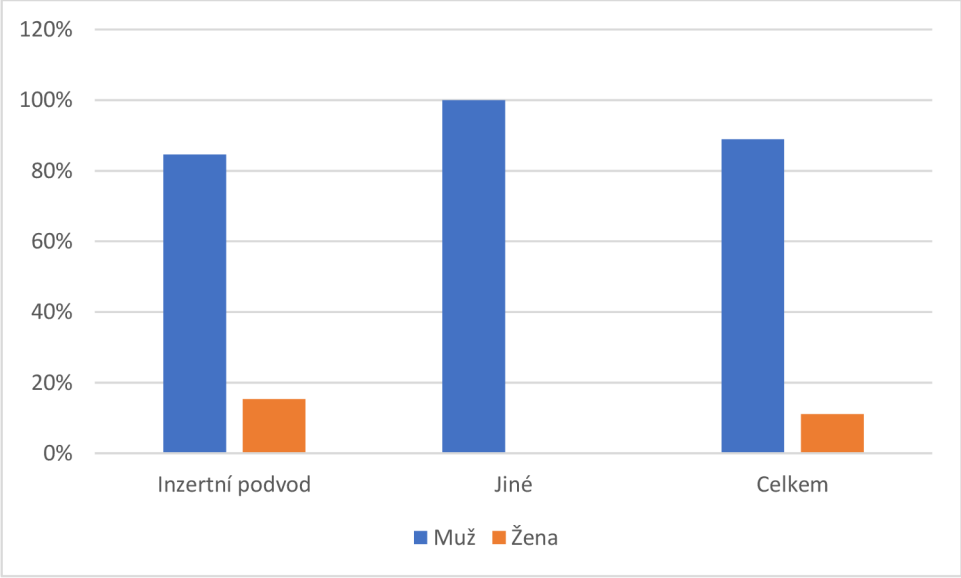
Z výzkumného souboru o 80 případech se jednalo o 14 objasněných případů a celkem 18 pachatelů. 16 (89 %) pachatelů byli muži a 2 (11 %) pachatelé byly ženy.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – pachatelé nebyli zjištěni.

Inzertní podvod – celkem ze 13 pachatelů bylo 11 (85 %) mužů a 2 (15 %) ženy.

Jiné – celkem z 5 pachatelů bylo 5 (100 %) mužů.



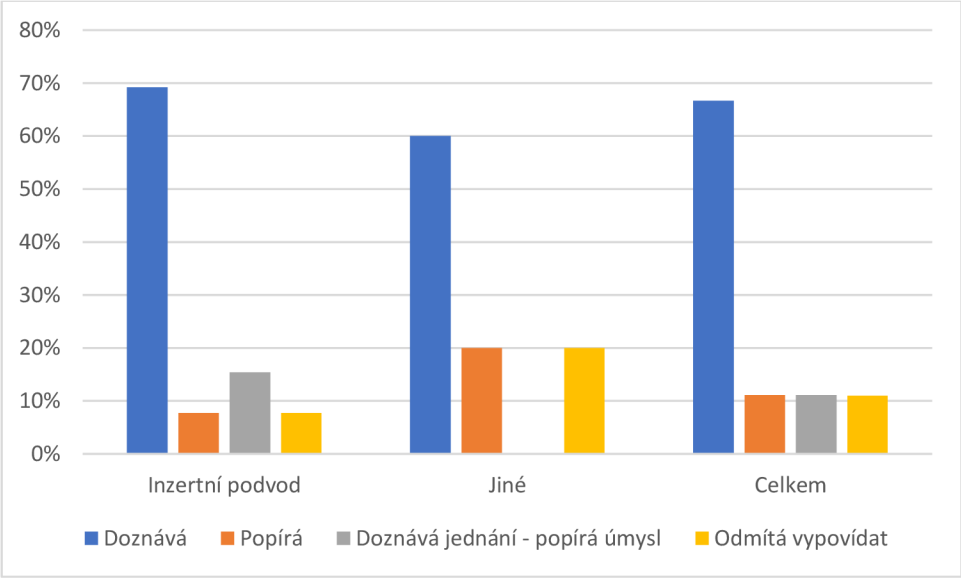
Graf 12: Pohlaví pachatele.

Zdroj: Vlastní zpracování

Otázka č. 15 byla zaměřena na zjištění, jaká je typická obhajoba pachatele.

Z výzkumného souboru o 80 případech se jednalo o 14 objasněných případů a celkem 18 pachatelů. 12 (67 %) pachatelů doznává trestnou činnost, 2 (11 %) pachatelé popírají trestnou činnost, 2 (11 %) pachatelé doznávají jednání, ale popírají úmysl a 2 (11 %) pachatelé odmítají vypovídat.

U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – pachatelé nebyli zjištěni.
Inzertní podvod – celkem ze 13 pachatelů jich 9 (69 %) doznává trestnou činnost, 1 (8 %) pachatel popírá trestnou činnost, 2 (15 %) pachatelé doznávají jednání, ale popírají úmysl a 1 (8 %) pachatel odmítá vypovídat.
Jiné – celkem z 5 pachatelů jich 3 (60 %) doznávají trestnou činnost, 1 (20 %) pachatel popírá trestnou činnost a 1 (20 %) pachatel odmítá vypovídat.



Graf 13: Obhajoba pachatele.

Zdroj: Vlastní zpracování

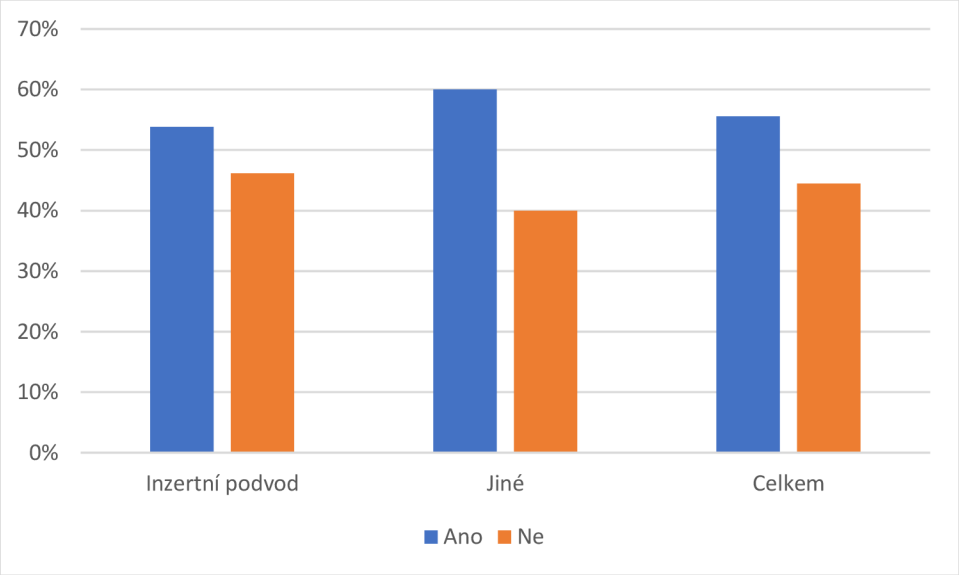
Otázka č. 16 byla zaměřena na zjištění, jak často ovlivňoval pachatel svědky.

Výzkumný soubor obsahoval 80 případů. V 80 (100 %) případech bylo zjištěno, že pachatel svědky neovlivňoval. Grafické znázornění nebylo použito.

Otázka č. 17 byla zaměřena na zjištění, jestli měl pachatel předchozí kriminální zkušenost.

Z výzkumného souboru o 80 případech se jednalo o 14 objasněných případů a celkem 18 pachatelů. 10 (56 %) pachatelů mělo předchozí kriminální zkušenost a 8 (44 %) pachatelů ji nemělo.

U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – pachatelé nebyli zjištěni.
Inzertní podvod – celkem ze 13 pachatelů jich 7 (54 %) mělo předchozí kriminální zkušenost a 6 (46 %) pachatelů ji nemělo.
Jiné – celkem z 5 pachatelů jich 3 (60 %) měli předchozí kriminální zkušenost a 2 (40 %) pachatelé ji neměli.



Graf 14: Kriminální zkušenost pachatele.

Zdroj: Vlastní zpracování

Otázka č. 18 byla zaměřena na zjištění, jestli byl pachatel v minulosti odsouzen za trestný čin podvod.

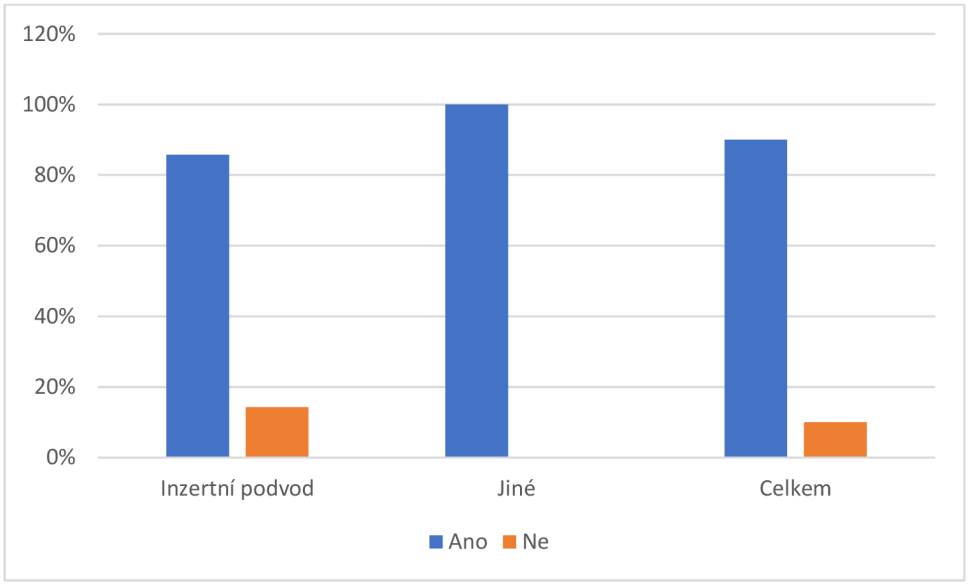
Z výzkumného souboru o 80 případech se jednalo o 14 objasněných případů a celkem 18 pachatelů. 10 pachatelů mělo předchozí kriminální zkušenost. 9 (90 %) pachatelů bylo odsouzeno za trestný čin podvod a 1 (10 %) pachatel byl odsouzen za jiný trestný čin.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – pachatelé nebyli zjištěni.

Inzertní podvod – celkem ze 7 pachatelů jich 6 (86 %) bylo odsouzeno za trestný čin podvod a 1 (14 %) pachatel byl odsouzen za jiný trestný čin.

Jiné – celkem ze 3 pachatelů byli 3 (100 %) odsouzeni za trestný čin podvod.



Graf 15: Předchozí odsouzení za podvod.

Zdroj: Vlastní zpracování

Otázka č. 19 byla zaměřena na zjištění, jaké měl pachatel vzdělání.

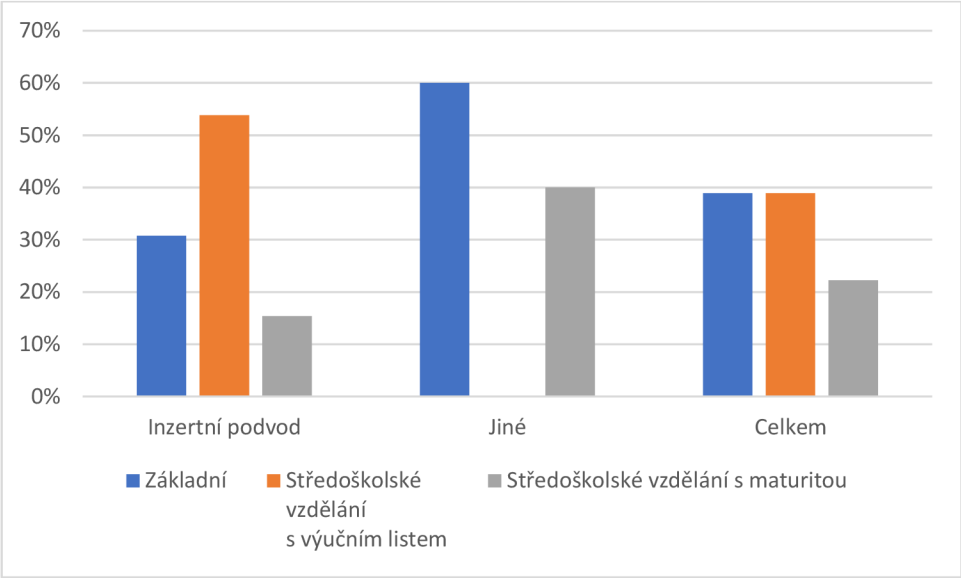
Z výzkumného souboru o 80 případech se jednalo o 14 objasněných případů a celkem 18 pachatelů. Celkem 7 (39 %) pachatelů mělo základní vzdělání, 7 (39 %) pachatelů mělo středoškolské vzdělání s výučním listem a 4 (22 %) pachatelé měli středoškolské vzdělání s maturitou.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – pachatelé nebyli zjištěni.

Inzertní podvod – celkem ze 13 pachatelů mělo 4 (31 %) základní vzdělání, 7 (54 %) pachatelů mělo středoškolské vzdělání s výučním listem a 2 (15 %) pachatelé měli středoškolské vzdělání s maturitou.

Jiné – celkem z 5 pachatelů měli 3 (60 %) základní vzdělání a 2 (40 %) pachatelé měli středoškolské vzdělání s maturitou.



Graf 16: Vzdělání pachatele.

Zdroj: Vlastní zpracování

Otázka č. 20 byla zaměřena na zjištění, jaké měl pachatel zaměstnání.

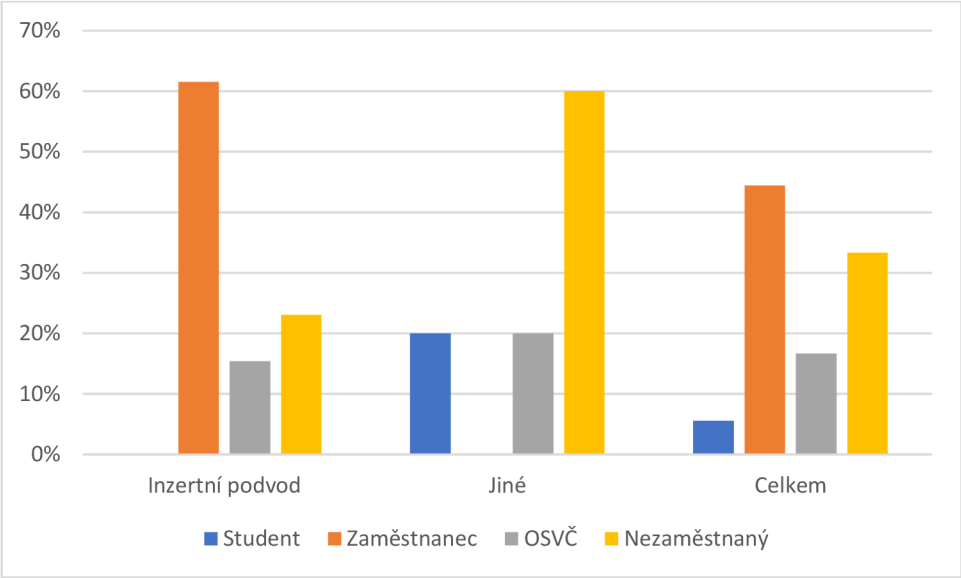
Z výzkumného souboru o 80 případech se jednalo o 14 objasněných případů a celkem 18 pachatelů. 1 (6 %) pachatel byl student, 8 (44 %) pachatelů bylo v zaměstnaneckém poměru, 3 (17 %) pachatelé pracovali jako OSVČ a 6 (33 %) pachatelů bylo nezaměstnaných.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – pachatelé nebyli zjištěni.

Inzertní podvod – celkem ze 13 pachatelů bylo 8 (62 %) v zaměstnaneckém poměru, 2 (15 %) pachatelé pracovali jako OSVČ a 3 (23 %) pachatelé byli nezaměstnaní.

Jiné – celkem z 5 pachatelů byl 1 (20 %) student, 1 (20 %) pachatel pracovali jako OSVČ a 3 (60 %) pachatelé byli nezaměstnaní.



Graf 17: Zaměstnání pachatele.

Zdroj: Vlastní zpracování

3.6.1.4 Osobnostní rysy oběti trestného činu

Otázka č. 21 byla zaměřena na zjištění, jestli je poškozeným fyzická nebo právnická osoba.

Výzkumný soubor obsahoval 80 případů. V těchto případech bylo zjištěno celkem 238 poškozených a z toho bylo 232 (97 %) fyzických osob a 6 (3 %) právnických osob.

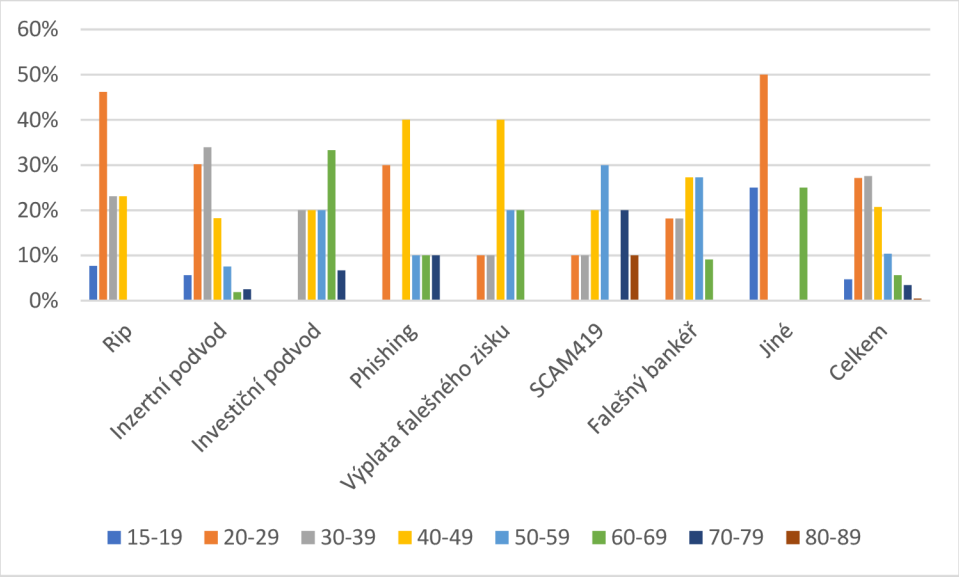
U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod, inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – 228 poškozených a z toho bylo 228 (100 %) fyzických osob.
Jiné – 10 poškozených a z toho bylo 4 (40 %) fyzických osob a 6 (60 %) právnických osob.
Grafické znázornění nebylo použito.

Otázka č. 22 byla zaměřena na zjištění, jaký je věk oběti.

Výzkumný soubor obsahoval 80 případů. V těchto případech bylo zjištěno celkem 232 poškozených fyzických osob (obětí) a z toho ve věkovém rozmezí 15-19 let 11(5%) obětí, 20-29 let - 63 (27 %) obětí, 30-39 let - 64 (28 %) obětí, 40-49 let - 48 (21 %) obětí, 50-59 let - 24 (10 %) obětí, 60-69 let - 13 (6 %) obětí, 70-79 let - 8 (3 %) obětí, 80-89 let - 1 (0,4 %) oběť.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – celkem 13 obětí a z toho ve věkovém rozmezí 15-19 let - 1 (8 %) oběť, 20-29 let celkem 6 (46 %) obětí, 30-39 let celkem 3 (23 %) oběti, 40-49 let celkem 3 (23 %) oběti. **Inzertní podvod** – celkem 159 obětí a z toho ve věkovém rozmezí 15-19 let - 9 (6 %) obětí, 20-29 let - 48 (30 %) obětí, 30-39 let - 54 (34 %) obětí, 40-49 let - 29 (18 %) obětí, 50-59 let - 12 (8 %) obětí, 60-69 let - 3 (2 %) oběti, 70-79 let - 4 (3 %) oběti. **Investiční podvod** – celkem 15 obětí a z toho ve věkovém rozmezí 30-39 let - 3 (20 %) oběti, 40-49 let - 3 (20 %) oběti, 50-59 let - 3 (20 %) oběti, 60-69 let - 5 (33 %) obětí, 70-79 let - 1 (7 %) oběť. **Phishing** – celkem 10 obětí a z toho ve věkovém rozmezí 20-29 let - 3 (30 %) oběti, 40-49 let - 4 (40 %) oběti, 50-59 let – 1 (10 %) oběť, 60-69 let - 1 (10 %) oběť, 70-79 let - 1 (10 %) oběť. **Výplata falešného zisku** – celkem 10 obětí a z toho ve věkovém rozmezí 20-29 let - 1 (10 %) oběť, 30-39 let – 1 (10 %) oběť, 40-49 let - 4 (40 %) oběti, 50-59 let - 2 (20 %) oběti, 60-69 let - 2 (20 %) oběti. **SCAM419** – celkem 10 obětí a z toho ve věkovém rozmezí 20-29 let - 1 (10 %) oběť, 30-39 let - 1 (10 %) oběť, 40-49 let -2 (20 %) oběti, 50-59 let - 3 (30 %) oběti, 70-79 let - 2 (20 %) oběti, 80-89 let - 1 (10 %) oběť. **Falešný bankéř** – celkem 11 obětí a z toho ve věkovém rozmezí 20-29 let - 2 (18 %) oběti, 30-39 let - 2 (18 %) oběti, 40-49 let - 3 (27 %) oběti, 50-59 let - 3 (27 %) oběti, 60-69 let - 1 (9 %) oběť. **Jiné** – celkem 4 oběti a z toho ve věkovém rozmezí 15-19 let - 1 (25 %) oběť, 20-29 let - 2 (50 %) oběti, 60-69 let - 1 (25 %) oběť.



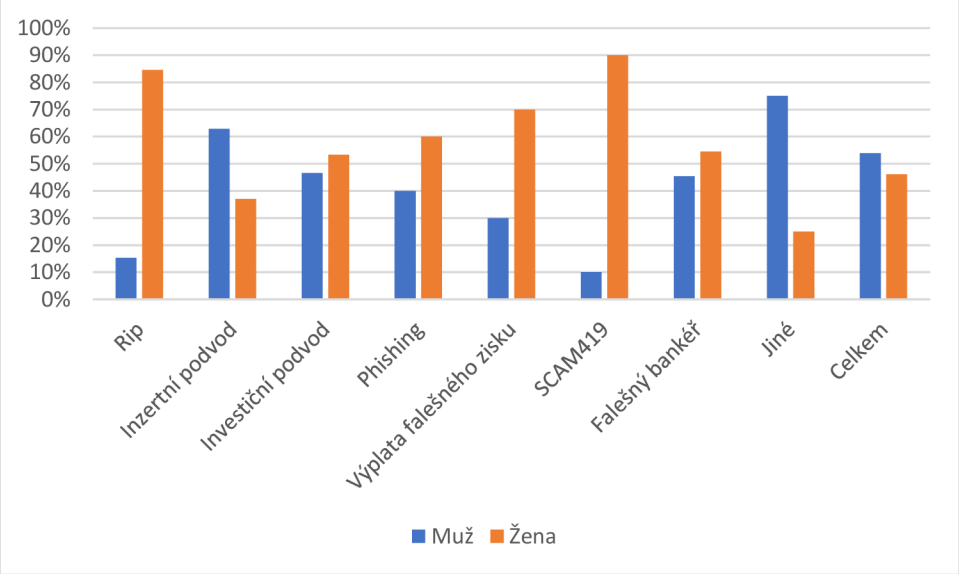
Graf 18: Věk oběti.

Zdroj: Vlastní zpracování

Otázka č. 23 byla zaměřena na zjištění, jaké je pohlaví oběti.

Výzkumný soubor obsahoval 80 případů. V těchto případech bylo zjištěno celkem 232 poškozených fyzických osob – obětí a z toho bylo celkem 125 (54 %) mužů a 107 (46 %) žen.

U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod – celkem 13 obětí a z toho 2 (15 %) muži a 11 (85 %) žen.
Inzertní podvod – celkem 159 obětí a z toho 100 (63 %) mužů a 59 (37 %) žen.
Investiční podvod – celkem 15 obětí a z toho 7 (47 %) mužů a 8 (53 %) žen.
Phishing – celkem 10 obětí a z toho 4 (40 %) muži a 6 (60 %) žen.
Výplata falešného zisku – celkem 10 obětí a z toho 3 (30 %) muži a 7 (70 %) žen.
SCAM419 – celkem 10 obětí a z toho 1 (10 %) muž a 9 (90 %) žen.
Falešný bankéř – celkem 11 obětí a z toho 5 (45 %) mužů a 6 (55 %) žen.
Jiné – celkem 4 oběti a z toho 3 (75 %) muži a 1 (25 %) žena.



Graf 19: Pohlaví oběti.

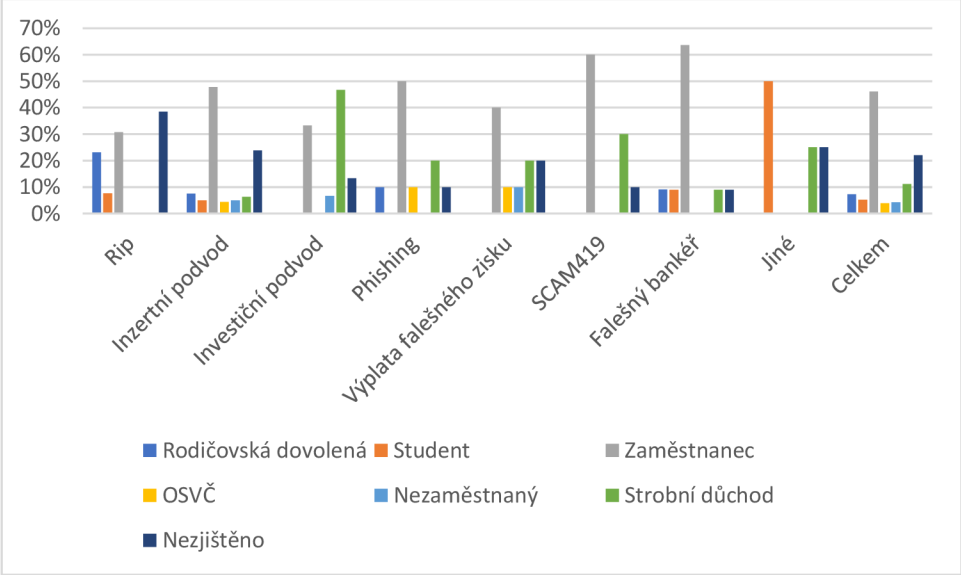
Zdroj: Vlastní zpracování

Otázka č. 24 byla zaměřena na zjištění, jaké měla oběť zaměstnání.

Výzkumný soubor obsahoval 80 případů. V těchto případech bylo zjištěno celkem 232 poškozených fyzických osob – obětí a z toho bylo 17 (7 %) na rodičovské dovolené, 12 (5 %) studentů, 107 (46 %) zaměstnanců, 9 (4 %) OSVČ, 10 (4 %) nezaměstnaných, 26 (11 %) starobních důchodců a u 51 (22 %) obětí nebylo zaměstnání zjištěno.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – celkem 13 obětí a z toho byli 3 (23 %) na rodičovské dovolené, 1 (8 %) student, 4 (31 %) zaměstnanci a u 5 (38 %) obětí nebylo zaměstnání zjištěno. **Inzertní podvod** – celkem 159 obětí a z toho bylo 12 (8 %) na rodičovské dovolené, 8 (5 %) studentů, 76 (48 %) zaměstnanců, 7 (4 %) OSVČ, 8 (5 %) nezaměstnaných, 10 (6 %) starobních důchodců a u 38 (24 %) obětí nebylo zaměstnání zjištěno. **Investiční podvod** – celkem 15 obětí a z toho bylo 5 (33 %) zaměstnanců, 1 (7 %) nezaměstnaných, 7 (47 %) starobních důchodců a u 2 (13 %) obětí nebylo zaměstnání zjištěno. **Phishing** – celkem 10 obětí a z toho bylo 1 (10 %) na rodičovské dovolené, 5 (50 %) zaměstnanců, 1 (10 %) OSVČ, 2 (20 %) starobní důchodci a u 1 (10 %) oběti nebylo zaměstnání zjištěno. **Výplata falešného zisku** – celkem 10 obětí a z toho byli 4 (40 %) zaměstnanci, 1 (10 %) OSVČ, 1 (10 %) nezaměstnaný, 2 (20 %) starobní důchodci a u 2 (20 %) obětí nebylo zaměstnání zjištěno. **SCAM419** – celkem 10 obětí a z toho bylo 6 (60 %) zaměstnanců, 3 (30 %) starobní důchodci a u 1 (10 %) oběti nebylo zaměstnání zjištěno. **Falešný bankéř** – celkem 11 obětí a z toho byl 1 (9 %) na rodičovské dovolené, 1 (9 %) student, 7 (64 %) zaměstnanců, 1 (9 %) starobní důchodce a u 1 (9 %) oběti nebylo zaměstnání zjištěno. **Jiné** – celkem 4 oběti a z toho byli 2 (50 %) studenti, 1 (25 %) starobní důchodce a u 1 (25 %) oběti nebylo zaměstnání zjištěno.



Graf 20: Zaměstnání oběti.

Zdroj: Vlastní zpracování

3.6.1.5 Motiv činu

Otázka č. 25 byla zaměřena na zjištění, jaký byl motiv činu.

Výzkumný soubor obsahoval 80 případů. V těchto případech bylo zjištěno celkem 238 poškozených (fyzické i právnické osoby) a ve všech šlo o zištný motiv (100 %). Grafické znázornění nebylo použito.

3.6.2 Výsledky k dílčímu cíli č. 1

Dílčím cílem č. 1 bylo zjistit, jaké jsou typické stopy a jiné soudní důkazy.

Otázka č. 26 byla zaměřena na zjištění, jaké kriminalistické stopy a jiné soudní důkazy byly zajišťovány.

Výzkumný soubor obsahoval 80 případů. Celkem v 80 (100 %) případech byly zajištěny paměťové stopy, v 69 (86 %) případech digitální stopy, v 55 (69 %) případech byly zajištěny písemnosti, v 72 (90 %) případech bankovní informace, v 41 (51 %) případech telekomunikační provoz podle § 88a trestního řádu, ve 20 (25 %) případech informace SIM/IMEI a ve 2 (3 %) případech věcné důkazy.

U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod – z celkem 10 případů byly paměťové stopy zajištěny v 10 (100 %) případech, digitální stopy v 6 (60 %) případech, písemnosti v 7 (70 %) případech, bankovní informace v 10 (100 %) případech, telekomunikační provoz podle § 88a trestního řádu v 8 (80 %) případech, informace SIM/IMEI nebyly zjišťovány.
Inzertní podvod – z celkem 10 případů byly paměťové stopy zajištěny v 10 (100 %) případech, digitální stopy v 7 (70 %) případech, písemnosti v 9 (90 %) případech, bankovní informace v 10 (100 %) případech, telekomunikační provoz podle § 88a trestního řádu ve 4 (40 %) případech, informace SIM/IMEI v 8 (80 %) případech a ve 2 (3 %) případech věcné důkazy.
Investiční podvod – z celkem 10 případů byly paměťové stopy zajištěny v 10 (100 %) případech, digitální stopy v 10 (100 %) případech, písemnosti v 10 (100 %) případů, bankovní informace v 10 (100 %) případech, telekomunikační provoz podle § 88a trestního řádu v 6 (60 %) případech, informace SIM/IMEI ve 2 (20 %) případech.
Phishing – z celkem 10 případů byly paměťové stopy zajištěny v 10 (100 %) případech, digitální stopy v 8 (80 %) případech, písemnosti ve 4 (40 %) případech,

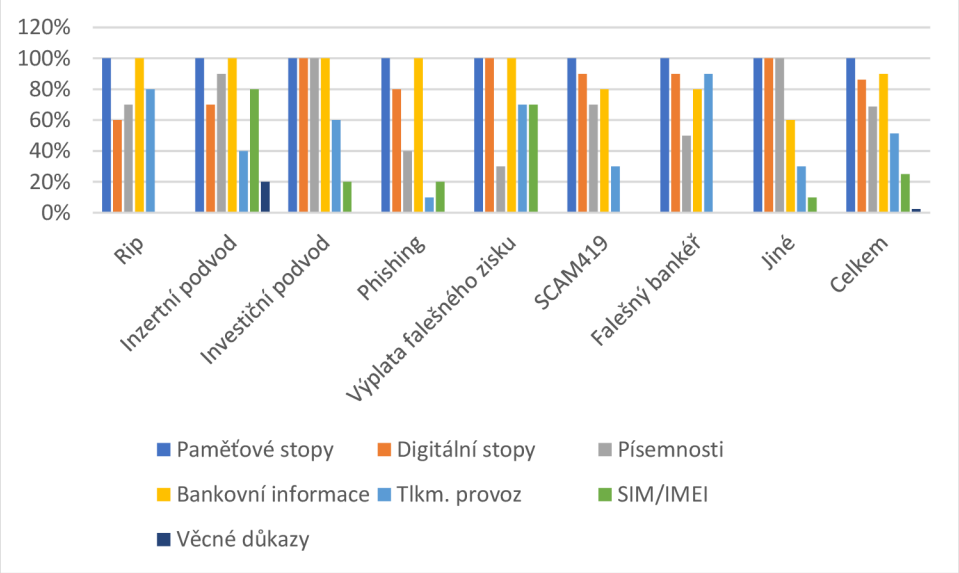
bankovní informace v 10 (100 %) případech, telekomunikační provoz podle § 88a trestního řádu v 1 (10 %) případech, informace SIM/IMEI ve 2 (20 %) případech.

Výplata falešného zisku – z celkem 10 případů byly paměťové stopy zajištěny v 10 (100 %) případech, digitální stopy v 10 (100 %) případech, písemnosti ve 3 (30 %) případech, bankovní informace v 10 (100 %) případech, telekomunikační provoz podle § 88a trestního řádu v 7 (70 %) případech, informace SIM/IMEI v 7 (70 %) případech.

SCAM419 – z celkem 10 případů byly paměťové stopy zajištěny v 10 (100 %) případech, digitální stopy v 9 (90 %) případech, písemnosti v 7 (70 %) případech, bankovní informace v 8 (80 %) případech, telekomunikační provoz podle § 88a trestního řádu ve 3 (30 %) případech, informace SIM/IMEI nebyly zjišťovány.

Falešný bankéř – z celkem 10 případů byly paměťové stopy zajištěny v 10 (100 %) případech, digitální stopy v 9 (90 %) případech, písemnosti v 5 (50 %) případech, bankovní informace v 8 (80 %) případech, telekomunikační provoz podle § 88a trestního řádu v 9 (90 %) případech, informace SIM/IMEI nebyly zjišťovány.

Jiné – z celkem 10 případů byly paměťové stopy zajištěny v 10 (100 %) případech, digitální stopy v 10 (100 %) případech, písemnosti v 10 (100 %) případech, bankovní informace v 6 (60 %) případech, telekomunikační provoz podle § 88a trestního řádu ve 3 (30 %) případech, informace SIM/IMEI v 1 (70 %) případě.



Graf 21: Kriminalistické stopy a jiné soudní důkazy.

Zdroj: Vlastní zpracování

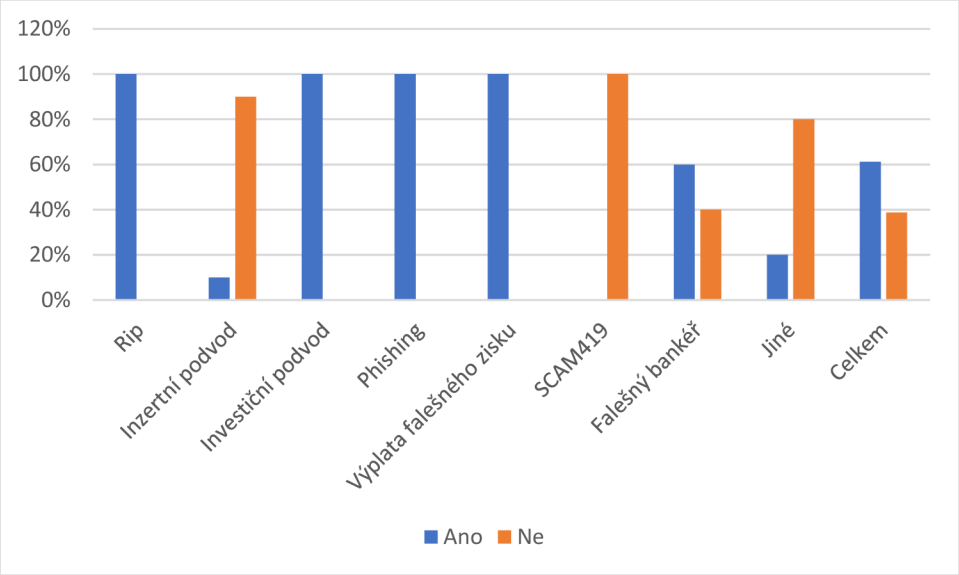
3.6.3 Výsledky k dílčímu cíli č. 2

Dílčím cílem č. 2 bylo zjistit, jaké jsou zvláštnosti předmětu vyšetřování u internetových podvodů.

Otázka č. 27 byla zaměřena na zjištění, jestli byl podvod kvalifikován v souběhu s jiným trestným činem.

Výzkumný soubor obsahoval 80 případů. Celkem v 49 (61 %) případech se jednalo o souběh podvodu s jiným trestným činem a v 31 (39 %) případech nebyl souběh kvalifikován.

U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku – ve všech případech (100 %) se jednalo o souběh podvodu s jiným trestným činem.
Inzertní podvod – v 1 (10 %) případu se jednalo o souběh podvodu s jiným trestným činem a v 9 (90 %) případech nebyl souběh kvalifikován.
SCAM419 – ve všech 10 (100 %) případech se nejednalo o souběh podvodu s jiným trestným činem.
Falešný bankéř – v 6 (60 %) případech se jednalo o souběh podvodu s jiným trestným činem a ve 4 (40 %) případech nebyl souběh kvalifikován.
Jiné – ve 2 (20 %) případech se jednalo o souběh podvodu s jiným trestným činem a v 8 (80 %) případech nebyl souběh kvalifikován.



Graf 22: Souběh trestných činů.

Zdroj: Vlastní zpracování

Otázka č. 28 byla zaměřena na zjištění, jaké jiné trestné činy byly kvalifikovány společně s podvodem.

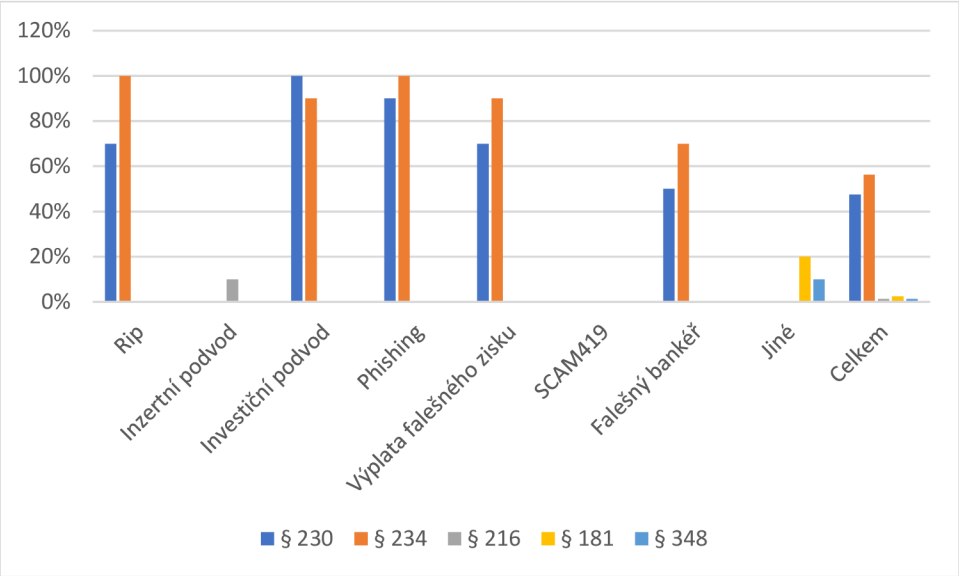
Výzkumný soubor obsahoval 80 případů. V jednotlivých případech mohlo dojít k několika různým právním kvalifikacím. Tato informace má na procentuální vyjádření ten význam, že součet procent u jednotlivých způsobů jednání pachatele a způsobů kvalifikací není roven 100 %.

Společně s trestným činem podvod bylo kvalifikováno 38 (48 %) případů trestného činu neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací podle § 230 trestního zákoníku, 45 (56 %) případů trestného činu neoprávněné opatření, padělání a pozměnění platebního prostředku podle § 234 trestního zákoníku, 1 (1 %) případ trestného činu legalizace výnosů z trestné činnosti podle § 216 trestního zákoníku, 2 (3 %) případy trestného činu poškození cizích práv podle § 181 trestního zákoníku a 1 (1 %) případ trestného činu padělání a pozměnění veřejné listiny podle § 348 trestního zákoníku. Dále budou používána pouze čísla §§.

U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod – společně s trestným činem podvod bylo kvalifikováno 7 (70 %) případů podle § 230 trestního zákoníku, 10 (100 %) případů podle § 234 trestního zákoníku. Další souběhy nebyly kvalifikovány.
Inzertní podvod – společně s trestným činem podvod byl kvalifikován 1 (1 %) případ podle § 216 trestního zákoníku. Další souběhy nebyly kvalifikovány.
Investiční podvod – společně s trestným činem podvod bylo kvalifikováno 10 (100 %) případů podle § 230 trestního zákoníku, 9 (90 %) případů podle § 234 trestního zákoníku. Další souběhy nebyly kvalifikovány.
Phishing – společně s trestným činem podvod bylo kvalifikováno 9 (90 %) případů podle § 230 trestního zákoníku, 10 (100 %) případů podle § 234 trestního zákoníku. Další souběhy nebyly kvalifikovány.
Výplata falešného zisku – společně s trestným činem podvod bylo kvalifikováno 7 (70 %) případů podle § 230 trestního zákoníku, 9 (90 %) případů podle § 234 trestního zákoníku. Další souběhy nebyly kvalifikovány.
SCAM419 – nebyly kvalifikovány žádné souběhy.

Falešný bankéř – společně s trestným činem podvod bylo kvalifikováno 5 (50 %) případů podle § 230 trestního zákoníku, 7 (70 %) případů podle § 234 trestního zákoníku. Další souběhy nebyly kvalifikovány.

Jiné – společně s trestným činem podvod byly kvalifikovány 2 (20 %) případy podle § 181 trestního zákoníku a 1 (10 %) případ podle § 348 trestního zákoníku.



Graf 23: Trestné činy v souběhu.

Zdroj: Vlastní zpracování

Otázka č. 29 byla zaměřena na zjištění, v kolika případech je případ dílčím skutkem pokračujícího trestného činu podvod.

Výzkumný soubor obsahoval 80 případů. Celkem v 19 (24 %) případech je případ dílčím skutkem pokračujícího trestného činu podvod a v 61 (76 %) případech není.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – ve 3 (30 %) případech se jedná o dílčí skutek a v 7 (70 %) případech není.

Inzertní podvod – v 8 (80 %) případech se jedná o dílčí skutek a ve 2 (20 %) případech není.

Investiční podvod – ve 4 (40 %) případech se jedná o dílčí skutek a v 6 (60 %) případech není.

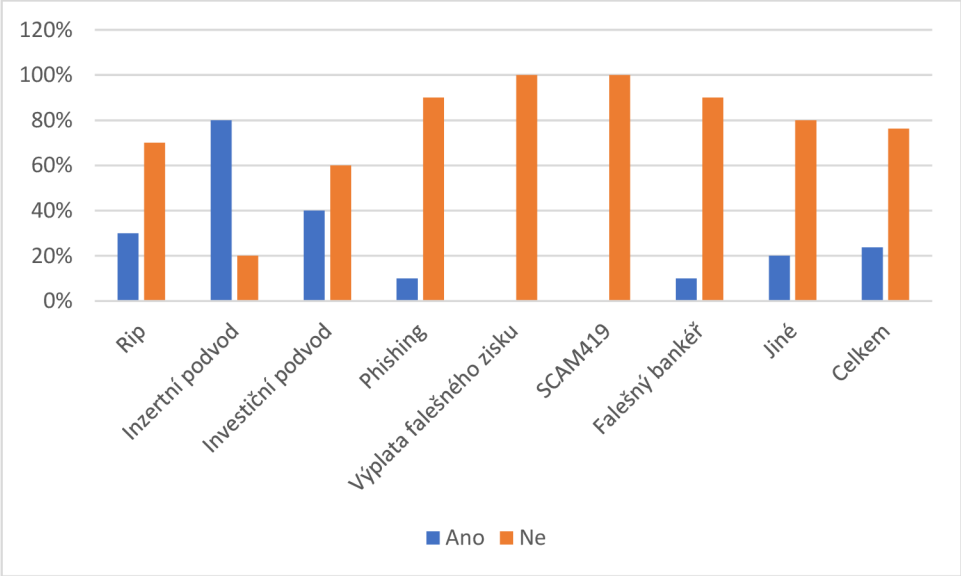
Phishing – v 1 (10 %) případu se jedná o dílčí skutek a v 9 (90 %) případech není.

Výplata falešného zisku – všech 10 (100 %) případů není dílčím skutkem pokračujícího trestného činu podvod.

SCAM419 – všech 10 (100 %) případů není dílčím skutkem pokračujícího trestného činu podvod.

Falešný bankéř – v 1 (10 %) případu se jedná o dílčí skutek a v 9 (90 %) případech není.

Jiné – ve 2 (20 %) případech se jedná o dílčí skutek a v 8 (80 %) případech tomu tak není.



Graf 24: Dílčí skutek podvodu.

Zdroj: Vlastní zpracování

3.6.4 Výsledky k dílčímu cíli č. 3

Dílčím cílem číslo 3 bylo zjistit, jaké jsou typické podněty a jejich zvláštnosti u internetových podvodů.

Otázka č. 30 byla zaměřena na zjištění, za jak dlouho po činu oznámil poškozený skutek na policii.

Výzkumný soubor obsahoval 80 případů. V těchto případech bylo zjištěno celkem 238 poškozených (fyzické i právnické osoby), které oznámily jednotlivé skutky takto: ve 28 (12 %) případech do 24 hodin, ve 40 (12 %) případech do týdne, v 59 (25 %) případech do 1 měsíce, ve 107 (45 %) případech do 6 měsíců ve 4 (2 %) případech do 12 měsíců.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – celkem 13 případů, které byly oznámeny takto: ve 4 (31 %) případech do 24 hodin, v 7 (54 %) případech do týdne a ve 2 (15 %) případech do 1 měsíce.

Inzertní podvod – celkem 159 případů, které byly oznámeny takto: v 1 (1 %) případu do 24 hodin, v 15 (9 %) případech do týdne, ve 45 (28 %) případech do 1 měsíce a v 98 (62 %) případech do 6 měsíců.

Investiční podvod – celkem 15 případů, které byly oznámeny takto: v 7 (47 %) případech do týdne, v 5 (33 %) případech do 1 měsíce a ve 3 (20 %) případech do 6 měsíců.

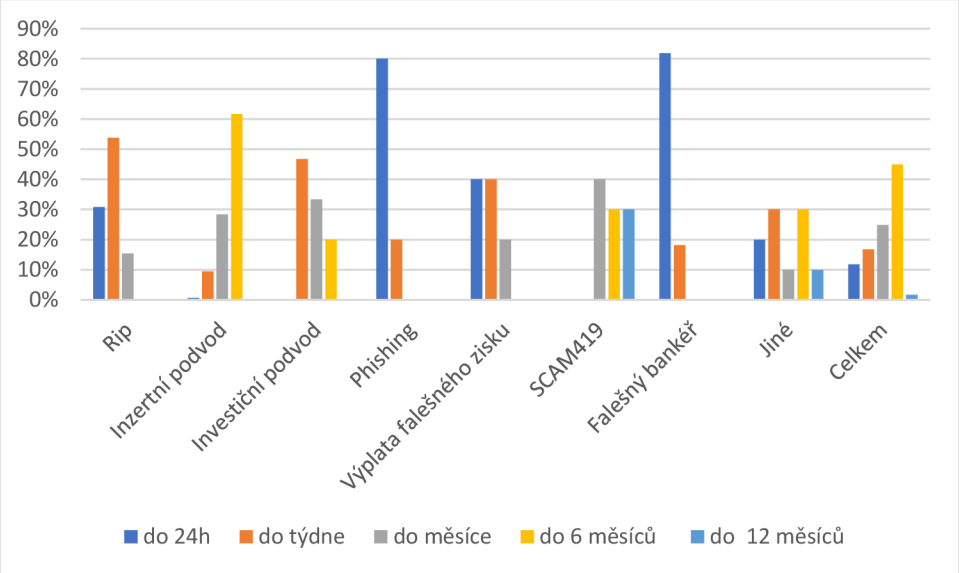
Phishing – celkem 10 případů, které byly oznámeny takto: v 8 (80 %) případech do 24 hodin a ve 2 (20 %) případech do týdne.

Výplata falešného zisku – celkem 10 případů, které byly oznámeny takto: ve 4 (40 %) případech do 24 hodin, ve 4 (40 %) případech do týdne, ve 2 (20 %) případech do 1 měsíce.

SCAM419 – celkem 10 případů, které byly oznámeny takto: ve 4 (40 %) případech do 1 měsíce, ve 3 (30 %) případech do 6 měsíců a ve 3 (30 %) případech do 12 měsíců.

Falešný bankéř – celkem 11 případů, které byly oznámeny takto: v 9 (82 %) případech do 24 hodin a ve 2 (18 %) případech do týdne.

Jiné – celkem 10 případů, které byly oznámeny takto: ve 2 (20 %) případech do 24 hodin, ve 3 (30 %) případech do týdne, v 1 (10 %) případu do 1 měsíce, ve 3 (30 %) případech do 6 měsíců a v 1 (10 %) případu do 12 měsíců.



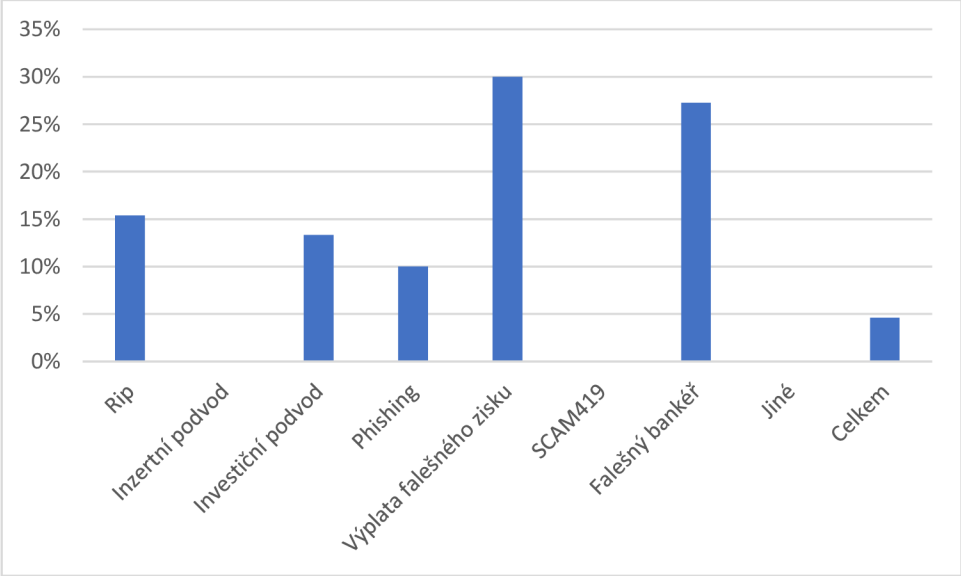
Graf 25: Doba oznámení po činu.

Zdroj: Vlastní zpracování

Otázka č. 31 byla zaměřena na zjištění, jaké podstatné informace poškozený o průběhu podvodu nesdělil.

Výzkumný soubor obsahoval 80 případů. V těchto případech bylo zjištěno celkem 238 poškozených (fyzické i právnické osoby) a z toho celkem v 11 (5 %) případech nedošlo ke sdělení podstatné informace.
U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – celkem 13 poškozených z toho 2 (15 %) nesdělili podstatné informace.
Inzertní podvod – celkem 159 poškozených a všichni sdělili podstatné informace (100 %).
Investiční podvod – celkem 15 poškozených z toho 2 (13 %) nesdělili podstatné informace.
Phishing – celkem 10 poškozených z toho 1 (10 %) nesdělil podstatné informace.
Výplata falešného zisku – celkem 10 poškozených z toho 3 (30 %) nesdělili podstatné informace.
SCAM419 – celkem 10 poškozených a všichni sdělili podstatné informace (100 %).
Falešný bankéř – celkem 11 poškozených z toho 3 (27 %) nesdělili podstatné informace.
Jiné – celkem 10 poškozených a všichni sdělili podstatné informace (100 %).



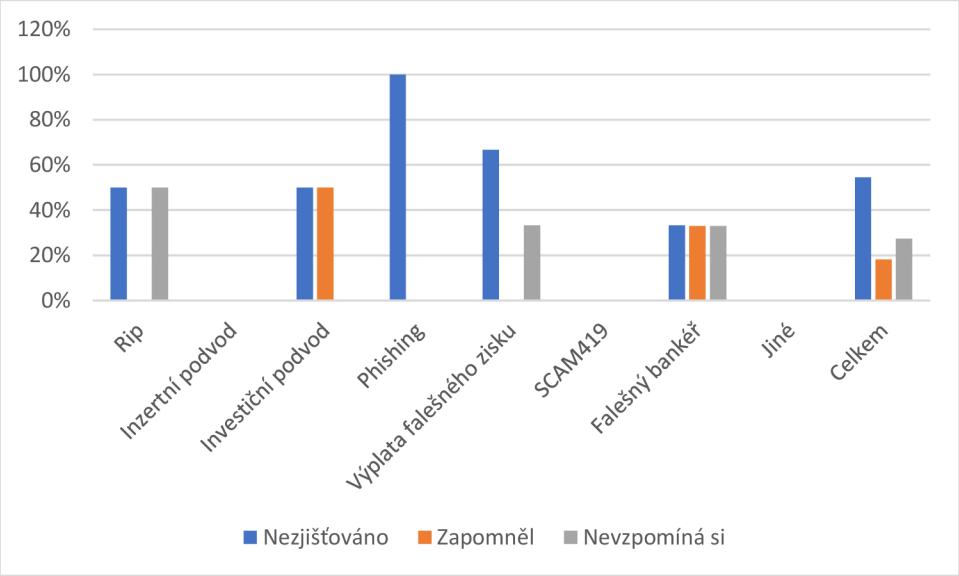
Graf 26: Nesdělení informací.

Zdroj: Vlastní zpracování

Otázka č. 32 byla zaměřena na zjištění, co bylo důvodem nesdělení informace.

Výzkumný soubor obsahoval 80 případů. V těchto případech bylo zjištěno celkem 238 poškozených (fyzické i právnické osoby) a z toho celkem v 11 případech nedošlo ke sdělení podstatné informace, a to z těchto důvodů: v 6 (55 %) případech to nebylo zjišťováno, ve 2 (18 %) případech poškozený zapomněl a ve 3 (27 %) případech si poškozený nevzpomíná.

U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod – celkem ve 2 případech a v 1 (50 %) to nebylo zjišťováno a v 1 (50 %) si poškozený nevzpomíná.
Inzertní podvod – podstatné informace sděleny.
Investiční podvod – celkem ve 2 případech a v 1 (50 %) to nebylo zjišťováno a v 1 (50 %) poškozený zapomněl.
Phishing – celkem v 1 případu a nebylo to zjišťováno (100 %).
Výplata falešného zisku – celkem ve 3 případech a ve 2 (67 %) to nebylo zjišťováno a v 1 (33 %) si poškozený nevzpomíná.
SCAM419 – podstatné informace sděleny.
Falešný bankéř – celkem ve 3 případech a v 1 (33 %) to nebylo zjišťováno, v 1 (33 %) poškozený zapomněl a v 1 (33 %) si poškozený nevzpomíná.
Jiné – podstatné informace sděleny.



Graf 27: Důvod nesdělení informací.

Zdroj: Vlastní zpracování

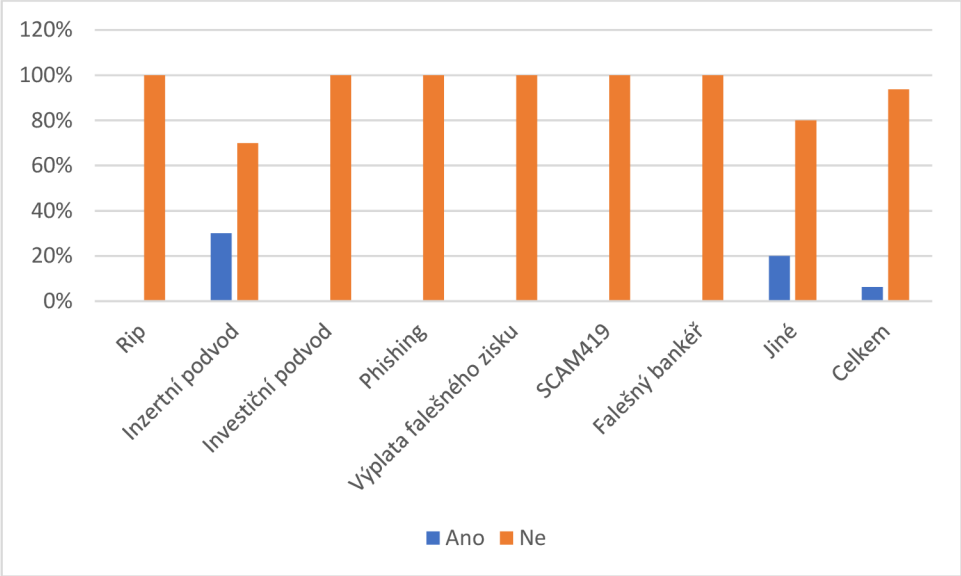
3.6.5 Výsledky k dílčímu cíli č. 4

Dílčím cílem č. 4 bylo zjistit, jaké jsou typické počáteční vyšetřovací situace u internetových podvodů.

Otázka č. 33 byla zaměřena na zjištěné, jestli je známa totožnost pachatele v počáteční etapě vyšetřování.

Výzkumný soubor obsahoval 80 případů. Totožnost pachatele byla známa v 5 (6 %) případech a v 75 (94 %) případech známa nebyla.

U jednotlivých způsobů jednání pachatele byla situace následující:
Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – totožnost nebyla známa ve všech případech (100 %).
Inzertní podvod – celkem z 10 případů nebyla totožnost známa v 7 (70 %) případech a ve 3 (30 %) případech byla známa.
Jiné – celkem z 10 případů nebyla totožnost známa v 8 (80 %) případech a ve 2 (20 %) případech byla známa.



Graf 28: Známá totožnost pachatele.

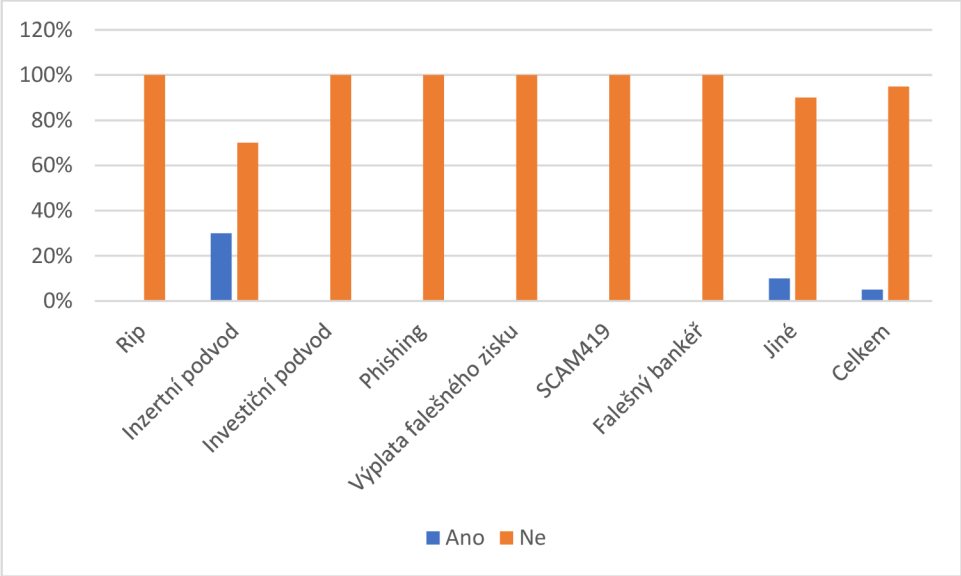
Zdroj: Vlastní zpracování

Otázka č. 34 byla zaměřena na zjištění, jestli je známo místo pobytu pachatele v počáteční etapě vyšetřování.

Výzkumný soubor obsahoval 80 případů. Místo pobytu pachatele bylo známo ve 4 (5 %) případech a v 76 (95 %) případech známo nebylo.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř – místo pobytu nebylo známo ve všech případech (100 %).
Inzertní podvod – celkem z 10 případů nebylo místo pobytu známo v 7 (70 %) případech a ve 3 (30 %) případech bylo známo.
Jiné – celkem z 10 případů nebylo místo pobytu známo v 9 (90 %) případech a v 1 (10 %) případu bylo známo.



Graf 29: Známý pobyt pachatele.

Zdroj: Vlastní zpracování

3.6.6 Výsledky k dílčímu cíli č. 5

Dílčím cílem č. 5 bylo zjistit, jaké jsou zvláštnosti počátečních úkonu u internetových podvodů.

Otázka č. 35 byla zaměřena na zjištění, jaké byly provedeny počáteční úkony.

Výzkumný soubor obsahoval 80 případů. Celkem v 77 (96 %) případech byl proveden výslech oznamovatele, v 55 (69 %) případech byly zajištěny předložené písemnosti, ve 3 (4 %) případech došlo k vydání věci, ve 37 (46 %) případech byl dán souhlas podle § 88a odst. 4 trestního řádu k vyžádání telekomunikačního provozu, v 32 (40 %) případech byl dán souhlas s vyžádáním bankovních informací, ve 35 (44 %) případech byly zajištěny digitální stopy a v 18 (23 %) případech byly postupem podle § 79a trestního řádu zajištěny finanční prostředky na účtu banky.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – celkem z 10 případů byl v 10 (100 %) případech proveden výslech oznamovatele, v 7 (70 %) případech byly zajištěny předložené písemnosti, v 7 (70 %) případech byl dán souhlas podle § 88a odst. 4 trestního řádu k vyžádání telekomunikačního provozu, ve 3 (30 %) případech byly zajištěny digitální stopy a ve 2 (20 %) případech byly postupem podle § 79a trestního řádu zajištěny finanční prostředky na účtu banky.

Inzertní podvod – celkem z 10 případů byl v 9 (90 %) případech proveden výslech oznamovatele, v 9 (90 %) případech byly zajištěny předložené písemnosti, ve 2 (20 %) případech byl dán souhlas podle § 88a odst. 4 trestního řádu k vyžádání telekomunikačního provozu, v 7 (70 %) případech byly zajištěny digitální stopy a ve 3 (30 %) případech byly postupem podle § 79a trestního řádu zajištěny finanční prostředky na účtu banky.

Investiční podvod – celkem z 10 případů byl v 10 (100 %) případech proveden výslech oznamovatele, v 10 (100 %) případech byly zajištěny předložené písemnosti, v 7 (70 %) případech byl dán souhlas podle § 88a odst. 4 trestního řádu k vyžádání telekomunikačního provozu, v 5 (50 %) případech byly zajištěny digitální stopy a ve 4 (40 %) případech byly postupem podle § 79a trestního řádu zajištěny finanční prostředky na účtu banky.

Phishing – celkem z 10 případů byl v 77 (96 %) případech proveden výslech oznamovatele, v 55 (69 %) případech byly zajištěny předložené písemnosti, ve 3 (4 %) případech došlo k vydání věci, ve 37 (46 %) případech byl dán souhlas podle § 88a odst. 4 trestního řádu k vyžádání telekomunikačního provozu, ve 32 (40 %) případech byl dán souhlas s vyžádáním bankovních informací, ve 35 (44 %) případech byly zajištěny digitální stopy a v 18 (23 %) případech byly postupem podle § 79a trestního řádu zajištěny finanční prostředky na účtu banky.

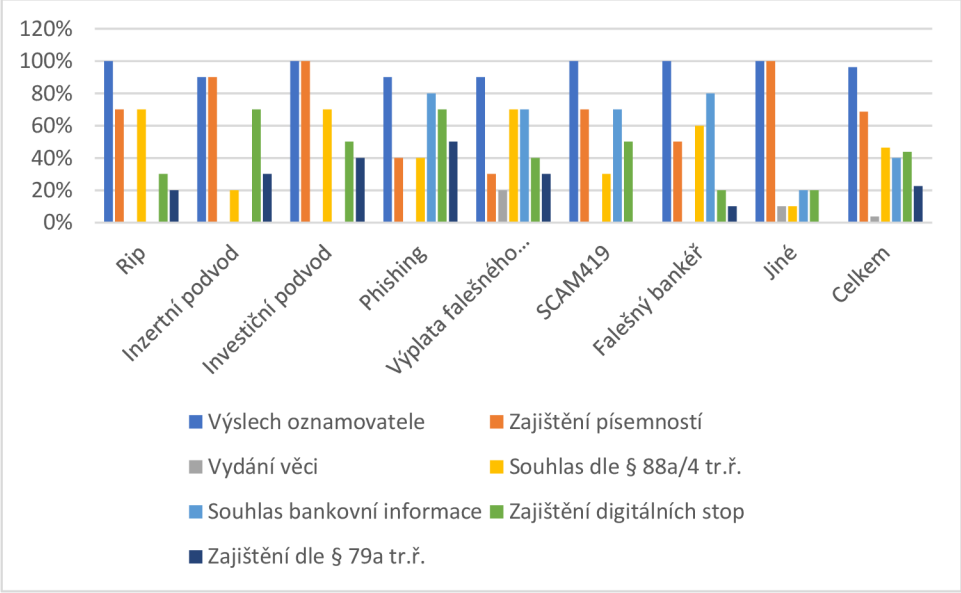
Výplata falešného zisku – celkem z 10 případů byl v 9 (90 %) případech proveden výslech oznamovatele, ve 3 (30 %) případech byly zajištěny předložené písemnosti, ve 2 (20 %) případech došlo k vydání věci, v 7 (70 %) případech byl dán souhlas podle § 88a odst. 4 trestního řádu k vyžádání telekomunikačního provozu, v 7 (70 %) případech byl dán souhlas s vyžádáním bankovních informací, ve 4 (40 %) případech byly zajištěny digitální stopy a ve 3 (30 %) případech byly postupem podle § 79a trestního řádu zajištěny finanční prostředky na účtu banky.

SCAM419 – celkem z 10 případů byl v 10 (100 %) případech proveden výslech oznamovatele, v 7 (70 %) případech byly zajištěny předložené písemnosti, ve 3 (30 %)

případech byl dán souhlas podle § 88a odst. 4 trestního řádu k vyžádání telekomunikačního provozu, v 7 (70 %) případech byl dán souhlas s vyžádáním bankovních informací, v 5 (50 %) případech byly zajištěny digitální stopy.

Falešný bankéř – celkem z 10 případů byl v 10 (100 %) případech proveden výslech oznamovatele, v 5 (50 %) případech byly zajištěny předložené písemnosti, v 6 (60 %) případech byl dán souhlas podle § 88a odst. 4 trestního řádu k vyžádání telekomunikačního provozu, v 8 (80 %) případech byl dán souhlas s vyžádáním bankovních informací, ve 2 (20 %) případech byly zajištěny digitální stopy a v 1 (10 %) případech byly postupem podle § 79a trestního řádu zajištěny finanční prostředky na účtu banky.

Jiné – celkem z 10 případů byl v 10 (100 %) případech proveden výslech oznamovatele, v 10 (100 %) případech byly zajištěny předložené písemnosti, v 1 (10 %) případu došlo k vydání věci, v 1 (10 %) případech byl dán souhlas podle § 88a odst. 4 trestního řádu k vyžádání telekomunikačního provozu, ve 2 (20 %) případech byl dán souhlas s vyžádáním bankovních informací, ve 2 (20 %) případech byly zajištěny digitální stopy.



Graf 30: Počáteční úkony.

Zdroj: Vlastní zpracování

3.6.7 Výsledky k dílčímu cíli č. 6

Dílčím cílem č. 6 bylo zjistit, jaké jsou zvláštnosti následných úkonů u internetových podvodů.

Otázka č. 36 byla zaměřena na zjištění, jaké následné úkony byly provedeny po oznámení.

Výzkumný soubor obsahoval 80 případů. Celkem ve 3 (4 %) případech byl proveden výslech poškozeného, ve 14 (18 %) případech výslech obviněného, v 1 (1 %) případu domovní prohlídka, ve 4 (5 %) případech vydání věci, ve 23 (29 %) případech informace SIM/IMEI, ve 44 (55 %) případech telekomunikační provoz postupem podle § 88a trestního řádu, ve 38 (48 %) případech žádost do zahraničí, ve 13 (16 %) případech právní pomoc, ve 45 (56 %) případech zajištění digitálních stop, v 7 (9 %) případech forenzní analýza, ve 2 (3 %) případech byly postupem podle § 79a trestního řádu zajištěny finanční prostředky na účtu banky, v 64 (80 %) případech byly vyžádány bankovní informace.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – celkem z 10 případů byl ve 2 (20 %) případech proveden úkon informace SIM/IMEI, v 7 (70 %) případech telekomunikační provoz postupem podle § 88a trestního řádu, v 10 (100 %) případech žádost do zahraničí, ve 3 (30 %) případech právní pomoc, ve 4 (40 %) případech zajištění digitálních stop, v 8 (80 %) případech byly vyžádány bankovní informace.

Inzertní podvod – celkem z 10 případů byl v 1 (10 %) případu proveden výslech poškozeného, ve 10 (100 %) případech výslech obviněného, ve 4 (40 %) případech vydání věci, v 8 (80 %) případech informace SIM/IMEI, v 5 (50 %) případech telekomunikační provoz postupem podle § 88a trestního řádu, ve 4 (40 %) případech zajištění digitálních stop, ve 4 (40 %) případů forenzní analýza, v 10 (100 %) případech byly vyžádány bankovní informace.

Investiční podvod – celkem z 10 případů byl ve 2 (20 %) případech proveden úkon informace SIM/IMEI, v 7 (70 %) případech telekomunikační provoz postupem podle § 88a trestního řádu, v 9 (90 %) případech žádost do zahraničí, ve 3 (30 %) případech právní pomoc, v 8 (80 %) případech zajištění digitálních stop, ve 2 (20 %) případech forenzní analýza, v 9 (90 %) případech byly vyžádány bankovní informace.

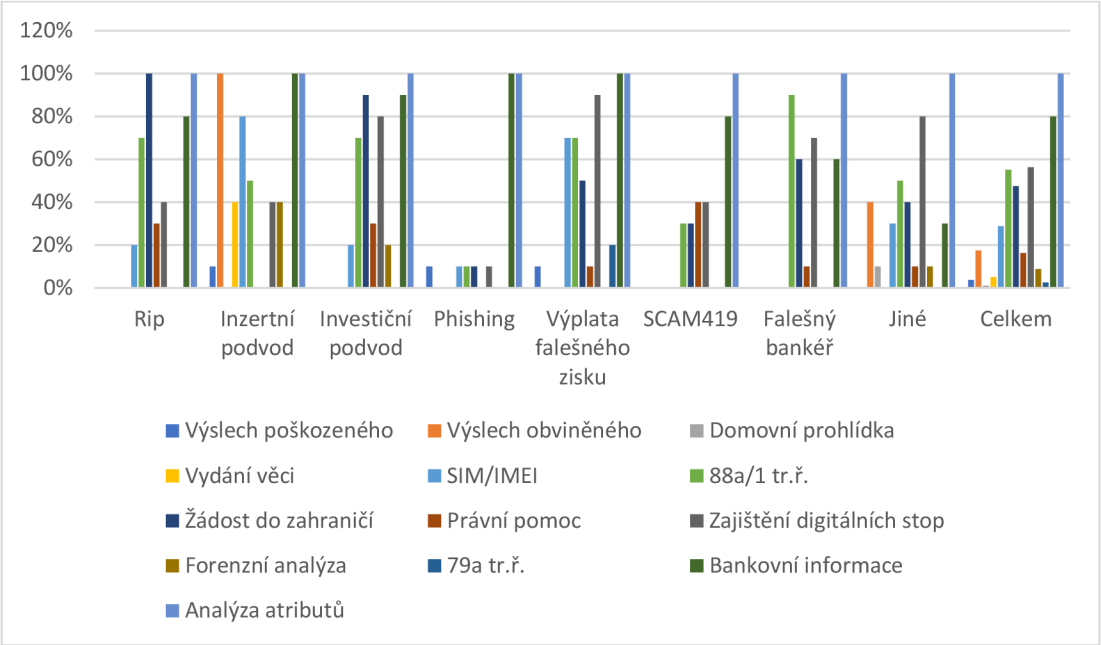
Phishing – celkem z 10 případů byl v 1 (10 %) případu proveden výslech poškozeného, v 1 (10 %) případu informace SIM/IMEI, v 1 (10 %) případu telekomunikační provoz postupem podle § 88a trestního řádu, v 1 (10 %) případu žádost do zahraničí, v 1 (10 %) případech zajištění digitálních stop, v 10 (100 %) případech byly vyžádány bankovní informace.

Výplata falešného zisku – celkem z 10 případů byl proveden v 1 (10 %) případu výslech poškozeného, v 7 (70 %) případech informace SIM/IMEI, v 7 (70 %) případech telekomunikační provoz postupem podle § 88a trestního řádu, v 5 (50 %) případech žádost do zahraničí, v 1 (10 %) případu právní pomoc, v 9 (90 %) případech zajištění digitálních stop, ve 2 (20 %) případech byly postupem podle § 79a trestního řádu zajištěny finanční prostředky na účtu banky, v 10 (100 %) případech byly vyžádány bankovní informace.

SCAM419 – celkem z 10 případů byl proveden ve 3 (30 %) případech telekomunikační provoz postupem podle § 88a trestního řádu, ve 3 (30 %) případech žádost do zahraničí, ve 4 (40 %) případech právní pomoc, ve 4 (40 %) případech zajištění digitálních stop, v 8 (80 %) případech byly vyžádány bankovní informace.

Falešný bankéř – celkem z 10 případů byl proveden v 9 (90 %) případech telekomunikační provoz postupem podle § 88a trestního řádu, v 6 (60 %) případech žádost do zahraničí, v 1 (10 %) případu právní pomoc, v 7 (70 %) případech zajištění digitálních stop, v 6 (60 %) případech byly vyžádány bankovní informace.

Jiné – celkem z 10 případů byl proveden ve 4 (40 %) případech výslech obviněného, v 1 (10 %) případě domovní prohlídka, ve 3 (30 %) případech informace SIM/IMEI, v 5 (50 %) případech telekomunikační provoz postupem podle § 88a trestního řádu, ve 4 (40 %) případech žádost do zahraničí, v 1 (10 %) případu právní pomoc, v 8 (80 %) případech zajištění digitálních stop, v 1 (10 %) případu forenzní analýza, ve 3 (30 %) případech byly vyžádány bankovní informace.



Graf 31: Následné úkony.

Zdroj: Vlastní zpracování

Otázka č. 37 byla zaměřena na zjištění, jaká doba uplynula od oznámení po zahájení trestního stíhání či rozhodnutí ve věci.

Výzkumný soubor obsahoval 80 případů. Do 1 měsíce byly ukončeny 2 (3 %) případy, do 6 měsíců 58 (73 %) případů, do 1 roku 16 (20 %) případů a po více než 1 roce byly ukončeny 4 (5 %) případy.

U jednotlivých způsobů jednání pachatele byla situace následující:

Reverzní inzertní podvod – celkem z 10 případů bylo do 6 měsíců ukončeno 10 (100 %) případů.

Inzertní podvod – celkem z 10 případů bylo do 6 měsíců ukončeno 6 (60 %) případů, do 1 roku 4 (40 %) případy.

Investiční podvod – celkem z 10 případů bylo do 6 měsíců ukončeno 5 (50 %) případů, do 1 roku 3 (30 %) případy a po více než 1 roce byly ukončeny 2 (20 %) případy.

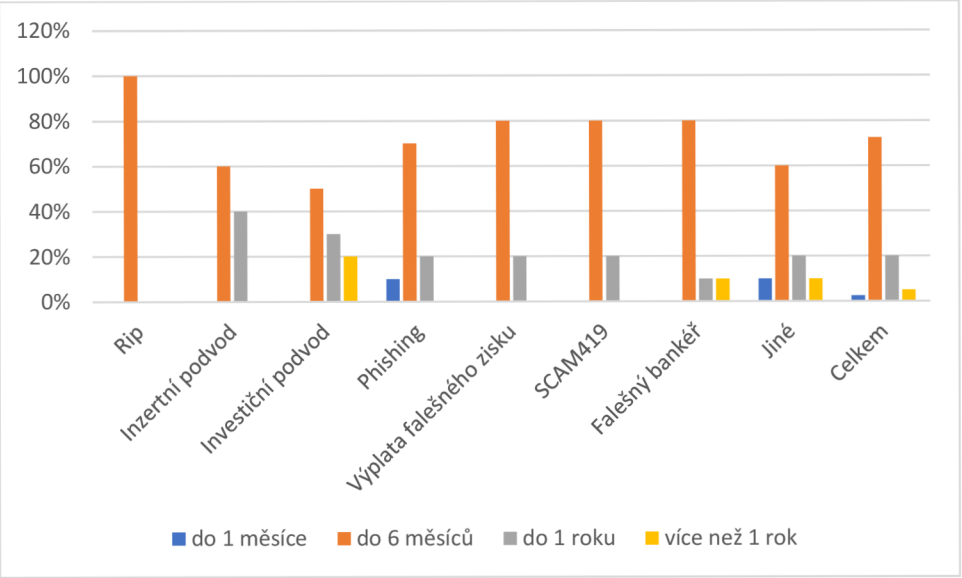
Phishing – celkem z 10 případů byl do 1 měsíce ukončen 1 (10 %) případ, do 6 měsíců 7 (70 %) případů, do 1 roku 2 (20 %) případy.

Výplata falešného zisku – celkem z 10 případů bylo do 6 měsíců ukončeno 8 (80 %) případů, do 1 roku 2 (20 %) případy.

SCAM419 – celkem z 10 případů bylo do 6 měsíců ukončeno 8 (80 %) případů, do 1 roku 2 (20 %) případy.

Falešný bankéř – celkem z 10 případů bylo do 6 měsíců ukončeno 8 (80 %) případů, do 1 roku 1 (10 %) případ a po více než 1 roce byl ukončen 1 (10 %) případ.

Jiné – celkem z 10 případů byl do měsíce ukončen 1 (10 %) případ, do 6 měsíců 6 (60 %) případů, do 1 roku 2 (20 %) případy a po více než 1 roce byl ukončen 1 (10 %) případ.



Graf 32: Doba do rozhodnutí ve věci.

Zdroj: Vlastní zpracování

4. METODIKA VYŠETŘOVÁNÍ INTERNETOVÝCH PODVODŮ

4.1 Kriminalistická charakteristika internetových podvodů

Internetové podvody jsou zaměřeny proti komukoliv, kdo užívá jakékoliv zařízení s přístupem do internetu nebo užívá zařízení, které mu umožňuje vést telefonní hovory v telekomunikační síti. Jedná se o druh trestného činu, který řadíme do skupiny majetkové kriminality. Internetový podvod kvalifikujeme podle § 209 trestního zákoníku.

Internetové podvody jsou velmi nebezpečným druhem majetkové trestné činnosti, které způsobují škody zejména fyzickým obětem, ale nevyhýbají se ani právnickým osobám. Velkou změnou proti minulosti je zejména to, že pachatelé své útoky cílí na veškeré dostupné finanční prostředky poškozených, a proto způsobují významné majetkové škody. Primárním cílem již není připravit poškozeného o jím zaslané finanční prostředky, ale získat přístup do internetového bankovnictví a odčerpat dostupný zůstatek včetně případného předschváleného úvěru.

Podle zprávy České bankovní asociace ze dne 30. ledna 2024 je celkový počet napadených klientů bank za rok 2023 celkem 69 685 tisíc a objem odčerpaných prostředků 1,35 miliardy korun.[56]

4.1.1 Kriminální situace

Za významné prvky kriminální situace u internetových podvodů můžeme považovat:

- dostupnost internetu a hlasových služeb,
- vlastnosti internetu zejména pak jeho anonymitu, globálnost, okamžitost,
- hospodářské, politické a společenské klima,
- zahraniční charakter jak při páchání, tak při odvádění výnosů z trestné činnosti,
- úroveň právního režimu místní, zahraniční (s ohledem na převážně zapojení mezinárodního prvku),
- dostupnost informací vyžadovaných ze zahraniční,
- úroveň odborné připravenosti orgánu činných v trestním řízení,

[56] Česká bankovní asociace, 2024. *Češi a kyberbezpečnost 2024* [online]. [cit. 10.12.2023]. Dostupné z: https://cbaonline.cz/cesi-a-kyberbezpecnost-2024.

- vlastnosti oběti jako důvěřivost, snaha rychle zbohatnout, nezkušenost s technologiemi,
- nízká objasněnost případů.

Podle zprávy Českého statistického úřadu pro rok 2022 využilo internet alespoň jedenkrát v životě ve věkové kategorii 16+ celkem 89,5 % osob v ČR.[57]

Podle zprávy Českého statistického úřadu pro rok 2023 bylo v roce 2021 celkem 1,302 milionů účastníků hlasové služby v pevné síti v Česku[58] a celkem 14,943 milionů účastníků hlasové služby v mobilní síti v Česku.[59]

S ohledem na celkový počet obyvatel České republiky, který k 30.6.2023 činí 10,87 milionů,[60] lze konstatovat, že internetový útok může zasáhnout kohokoliv.

Za nárůstem zcela jistě stojí celospolečenské události posledních let jako:

- celosvětová pandemie onemocnění COVID-19 (2019-2022), která mimo mnohá úmrtí zapříčinila i zpřetrhání obchodních vazeb a kumulaci finančních prostředků, které nebyly za co utrácet,
- razantní zdražení energií, které započalo v posledním čtvrtletí roku 2021,
- válečný konflikt na Ukrajině, který vypukl 24. února 2022.

To vše vedlo k nárustu inflace, která za rok 2022 činila 15,1 %, přestože od roku 2000 nepřekročila míru 6.3 %.[61]

Nahromaděné finanční prostředky z doby covidu a touha po jejich zhodnocení vedla k tomu, že pachatelé začali využívat záminku zhodnocení investic pro své obohacení. Tomuto závěru nasvědčují i výsledky provedeného výzkumu, kdy bylo zjištěno, že

---

[57] ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2022. Osoby v ČR používající internet, 2022: Tabulka 2.1. In: *Využívání informačních a komunikačních technologií v domácnostech a mezi osobami za období 2022* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/documents/10180/164606768/06200422.pdf/1c5c22c0-8941-4670-9698-e949482b0c35?version=1.3.

[58] ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2023. Účastníci hlasové služby v pevné síti v Česku: Tab. A1. In: *Informační společnost v číslech – 2023 - Česká republika a EU* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/documents/10180/191186455/06100423.pdf/879a3104-e54c-4f4e-b768-b0bd057ac006?version=1.3.

[59] ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2023. Účastníci hlasové služby v mobilní síti v Česku: Tab. A2. In: *Informační společnost v číslech – 2023 - Česká republika a EU* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/documents/10180/191186455/06100423.pdf/879a3104-e54c-4f4e-b768-b0bd057ac006?version=1.3.

[60] ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2023. *Pohyb obyvatelstva - 1. pololetí 2023* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/csu/czso/cri/pohyb-obyvatelstva-1-pololeti-2023.

[61] *ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2023. Věc: Výpis ze statistického zjišťování* [online]. [cit. 10.12.2023]. Dostupné z: https://www.czso.cz/documents/10180/132433649/Inflace_2000_2023.pdf.

19 % internetových podvodů má souvislost s investováním, což se promítlo do těchto způsobů jednání pachatele: investiční podvod, výplata falešného zisku (otázka č. 1).

Velkou měrou se na kriminální situaci podílí i zapojení zahraničního prvku a to, jak ve smyslu páchání ze zahraničí, tak ve smyslu vyvedení finančních prostředků do zahraničí. Jak ukázal výzkum, zahraniční prvek je obsažen celkem u 84 % případů (otázka č. 11).

Zapojení zahraničního prvku do trestné činnosti má velký význam i pro objasněnost trestných činů. Výzkumem bylo zjištěno, že z celkem z 67 případů se zahraničním prvkem byl objasněn 1 (1 %) případ. U všech objasněných inzertních podvodů, nebyl zahraniční prvek přítomen.

Vývojový trend v oblasti objasněnosti trestných činů spáchaných internetem a ostatními sítěmi v letech 2016-2022 můžeme sledovat v přiložené tabulce[62] sestavené autorem podle dat Policie České republiky:

Registrované a objasněné skutky v České republice, celková kriminalita od roku 2016							
rok	**2022**	**2021**	**2020**	**2019**	**2018**	**2017**	**2016**
registrované skutky	181 991	153 233	165 525	199 221	192 405	202 303	218 162
z toho objasněno	81 474	72 493	77 786	93 202	92 795	94 890	101 678
objasněnost	44,8%	47,3%	47,0%	46,8%	48,2%	46,9%	46,6%
spácháno internetem a ostatními sítěmi:							
registrované skutky	18 554	9 518	8 073	8 417	6 815	5 654	4 990
z toho objasněno	2 799	2 356	2 466	3 124	3 256	2 782	2 558
objasněnost	15,1%	24,8%	30,5%	37,1%	47,8%	49,2%	51,3%

Tabulka 1: Registrované a objasněné skutky v ČR v letech 2016–2022.

Zdroj: Policie ČR

Na výše uvedených datech je zřejmé, jaký měla výše popsaná společenská, hospodářská a politická situace vliv na nárůst počtu trestných činů spáchaných internetem a ostatními sítěmi. Významné jsou zejména tyto souvislosti u případů spáchaným internetem a jinými sítěmi:

1) bezprecedentní nárůst případů mezi lety 2021–2022, kdy se zvýšil o 9 036 (94,9 %),

[62] VINČÁLEK, Jakub. Jak se vyvíjí objasněnost trestných činů v kyberprostoru. *STATISTIKA&MY* [online]. 2023, roč. 13, č. 5. [cit. 10.02.2024]. Dostupné z: https://www.statistikaamy.cz/wp-content/uploads/2023/05/18042305.pdf.

2) nízká míra objasněnosti za rok 2022, která činí 15,1 % (objasněnost všech registrovaných skutků 44,8 %), objasněnost u výzkumného vzorku 7 % (otázka č. 12),

3) mezi jednotlivými lety v období 2016–2022 se počet objasněných případů téměř neliší (2356 až 3256), přestože nárůst registrovaných skutků ve stejném období je vyšší o 13 564 případů (271,8 %),

Domnívám se, že s ohledem na zjištěné statistické údaje dotváří nízká míra objasněnosti kriminální situaci a může pachatele podněcovat k dalšímu páchání.

4.1.2 Způsob páchání

Způsoby, kterými lze spáchat internetový podvod jsou velmi různorodé a s jistou nadsázkou lze říct, že lze vymyslet nekonečné množství podvodných jednání. Ustanovení § 209 trestního zákoníku nám definuje podvod jako jednání, při kterém pachatel sebe nebo jiného obohatí tím, že:

- uvede někoho v omyl,
- využije něčího omylu, nebo
- zamlčí podstatné skutečnosti,

a způsobí tak na cizím majetku škodu nikoliv nepatrnou.

Podstatou podvodného jednání je tedy vyvolání nebo využití falešných představ poškozeného o určitých okolnostech nebo zamlčení podstatných skutečností, přičemž lze tyto okolnosti (skutečnosti) považovat za vhodné kritéria pro dělení typických způsobů páchání, které můžeme kategorizovat takto:

1. uvedení v omyl nebo využití omylu v osobě,
2. uvedení v omyl nebo využití omylu ve vztahu k věcem,
3. uvedení v omyl nebo využití omylu ve faktu činnosti či události,
4. uvedení v omyl nebo využití omylu ve vztahu k příslibům,
5. zamlčení podstatných skutečností,
6. trikové podvody,
7. uvedení v omyl nebo využití omylu kombinováním výše uvedených způsobů.[63]

[63] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4, str. 185-187.

Na základě provedeného terénního šetření (otázka č. 1) jsem zjistil nejčastější způsoby jednání pachatele a typické způsoby páchání můžeme doplnit takto:

1. Uvedení v omyl nebo využití omylu ve faktu činnosti či události u „**reverzních inzertních podvodů**“, kdy má poškozený mylnou představu o vzniku události, tedy o prodeji zboží, při které mu pachatel pod falešnou záminkou získání peněz za nabízené zboží zašle phishingový odkaz, který pachateli slouží k získání přihlašovacích údajů do internetového bankovnictví nebo k získání identifikátorů platební karty poškozeného, které následně zneužije.
2. Uvedení v omyl nebo využití omylu ve vztahu k věcem u „**inzertních podvodů**“ při nákupu věcí, zvířat, služeb, kdy je poškozený uváděn v omyl ve vztahu k existenci věci (její kvalitě), zvířete, služby (např. vyhraná aukce na prodej neexistujícího zájezdu).
3. Kombinace způsobů uvedení v omyl nebo využití omylu v osobě a uvedení v omyl nebo využití omylu ve faktu činnosti či události, u „**investičních podvodů**“, kdy je poškozený uveden v omyl ve vztahu k pracovnímu postavení pachatele, kdy se mylně domnívá, že se jedná o pracovníka investiční společnosti a v případech, kdy pachatel získá na základě vzdáleného přístupu i přístup do zařízení poškozeného, má poškozený mylnou představu o činnosti pachatele, kdy se domnívá, že prováděné transakce slouží k investování jeho finančních prostředků.
4. Kombinace způsobů uvedení v omyl nebo využití omylu v osobě a uvedení v omyl nebo využití omylu ve faktu činnosti či události, u „**phishingu**“, kdy je poškozený uveden v omyl ve vztahu k pracovnímu postavení pachatele, kdy se mylně domnívá, že doručenou zprávu s odkazem zaslala odpovědná osoba deklarované společnosti či instituce a dále je poškozený uveden v omyl ve faktu události, kdy se mylně domnívá, že mu vznikl určitý nárok na získání finančních prostředků nebo, že se přihlašuje na legitimní stránky banky.
5. Kombinace způsobů uvedení v omyl nebo využití omylu v osobě a uvedení v omyl nebo využití omylu ve faktu činnosti či události, u „**výplaty falešného zisku**“, kdy je poškozený uveden v omyl ve vztahu k pracovnímu postavení pachatele, kdy se mylně domnívá, že se jedná o pracovníka deklarované společnosti, dále je poškozený uveden v omyl ve faktu události, kdy se mylně domnívá, že mu vznikl určitý nárok na vyplacení zisku a v případech, kdy

pachatel získá na základě vzdáleného přístupu i přístup do zařízení poškozeného, má poškozený mylnou představu o činnosti pachatele, kdy se domnívá, že prováděné transakce slouží k získání finančních prostředků.

6. Kombinace způsobů uvedení v omyl nebo využití omylu v osobě, uvedení v omyl nebo využití omylu ve faktu činnosti či události a uvedení v omyl nebo využití omylu ve vztahu k příslibům u „**Scam 419**“, kdy je poškozený uveden v omyl ve vztahu k totožnosti osoby, se kterou komunikuje (falešný lékař, voják apod.), dále je uveden v omyl ve faktu události (dědictví, nemoc apod.) a u případů s nabídkou na uzavření sňatku je poškozený uveden omyl ve vztahu k příslibům.
7. Kombinace způsobů uvedení v omyl nebo využití omylu v osobě a uvedení v omyl nebo využití omylu ve faktu činnosti či události, u „**falešných bankéřů**“, kdy je poškozený uveden v omyl ve vztahu k pracovnímu postavení pachatele, kdy se mylně domnívá, že se jedná o pracovníka banky, dále je uveden v omyl ve faktu události, kdy je mu předestřeno, že jeho bankovní účet byl napaden a je v nebezpečí.
8. Uvedení v omyl nebo využití omylu kombinováním výše uvedených základních způsobů u „**jiných podvodných jednáních**“, kdy bylo výzkumem zjištěno dalších 19 různých způsobů provedení internetového podvodu.

O způsobu páchání jsem zjistil tyto další informace.

Nejčastěji využitým komunikačním prostředkem byl e-mail ve 48 % případech a hlasové služby (volání) v 43 % případech. Podle údajů Českého statistického úřadu pro rok 2022 používá 99,8 % osob v Česku mobilní telefon[64] a e-mail je podle údajů Českého statistického úřadu s 94,2 % nejčastěji používaný prostředek komunikace na internetu.[65] U podvodů typu: investiční podvod, výplata falešného zisku a falešný bankéř, byli poškození ve 100 % kontaktování přes telefonní hovor a až následně dostávali případné instrukce jiným komunikačním prostředkem.

---

[64] ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2023. Osoby v Česku používající mobilní telefon; 2022: Tab. C1. In: *Informační společnost v číslech, 2023, Česká republika a EU* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/documents/10180/191186455/06100423.pdf/879a3104-e54c-4f4e-b768-b0bd057ac006?version=1.3.

[65] ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2022. Osoby v ČR komunikující přes internet s ostatními, 2022: Tabulka 5.1. In: *Využívání informačních a komunikačních technologií v domácnostech a mezi osobami za období 2022* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/documents/10180/164606768/06200422.pdf/1c5c22c0-8941-4670-9698-e949482b0c35?version=1.3.

Všeobecná dostupnost komunikačních prostředků je tedy jedním ze základních objektivních determinantů způsobu páchání internetových podvodů.

Pachatelé v 94 % případů jednali pod falešnou identitou a v 6 % vystupovali pod vlastním jménem, přičemž všechny tyto případy byly objasněny. Tyto objasněné případy neměli přesah do zahraničí a pachatelé se doznali.

Technických prostředků anonymizace komunikace využili pachatelé v 79 % případů a u 15 % případů to nebylo zjišťováno, ale vzhledem k tomu, že ani tyto případy nebyly objasněny lze to předpokládat. U podvodu typu falešný bankéř byla ve 100 % případů využita anonymizační technika spoofingu.

Lze tedy konstatovat, že až na výjimky, lze skrývání identity a používání technických prostředků anonymizace komunikace považovat za základní dějové a věcné komponenty způsobu páchání internetových podvodů.

U objasněných trestných činů byla vlastní technika použita u 64 % případů a u 36 % případů to nebylo zjišťováno.

V minulosti byly internetové podvody založeny zejména na tom, že pachatel zboží nabízel k prodeji a toto nedoručil. Tento model byl však použit pouze v 17 % případů.

Pozici kupce měl pachatel u 35 % případů (pouze RIP) a ve 48 % měl jiné postavení.

Pachatelé k převodu peněz využívají nejčastěji bankovní účet a to v 81 %, převod na kryptoměnu ve 23 % a služeb převodů peněz ve 21 %. Ačkoliv se může zejména u bankovního účtu nebo u služeb převodu peněz jevit, že je snadná dohledatelnost jejich majitelů je potřeba si uvědomit tyto skutečnosti.

Bankovní účet:

- bývá zakládán osobami, které nemají občanství země Evropské unie a pobývají na jejím území na základě práva na pobyt, ale jejich pobyt není znám a bankovní účet založili za úplatu a předali k němu přístupové údaje neznámé osobě,
- bankovní účet je pachatelem založen on-line na jméno osoby, která byla zmanipulována tak, že k tomu poskytla potřebnou součinnost, aniž by věděla, že je na její jméno bankovní účet založen,
- k převodu peněz jsou využity bankovní účty poškozených osob, které pachatel ovládnul za součinnosti poškozených v jiné trestní věci.

Služby převodu peněz, bitcoinové směnárny:

- účet je pachatelem založen on-line na jméno osoby, která byla zmanipulována tak, že k tomu poskytla potřebnou součinnost, aniž by věděla, že na její jméno je takový účet založen,
- účty založené na zfalšované doklady,
- služba je anonymní.

Mezi objektivní determinant způsobu páchání řadíme i vztah mezi pachatelem a obětí. U objasněných případů bylo zjištěno, že pachatelem byla vždy cizí osoba. Otázka však byla zaměřena na osobní znalost mezi pachatelem a obětí. Pokud bychom však tento vztah vnímali v širších souvislostech tak to, že pachatel má o oběti osobní informace, kterými může oběť manipulovat, mu může významně napomoci při úspěšném páchání trestné činnosti. Typickým příkladem je jednání pachatele u způsobu „falešný bankéř".

Mezi další objektivní determinant způsobu páchání řadíme i existenci spolupachatelů. Ze 14 objasněných případů byly 4 spáchány ve spolupachatelství a to max. 2 osob. V případech, které byly součástí výzkumného souboru se však nejednalo o příliš sofistikovanou a rozsáhlou trestnou činnost, kdy spolupachatelství bylo spíše dílem okolností než potřeby. Z praxe je ovšem známo, že zejména u způsobu jednání pachatele: reverzní inzertní podvod, investiční podvod, výplata falešného zisku, falešný bankéř, se jedná o vysoce organizovanou trestnou činnost páchanou ze zahraničí za účasti desítek členů organizované zločinecké skupiny.

4.1.3 Osobnostní rysy pachatele trestného činu

Pachatelem internetového podvodu může být kdokoliv, kdo využívá služeb elektronických komunikací a má přístup k internetu nebo využívá interpersonální komunikační služby (hlasové volání, zasílání zpráv, elektronická pošta).[66]

Ze způsobů jednání pachatele, které byly zjištěny provedeným výzkumem nelze předpokládat, že by byl pro jednotlivé způsoby vhodný pouze jeden typ pachatele.

[66] Český telekomunikační úřad. *Dělení služeb elektronických komunikací* [online]. [cit. 10.12.2023]. Dostupné z: https://www.ctu.cz/deleni-sluzeb-elektronickych-komunikaci.

Jsou zde způsoby více technické, které jsou založeny pouze na komunikaci pomocí zpráv, kde však není potřeba na oběť příliš psychologicky působit. Jedná se zejména o reverzní inzertní podvody, phishing.

Způsoby psychologicko-technické, jako jsou investiční podvody, výplata falešného zisku, falešný bankéř, kde je nutné oběť nejenom přesvědčit o navozené situaci, ale mít i technickou znalost k vyvedení finančních prostředků.

Způsob vyloženě psychologický jako je SCAM419, kde se nejvíce projeví schopnost navazovat kontakty a tyto si udržet. Z provedeného výzkumu vyplynulo, že tyto trestné činy se oznamují s největší časovou prodlevou.

Podvodným způsobem, který se ve srovnání s jinými nejeví tak náročný, je inzertní podvod, kde postačí zjednodušeně řečeno vystavit inzerát a počkat až někdo zaplatí.

Posledním způsobem jsou „jiné“ podvody, které můžou být různou kombinací uvedeného. Zde je potřeba uvést, že objasněny byly pouze jednodušší způsoby jednání pachatele podobné svým provedením inzertním podvodům.

Nenáročnost provedení podvodu u způsobu jednání: inzertní podvod a jiné, se pak projevuje v tom, že tyto byly jako jediné objasněny.

Provedeným výzkumem bylo zjištěno, že nejčastějším pachatelem je muž (89 %) ve věku 20-29 let (50 %), který se již v minulosti trestné činnosti dopustil (56 %) a byl odsouzen za trestný čin podvod (90 %).

Dále bylo zjištěno, že pachatel je nejčastěji v zaměstnaneckém poměru a to ve 44 % a má základní (39 %) nebo středoškolské vzdělání s výučním listem (39 %).

Pachatelé v 67 % doznali trestnou činnost, v 11 % doznali jednání, ale popírali úmysl a ve zbylých případech odmítli vypovídat nebo trestnou činnost popírali.

4.1.4 Osobnostní rysy oběti trestného činu

Obětí internetového podvodu může být kdokoliv, kdo využívá služeb elektronických komunikací a má přístup k internetu nebo využívá interpersonální komunikační služby (hlasové volání, zasílání zpráv, elektronická pošta). Platí pro něj tedy stejné předpoklady, jako pro pachatele.

Kriminalistické učení považuje za oběť konkrétní fyzickou osobu, která utrpěla v souvislosti se spácháním trestného činu újmu na životě, zdraví, majetku či právech.[67] U zkoumaného vzorku 238 poškozených byly prvotně zjišťovány poškozené fyzické osoby, kterých bylo 97 %.

Jako průměrný věk oběti bylo zjištěno rozmezí 30-39 let v 28 %, 20-29 let v 27 %.

Vzhledem k reprezentativnímu výzkumnému vzorku, lze vyvrátit představu o tom, že obětmi internetových podvodů jsou zejména starší osoby. Ve věkovém rozmezí 60-89 let je pouze 9,4 % obětí a 11 % obětí je ve starobním důchodu. Největší skupinu obětí tvoří osoby ve věku 20-39 let a to 55 %.

Existuje však spojitost mezi některými způsoby jednání a věkem obětí, např. obětmi reverzních inzertních podvodů nejsou osoby nad 50 let věku a dále pak, že u investičních podvodů tvoří osoby starší 60 let 40 % obětí a u SCAM419 30 % obětí.

Největší skupinou obětí jsou pak zaměstnanci a to 46 %.

Muž byl pak obětí v 54 % procentech případů a žena v 46 % procentech případů. Pohlaví tedy u internetových podvodů nehraje zásadnější roli. Nicméně jsou zde určitá specifika, kdy v 90 % případů jsou obětmi ženy podvodu SCAM419 a v 85 % případů u reverzních inzertních podvodů. Muži na druhou stranu tvoří 63 % obětí u inzertních podvodů.

Společné znaky obětí jsou zejména:

- u reverzních inzertních podvodů důvěřivost, nedostatečná zkušenost s fungováním technologií,
- u inzertních podvodů důvěřivost až lehkomyslnost,
- u investičních podvodů a výplaty falešného zisku vidina rychlého, snadného zisku, nedostatečná zkušenost s fungováním technologií,
- u phishingu vidina rychlého a snadného zisku, nedostatečná zkušenost s fungováním technologií,
- u SCAM419 citová osamělost, důvěřivost,
- u falešného bankéře – důvěřivost, nedostatečná zkušenost s fungováním technologií,
- u jiných podvodů kombinace uvedeného, podle konkrétního způsobu jednání pachatele.

[67] MUSIL, Jan, Zdeněk KONRÁD a Jaroslav SUCHÁNEK. *Kriminalistika*. 2. přeprac. a dopl. vyd. Praha: C. H. Beck, 2004. ISBN 80-7179-878-9, str. 66.

4.1.5 Motiv činu

Skutková podstata trestného činu podvod vyžaduje, aby byla způsobena škoda na cizím majetku, a proto u internetových podvodů dominuje motiv zištný, a to zejména finanční.

Tento předpoklad potvrdil i provedený výzkum, kdy byl zištný motiv zjištěn u všech případů.

Vzhledem k charakteru u 74 % způsobu jednání: reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku, SCAM419, falešný bankéř, usilovali pachatelé o získání veškerých finančních prostředků poškozených, které jim buď sami odčerpali z bankovních účtů nebo jim poškození po vhodné manipulaci dobrovolně zaslali.

4.2 Typické stopy a jiné soudní důkazy

U většiny trestných činů bývá zpravidla místo činu výchozím bodem pro vyšetřování. Ohledáním místa a vyhodnocením jeho výsledků můžeme usoudit, zda došlo k trestnému činu a o jaký trestný čin se jedná. Na místě činu také nalézáme stopy, které nám pomáhají najít a usvědčit pachatele.[68]

U internetových podvodů stejně jako u obecných podvodů je místem spáchání místo: kde došlo k jednání pachatele, kde se pachatel obohatil a kde vznikla škoda. Vzhledem k tomu, že u internetových podvodů se používá komunikace na dálku, je místem spáchání i místo, kde se nacházel poškozený/pachatel v době komunikace s pachatelem/poškozeným. Zjištění místa, odkud jednal neznámý pachatel nám může pomoci k zajištění důkazů k jeho identifikaci, jako jsou např. kamerové záznamy z místa, kde se připojoval do sítě internet či docházelo k obohacení (výběr z bankomatů), zajištění použité techniky.

Paměťová stopa

Komunikaci chápeme jako interakci mezi pachatel a obětí, která probíhá buď v psané nebo hlasově podobě a zanechává tedy typickou stopu, a to ve formě paměťové stopy

[68] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4, str. 188.

poškozeného. Výchozím bodem tedy bývá výpověď poškozeného. Paměťové stopy byly zajištěny ve 100 % případů výzkumného souboru.

Digitální stopy

S ohledem na to, že komunikace probíhá za využití informačních a komunikačních technologií, můžeme stopy hledat v zařízeních, které tento přenos umožňují, ale také u provozovatelů služeb komunikačních systémů.

Zdrojem těchto stop jsou:

- **provozovatelé služeb komunikačních systémů**: jedná se o informace, které nemusí být nebo nejsou dostupné na zařízeních pachatele či poškozeného, ale na zařízeních takových provozovatelů: IP logy, MAC adresy, informace o prováděné činnosti (např. v bankovnictví) obsah zpráv, komunikace (e-mail) apod.,
- **mobilní zařízení** – např. mobilní telefon, tablet pachatele, ale i poškozeného, ve kterých je komunikace, kontakty, obrázkové a jiné soubory, tokenizovaná platební karta poškozeného a další stopy o činnosti pachatele,
- **výpočetní technika** – sem řadíme vše, co si můžeme představit pod pojmem počítač, kde se ukládají informace o činnosti pachatele jako komunikace, kontakty, obrázkové a jiné soubory, použité programy apod.

Digitální stopy z mobilních zařízení jsou zjišťovány jak u poškozeného, tak u pachatele. Provedeným výzkumem bylo zjištěno, že digitální stopy byly zajištěny u 86 % procent případů.

Zajištění písemností

Za listinný důkaz dle trestního řádu považujeme: *„listiny, které svým obsahem prokazují nebo vyvracejí dokazovanou skutečnost vztahující se k trestnému činu nebo k obviněnému“*.[69] Takové listiny byly od poškozených zajištěny v 69 % případů. Jedná se zejména o písemnosti, které předávají poškození během výslechu a týkají se především proběhlé komunikace a potvrzení o platebních transakcích.

[69] Zákon č. 141/1961 Sb., *o trestním řízení soudním* (*trestní řád)* v posledním znění, § 112.

Bankovní informace

Důležitým důkazem jsou bankovní informace, které nám umožňují zjistit identitu pachatele nebo osoby vědomě nebo nevědomě do trestného činu zapojeného. Za nevědomě zapojenou osobu můžeme považovat jiné poškozené, kterým pachatel po vhodné manipulaci ovládl jejich bankovní účet, který následně bez jejich vědomí použil k převodu finančních prostředků podvodně získaných u jiného poškozeného. Za bankovní informace považujeme v této práci i informace získané o převodu peněz od společností poskytující služby převodu peněz. Bankovní informace byly zjišťovány v 90 % případů. Důvodem pro nezjišťování těchto informací může být skutečnost, že byly použity služby poskytované v zemích s obtížnou vymahatelností práva nebo zemích, se kterými není navázána policejní ani justiční spolupráce.

Telekomunikační provoz

Důkaz spočívající ve zjištění informací o uskutečněném telekomunikačním provozu je pro objasňování internetových podvodů významným zdrojem informací. Telekomunikačním provozem rozumíme informace o provozních a lokalizačních údajích, jejichž rozsah je upraven vyhláškou.[70] Délka uchovávaní ve vyhlášce specifikovaných údajů je 6 měsíců.[71]

Zpravidla se jedná o informace ke zjištění telekomunikačního provozu u konkrétního účastníka hlasové služby nebo o zjištění provozních a lokalizačních údajů k IP adrese.

Údaje o telekomunikačním provozu u konkrétního účastníka nám umožňuje zjistit odchozí, příchozí volání, SMS a MMS zprávy, lokalizaci stanice podle buněk a u mobilních zařízení též IMEI použitých zařízení.

Provozní a lokalizační údaje se používají zejména ke zjištění informací k IP adrese, která nám umožňuje zjistit místo odkud pachatel komunikoval. Můžeme zjistit informace o Mac adrese, které nám následně může pomoci identifikovat konkrétní zařízení, které bylo užito pachatelem. Informace k IP adrese nevedou ke konkrétní osobě pachatele, ale do místa odkud pachatel komunikoval. Na takovém místě je

[70] Vyhláška č. 357/2012 Sb., *o uchovávání, předávání a likvidaci provozních a lokalizačních údajů* v posledním znění.
[71] Zákon č. 127/2005 Sb. *o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)* v posledním znění, § 97 odst. 3.

zapotřebí zajistit zařízení, pro zajištění digitálních stop, jejichž forenzní analýzou mohou být zjištěny informace vedoucí ke konkrétní osobě pachatele.

Zjišťování informací o telekomunikačním provozu do zahraniční je problematické s ohledem na dobu jejich uchovávání, která je v zahraničí různá a v době jejich vyžádání již nemusí být dostupná.

Údaje o telekomunikačním provozu byly zjišťovány v 51 % případů.

SIM/IMEI

Dalším významný zdrojem informací jsou informace provozně technického charakteru k SIM kartě, které slouží k identifikaci účastníka telefonní služby a informace k IMEI mobilního zařízení, což je jedinečné číslo k identifikaci zařízení. Z těchto informací lze zjistit v jakých dalších zařízeních byla použita konkrétní SIM karta nebo jaké SIM karty byly použity v konkrétním zařízení.

Tyto informace byly zjišťovány v 25 % případů výzkumného vzorku.

Věcné důkazy

Typickou stopu jsou věcné důkazy. Jedná se o věci, které pachatel zaslal poškozenému. Nejčastěji se jedná o zboží jiné kvality, zcela jiné zboží nebo napodobeniny originálů uměleckých děl. Věcné důkazy byly zajištěny ve 3 % případů výzkumného souboru a jednalo se o zaslané napodobeniny.

Pro potřeby vyšetřování je nutné všechny stopy a listinné a věcné důkazy zajistit.

4.3 Zvláštnosti předmětu vyšetřování

V relativně nedávné minulosti byla představa o internetovém podvodu taková, že se jednalo převážně o případy s podvodným prodejem zboží, kde hrála významnou úlohu subjektivní stránka trestného činu podvod. V takových případech je zapotřebí prokazovat, že pachatel již při inzerci zboží jednal s úmyslem jej nedodat a získat podvodným prodejem finanční prostředky poškozeného. Samotný fakt nedodání zboží však neznamená naplnění všech znaků skutkové podstaty trestného činu. Pro prokázaní úmyslu je zapotřebí důkladně zkoumat okolnosti případu. Častým trikem podvodníku bylo to, že na inzertních serverech, kde se hodnotila spolehlivost prodejce,

získali kladná hodnocení prodejem levných věcí a teprve následně vytvořili nabídky na prodej drahých věcí, které již však nedodali.

Prvotní kritéria výzkumného souboru splňovalo 654 případů, ze kterých bylo 7 (1 %) případů odloženo, protože se nejednalo o trestný čin. V současné době tedy není prokazování subjektivní stránky stěžejním problémem u internetových podvodů, a to i z toho důvodu, že inzertní podvody tvoří 17 % ze zjištěných způsobů jednání pachatele.

Zásadní zvláštností předmětu vyšetřování internetových podvodů je to, že je potřeba využít i různé jiné metodiky vyšetřování.

Internetový podvod je podle provedeného výzkumu v 61 % případů spáchán v souběhu s jiným trestným činem, který má zpracovanou svou samostatnou metodiku vyšetřování. Souběh je dokonce ve 100 % případů kvalifikován u reverzního inzertního podvodu, investičního podvodu, phishingu a u výplaty falešného zisku.

Nejčastější právní kvalifikací společně s podvodem je trestný čin neoprávněné opatření, padělání a pozměnění platebního prostředku podle § 234 trestního zákoníku v 56 % případů a trestný čin neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací podle § 230 trestního zákoníku ve 48 % případů. Při vyšetřování internetových podvodů je tedy zapotřebí pracovat i s metodikou vyšetřování kybernetické kriminality.

Znalost metodiky vyšetřování legalizace výnosů z trestné činnosti je důležitá s ohledem na způsoby, jakým pachatelé zastírají původ peněz. Často využívaným způsobem je přeposílání finančních prostředků přes bankovní účty jiných poškozených osob. Ve velké míře jsou využíváni cizí státní příslušníci, kteří za úplatu založí bankovní účet, přestože se na zdrojovém trestném činu nepodílejí.

Jak nám ukazuje praxe u objasněných případů reverzních inzertních podvodů je potřebná znalost metodiky vyšetřování organizované kriminality a metodiku vyšetřování trestné činnosti páchanou cizinci. Zejména u inzertních reverzních podvodů a investičních podvodů se jedná o organizované skupiny cizinců, kteří páchají trestnou činnost ze zahraničí.

Další důležitou zvláštností předmětu vyšetřování je to, že se často jedná o sériovou trestnou činnost, kde může počet poškozených dosáhnout i několika tisíců. Běžně se jedná o desítky, stovky poškozených v jednom trestném činu. Provedeným

výzkumem jsme zjistili, že dílčí skutky byly zaznamenány u 24 % případů. Toto je ovšem způsobeno zejména tím, že byly zkoumány ukončené případy. Z celkového počtu 647 případů jich bylo ukončeno 340 (52 %). Zbylé případy byly zejména postoupeny ke společnému řízení, protože se jednalo o sériovou trestnou činnost rozsáhlejšího charakteru.

Vysoký počet dílčích skutků klade na zpracovatele vysoké nároky co do řízení, organizace a plánovaní vyšetřování. V případech s vysokým počtem poškozených je vhodná spolupráce s analytickým pracovištěm, které pomůže vyšetřovateli nashromážděná data strukturovaně a přehledně zpracovat.

Další zvláštností internetových podvodů jsou jejich jednotlivé atributy, jejichž lustrace v informačních systémech policie nám pomáhá slučovat případy, které spolu souvisí a tím vést řízení ve stejné věci na jednom místě a v množství nashromážděných dat hledat informace pro objasnění trestné činnosti.

4.4 Typické podněty a jejich zvláštnosti

Oznámení fyzických osob a poškozených institucí

Typickým podnětem u internetového podvodu je oznámení fyzické osoby nebo zástupce poškozené společnosti učiněné na policejní součásti. V 96 % výzkumného vzorku bylo oznámení přijato policejním orgánem a byly provedeny počáteční úkony. Ve třech případech bylo zasláno oznámení e-mailem a úkony byly provedeny až po výslechu oznamovatele a upřesnění informací. Určitou míru latence této trestné činnosti lze předpokládat u inzertních podvodů a u některých podvodů z kategorie jiné podvody. Bude se zejména jednat o takové podvody, kde nedošlo ke způsobení škody, která by zásadně ovlivňovala život poškozeného.

Jinak tomu bude u ostatních druhů podvodů, které jsou zamířeny na veškeré finanční prostředky obětí, a to včetně případných úvěrů, které jménem poškozených uzavřou sami pachatelé, případně úvěrů, které si sjednají sami poškození zejména u podvodu SCAM419. U těchto druhů podvodů se velká latence předpokládat nedá.

Operativně pátrací činnost Policie ČR

Prostředky operativně pátrací činnosti lze uplatňovat zejména u těch případů, kde pachatel jedná podle určité šablony, která umožňuje přijmout opatření k zabránění

trestné činnosti a odhalení pachatele. Může se například jednat o zakládání podvodných e-shopů, kde lze učinit opatření na straně registrátora domén. Dalším příkladem může být phishingový útok prostřednictvím zaslaných SMS zpráv a opatření na straně provozovatelů služeb umožňujících hromadné zasílání SMS. U inzertních podvodů se nabízí operativní rozpracování případu na základě všech příchozích plateb na bankovní, ale i jiný účet pachatele za účelem zjištění všech poškozených, tedy i těch, kteří podvod nenahlásili. U investičních podvodů se nabízí aktivní vyhledání podvodných investičních platforem a jejich operativní rozpracování.

Doba oznámení

Doba, která uplyne od spáchání podvodu do jeho oznámení je značně odvislá od způsobu jednání pachatele. Výzkum pracoval s dobou oznámení u všech 238 poškozených a jako průměrná doba, která uplynula od spáchání do oznámení byla nejčastěji v rozmezí od 1 do 6 měsíců od činu (45 %). Tento výsledek je zásadně ovlivněn tím, že 159 poškozených bylo u inzertních podvodů, kde může pachatel s poškozenými stále komunikovat a udržovat je v přesvědčení, že zboží bude doručeno. Nejdelší doba od spáchání podvodu do jeho oznámení je u podvodu typu Scam 419, kde 30 % případů je oznámeno v době od 6 do 12 měsíců. Toto je dáno tím, že pachatel využívá oběť ke svému soustavnému, ale postupnému obohacování a většina oběti čin oznámí až už je téměř nebo zcela bez prostředků.

Opačným příkladem jsou oběti, které oznamují skutek do 24 hodin. Jedná se o jednání typu: phishing (80 %), falešný bankéř (82 %). U falešného bankéře je 100 % případů oznámeno do týdne.

Oznámení skutku je tedy odvislá od toho, jestli poškozený zaslal finanční prostředky dobrovolně, kde se doba prodlužuje nebo o ně přišel náhle, kdy čin oznamuje poškozený téměř okamžitě.

Nesdělení podstatných informací

Mezi zvláštnosti podnětů můžeme zařadit nesdělení podstatných informací o průběhu činu. Z oznámení 238 poškozených bylo zjištěno, že v 5 % případů došlo k nesdělení podstatné informace. Týká se to všech způsobů jednání, do kterých vstupuje technologie jako důležitý, v podstatě klíčový prvek podvodu. Týká se to tedy těchto jednání: reverzní inzertní podvod, investiční podvod, phishing, výplata falešného zisku a falešný bankéř.

Nesdělenou informací je skutečnost o míře součinnosti, které poskytl poškozený pachateli k ovládnutí bankovního účtu. Takovou součinnost poskytl poškozený vždy. Ve většině případů výzkumného souboru důvod nesdělení nebyl zjišťován (55 %). V ostatních případech buď poškozený zapomněl nebo si nevzpomíná. Průběh činu lze zrekonstruovat z bankovních informací.

4.5 Typické počáteční vyšetřovací situace

U internetových podvodů se můžeme setkat s těmito počátečnímu vyšetřovacími situacemi (per analogiam k obecnému podvodu):

1. *„zjištěné skutečnosti nedovolují učinit jednoznačný závěr o totožnosti pachatele a nasvědčují tomu, že byl spáchán trestný čin,*
2. *zjištěné skutečnosti dovolují učinit jednoznačný závěr o totožnosti pachatele, nasvědčují tomu, že byl spáchán trestný čin, pachatel se však zdržuje na neznámém místě,*
3. *zjištěné skutečnosti dovolují učinit jednoznačný závěr o totožnosti pachatele, místě jeho pobytu a nasvědčují tomu, že byl spáchán trestný čin.“*[72]

Provedeným výzkumem bylo zjištěno, že u 5 (z 80) případů vystupoval pachatel pod svým jménem. Jednalo se zejména o inzertní podvody a jiné podvody. U těchto konkrétních případů bylo ve 4 (z 80) případech známo i místo pobytu pachatele. Všechny tyto případy byly objasněny.
Jak je patrno nejčastěji se setkáváme se stavem popsaným v bodě 1.
U všech výše uvedených vyšetřovacích situací je v počáteční etapě potřeba soustředit svou pozornost:

- zajištění výnosů z trestné činnosti,
- úkonům k zabránění pokračování trestného činu,
- zajištění komunikace s pachatelem,
- zjištění finančních toků,
- telekomunikačnímu provozu,
- ověření totožnosti pachatele.

[72] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4, str. 190.

Je nutné zdůraznit, že u všech vyšetřovacích situací, je nutné věnovat pozornost všem aspektů vyšetřování. Internetové podvody nemají klasické místo činu, interakce probíhá v on-line prostoru a shromážděné informace nám poskytují indicie vedoucí k pachateli. Zdánlivá jednoznačnost získaných informací je relativní. Bankovní účet lze založit on-line na doklady, které pachatel vylákal od jiné osoby nebo je získal v kyberprostoru. Místo odkud pachatel vedl komunikaci zjištěné podle IP adresy, může být pouze místem, kde se nachází škodlivým kódem nakažený počítač a jeho uživatel nemá s trestnou činností nic společného.

U internetových podvodů se můžeme setkat po sdělení obvinění konkrétní osobě s těmito typickými vyšetřovacími situacemi (per analogiam k obecnému podvodu):

1. *„obviněný trestnou činnost doznává,*
2. *obviněný trestnou činnost zcela popírá,*
3. *obviněný doznává jednání, popírá však úmysl uvést někoho v omyl nebo využití omylu poškozeného,*
4. *obviněný odmítá vypovídat.“*[73]

Pro všechny čtyři situace platí, že je nutné věnovat pozornost důkladnému zjišťování a zajišťování všech pramenů důkazů, protože ve své podstatě u internetových podvodů neexistuje přímý usvědčující důkaz o činnosti pachatele, tak jak to může být u případů s fyzicky existujícím místem činu, a proto je nutné utvářet ucelené řetězce nepřímých důkazů svědčící o vině obviněného. Určitou výjimku o přímém usvědčujícím důkazu mohou tvořit případy, kde byly nasazeny operativně pátrací prostředky, které dokumentovaly právě probíhající trestnou činnost konkrétních osob.

Přestože by tomu tak být nemělo, může přiznání pachatele vyšetřovatele odradit od provedení nabízejících se úkonů. Kritickým bodem potom může být odvolání přiznání pachatele v čase, kdy již není možné některé důkazy opatřit (např. propadnutí lhůty 6 měsíců pro uchovávání provozních a lokalizačních údajů) a již není možné vytvořit ucelený řetězec nepřímých důkazů svědčící o vině obviněného.

[73] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4, str. 191.

4.6 Zvláštnosti počátečních úkonů a opatření

Počáteční úkony a opatření můžeme u internetových podvodů i s ohledem na provedený výzkum stanovit takto:

- výslech poškozeného (přijetí oznámení o trestném činu),
- zajištění věcí a písemností předaných oznamovatelem,
- předložení/vydání věci,
- ohledání předložených/vydaných věcí,
- zajištění digitálních stop
- zajištění výnosů z trestné činnosti,
- zabránit pachateli v dalším pokračování trestné činnosti,
- zajištění souhlasu ke zjištění údajů o telekomunikačním provozu,
- zajištění souhlasu ke zjištění bankovních informací.

Výslech poškozeného

Výslech poškozeného hraje ve vyšetřování internetových podvodů důležitou roli. Poškozený byl v kontaktu s pachatelem a jsou mu známy okolnosti podvodu. Zásadní význam je v případech, kdy došlo pouze k telefonickému hovoru. Výslech poškozeného by měl být proveden tak, aby byly zjištěny tyto informace:

1. datum a čas prvotního kontaktu, včetně vymezení zařízení použitých ke komunikaci a místa odkud komunikoval poškozený,
2. vymezení důvodu proč byla komunikace započata
    - inzerát, investování, reklama, zaslána SMS/e-mail zpráva, internetový odkaz, volání z banky apod.
    - přesná identifikace podnětů, které vedly k důvodu komunikace (číslo inzerátu, přesná adresa internetové stránky investiční společnosti apod.),
3. informace o komunikaci
    - použitý komunikačním prostředek: volání, e-mail, WhatsApp, Messenger, chat použité služby apod.,
    - uvedení, data, času a obsahu komunikace,
    - identifikátory komunikačního prostředku (např. přesný název facebookového profilu, nestačí pouze zobrazené jméno, tzv. display name,

který neumožňuje konkrétní identifikaci subjektu u společnosti provozující využitou službu komunikace),

4. pod jakým jménem pachatel vystupoval, jaké uváděl kontakty a jakých z těchto kontaktů využil ke komunikaci,
5. informace o činnostech provedených na základě komunikace
    - přesný popis toho co pachatel žádal, za jakým účelem a co mu bylo poskytnuto jako např. objednávka zboží, předání informace, předání autentizačního kódu, předání přístupových údajů, instalace programu na vzdálenou zprávu apod.,
    - u obdrženého fyzického předmětu uvést popis a jak s ním bylo naloženo,
6. informace o zaslaných finančních prostředcích
    - použité platební metody (platební karta, bankovní převod, mobilní platby, služby převodů peněz apod.)
    - veškeré konkrétní údaje, které byly pro platbu použity (výška převedené finanční částky, datum a čas transakce, číslo účtu, variabilní číslo, jméno a příjmení příjemce platby apod.),
7. jaké konkrétní kroky poškozený podniknul, když pojal podezření, že se stal obětí podvodu.

Zajištění věcí a písemností předaných oznamovatelem

Pokud poškozený předloží tištěné písemnosti nebo elektronické soubory dokumentující průběh činu, policejní orgán je zajistí. Takto zajištěné informace se mohou týkat proběhlé komunikace, potvrzení o proběhlých finančních transakcích apod. Na základě těchto přesných informacích mohou být přijímána správná neodkladná opatření. Eliminuje se pochybení vzniklé nepřesnými informacemi zjištěnými pouze z paměťové stopy poškozeného.

Předložení/vydání věci

Předložení/ vydání věci se může týkat věcí zaslaných pachatelem poškozenému nebo také zařízeních, které byly použity během komunikace. Je potřeba rozlišovat, jestli se věc předkládá za účelem ohledání a není ji potřeba zajistit pro účely trestního řízení nebo se věc vydává nejenom za účelem ohledání, ale i jejího zajištění.

Ohledání předložených/vydaných věcí

Pokud se ohledává věc zaslaná pachatelem, je vhodné k takovému úkonů přizvat kriminalistického technika za účelem vyhledání a zajištění stop po pachateli. Může se jednat o daktyloskopické stopy, biologické stopy, mikrostopy apod. Vyhodnocení těchto stop může být využito v dalším procesu dokazování.

Zajištění digitálních stop

Digitální stopy mohou být zajištěny z předložených zařízeních nebo ze služeb. Podle náročnosti úkonů může digitální stopy zajistit policejní orgán provádějící výslech poškozeného, kriminalistický IT specialista[74] (policista oprávněný na základě vydaného osvědčení provádět kriminalistickotechnické úkony při zajišťování výpočetní techniky a digitálních stop), kriminalistický znalec.

Zajištění výnosů z trestné činnosti

Zajištění výnosů z trestné činnosti provádí policista, který vede řízení, kde byla způsobena majetková újma či získán majetkový prospěch[75]. Procesně je postup upraven v § 79a trestního řádu. Úkon provádíme jako neodkladný, protože zde hrozí nebezpečí přesunu finančních prostředků jinam. Úkon není prováděn pouze za účelem zajištění výnosu trestné činnosti, ale i k zabránění pokračování trestné činnosti.

Zabránit pachateli v dalším pokračování trestné činnosti

„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.“[76]

Tento postup je účelné využít ve všech případech, kdy je prostřednictvím internetu přístupná informace, která může vést ke vzniku dalších poškozených (falešný e-shop, falešná stránka banky apod.). Ve výzkumném souboru nebyl tento postup použit.

Další možností je výše popsaný postup podle § 79a trestního řádu.

---

[74] POKYN policejního prezidenta č. 100/2018, *o kriminalistickotechnické činnosti* v posledním znění, čl. 5, odst. 1 písm. d).
[75] ZÁVAZNÝ POKYN policejního prezidenta č. 174/2011, *k provádění finančního šetření v trestním řízení* v posledním znění, čl. 3.
[76] Zákon č. 141/1961 Sb., *o trestním řízení soudním* (*trestní řád)* v posledním znění, § 7b.

Zajištění souhlasu ke zjištění údajů o telekomunikačním provozu

Postup, jehož využití zajistí bezodkladné zjištění údajů o uskutečněném telekomunikačním provozu a umožní nám vést rychlé a efektivní vyšetřování. Je potřeba mít neustále na paměti, že doba uchovávání těchto údajů je zákonem omezena na 6 měsíců. Zásadní význam má při využití podvodné techniky spoofingu, při které je použita technologie, u které operátoři drží potřebná data pro vystopování zdroje po velmi omezenou dobu.

Zajištění souhlasu ke zjištění bankovních informací

Postup, jehož využití zajistí bezodkladné zjištění údajů o uskutečněných bankovních transakcích a umožní nám vést rychlé a efektivní vyšetřování. Dále nám tyto informace pomáhají přesně rekonstruovat jednání pachatele a poškozeného ve vztahu k ovládnutí účtu pachatelem. Zejména je zapotřebí zjistit tyto informace:

- identifikace bankovního účtu: číslo účtu, majitel a disponent, další identifikační údaje,
- výpis bankovního účtu,
- logovací soubory s uvedením přesných časů připojení, IP adres, ze kterých došlo k připojení k bankovnímu účtu,
- popis prováděných činností,
- datum, čas, příjemce, znění zaslaných SMS a autorizačních zpráv (včetně popisu potvrzovaných činností),
- seznam zařízení, kde bylo aktivováno mobilní bankovnictví/smartbanking,
- identifikátor SEID (slouží k identifikaci zařízení, které byly použity při bezkontaktních platbách).

4.7 Zvláštnosti následných úkonů

Počáteční úkony a opatření můžeme u internetových podvodů i s ohledem na provedený výzkum stanovit takto: výslech poškozeného, výslech obviněného, domovní prohlídka, předložení/vydání věci, zjištění SIM/IMEI, telekomunikační provoz, žádost do zahraničí, právní pomoc, zajištění digitálních stop, kriminalistická expertíza, zajištění výnosů z trestné činnosti, bankovní informace, analýza atributů.

Výslech obviněného

Výslech obviněného klade na vyšetřovatele zvýšené nároky na znalosti v oblasti informačních a komunikačních technologií, zejména u těch typů podvodů, které byly páchány za výrazného použití technického prvku. Osoba pachatele je většinou technicky zdatná, zakrývá informace o provedení činu a své technické znalosti může využívat k popření své viny. Z tohoto důvodu je vhodné věc předem konzultovat s IT specialistou nebo znalcem v oblasti počítačové expertizy nebo výpočetní techniky. Výslech obviněného u inzertních podvodů, podvodů SCAM419 a u některých podvodů řazených pro účely této práce jako „jiné“ se v zásadě neliší od výslechu osoby obecného podvodu. U podvodů s nedodáním zboží nebo zbožím jiné kvality je zejména nutné důkladně zadokumentovat subjektivní stránku trestného činu.

Domovní prohlídky

Důvody domovních prohlídek, osobních prohlídek a prohlídek jiných prostor a pozemků jsou stejné jako u jiných trestných činů a způsob jejich provedení je dán trestním řádem.

Věcí důležitou pro trestní řízení jsou zejména:

- počítačové systémy (PC, notebooky, servery, routery apod.),
- komunikační technika (mobilné telefony, SIM karty apod.),
- hmotné nosiče dat (USB disky, HDD disky, optická média apod.).

Během prohlídek je potřeba se soustředit na všechnu dostupnou techniku, a ne pouze na aktuálně využívanou. Je nutné dbát na správné zajišťování, dokumentaci a balení. U systémů v zapnutém stavu je potřeba brát v úvahu připojení do cloudu nebo služeb a přijmout opatření k zajištění jejich obsahu. U všech zařízení, které jsou proti neoprávněnému přístupu chráněny zabezpečením je nutné zjistit přístupové údaje.

Vzhledem k technické náročnosti při zajišťování je vhodné úkony provádět s IT specialistou, kriminalistickým expertem případně znalcem.

Telekomunikační provoz

Telekomunikačnímu provozu jsme se již podrobně věnovali v kapitole o typických stopách a jiných soudních důkazech. V této etapě vyšetřování je nutné realizovat případný souhlas ke zjištění údajů o telekomunikačním provozu, případně podat dozorovému státnímu zástupci podnět k podání návrhu na vyžádání takových

informací u příslušného soudu. Je nutné mít neustále na paměti, že délka uchovávání takových informací je 6 měsíců. Můžeme zjistit nejenom telekomunikační provoz konkrétního účastníka hlasové služby nebo informace ke koncovému přípojnému bodu podle IP adresy, ale i provoz na označení základnové stanice Start a základnové stanice Stop (tzv. buňky). Jedná se o místa jejímž prostřednictvím je uživatel připojen do veřejné komunikační sítě při zahájení komunikace a při jejím ukončení.[77]

Právní pomoc a žádosti do zahraničí

Jak ukázal výzkum 84 % případů má zahraniční přesah. Tímto přesahem myslíme: zahraniční bankovní účet příjemce peněz, zahraniční služby převodu peněz, pachatelé vystupující pod identitou osob ze zahraničí, použití zahraničních telefonních čísel, zahraniční IP adresy, zahraniční poskytovatelé komunikátorů, zahraniční držitelé a provozovatelé internetových domén, zahraniční poskytovatelé webhostingu, zahraniční inzertní servery apod.

Získání informací postupem podle zákona o mezinárodní justiční spolupráci ve věcech trestních bylo použito v 16 % případů. Nejčastěji jsou zjišťovány bankovní informace. U internetových podvodů lze v případech, kde je pro účely trestního řízení zapotřebí zajistit urychlené uchování dat uložených v počítačovém systému nebo na nosiči informací, který se nachází na území cizího státu požádat o uchování takových dat.[78]

Vyšetřovatelé však používají i způsob přímého oslovení zahraničního subjektu a to ve 48 % případů. Může se jednat o zahraniční destinace, kde nemá Česká republika smlouvou upravenou spolupráci ve věcech trestních. Země se špatnou vymahatelností práva. Může se však jednat i o velké globální poskytovatele služeb, které informace poskytují sice na povolení soudu, ale příslušný příkaz je zaslán policejní cestou přes určený národní styčný bod. U případů výzkumného souboru nebyla využívána spolupráce policejních orgánů z jiných členských států.

Kriminalistická expertiza

„Kriminalistická expertiza chápaná jako metoda kriminalistické praktické činnosti a využívaná k odhalování a zkoumání stop a jiných důkazů a dekódování kriminalisticky, resp. důkazně relevantní informace, je pramenem důkazů v trestním

[77] Vyhláška č. 357/2012 Sb., *o uchovávání, předávání a likvidaci provozních a lokalizačních údajů* v posledním znění, § 1.
[78] Zákon č. 104/2013 Sb., *o mezinárodní justiční spolupráci ve věcech trestních* v posledním znění, § 65a.

řízení.“[79] Za experta je pak považován pracovník s náležitou kvalifikací a specializací, mající oprávnění k expertní činnosti a působící na Kriminalistickém ústavu Policie ČR nebo na některém z odborů kriminalistické techniky a expertiz krajských ředitelství Policie ČR.[80]

Provedeným výzkumem bylo zjištěno, že ani v jednom z případů nebyla provedena kriminalistická expertiza podle výše uvedeného vymezení. Ve všech případech byly zajištěny pouze digitální stopy.

Digitální stopy byly zajišťovány zejména kriminalistickým IT specialistou, který svou činnost provádí na základě vydaného osvědčení (viz kapitola Zvláštnosti počátečních úkonů a opatření**)** a má nejblíže k výše uvedenému vymezení experta.

Digitální stopy byly dále zajišťovány policisty provádějící prvotní úkony. Digitální stopou u internetových podvodů rozumíme v počáteční etapě zejména komunikaci mezi pachatelem a obětí, případně pachatelem nainstalované programy do zařízení poškozeného, jako např. program na vzdálenou zprávu zařízení. Pokud je zjištěn pachatel zajišťujeme digitální stopy v zařízeních pachatele.

Pro použití digitální stopy jako důkazu před soudem je rozhodující zajištění její integrity. Z tohoto důvodu je nutné, aby byl celý průběh zajištění řádně dokumentován, protokolován a integrita digitální stopy byla zajištěna výpočtem kontrolního součtu příslušného algoritmu.

Forenzní digitální analýza

Forenzní digitální analýza je druhem expertizy podle druhu odborných znalostí. Forenzní analýza zajištěných digitálních stop byla provedena v 9 % případů, a to kriminalistickým IT specialistou. Převážně se jednalo o ty situace, kde byl zjištěn program na vzdálenou zprávu zařízení poškozeného, k jejichž analýze je již potřeba specifických technických znalostí. V ostatních případech byla provedena zejména analýza proběhlé komunikace, která byla v digitální podobě získána ze zařízení nebo služeb. Tento druh analýzy provedl vyšetřovatel případně analytik.

[79] PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. aktualiz. a rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2, str. 560.
[80] Tamtéž, str. 560.

Bankovní informace a jiné informace k převodům peněz

Bankovní informace byly zjišťovány v 80 % případů. U ostatních případů byly zjišťovány informace o finančním toku u nebankovních institucí.

Bankovní instituce

Zjišťujeme tyto informace:

- identifikace bankovního účtu: číslo účtu, datum založení, majitel a disponent, další identifikační údaje,
- seznam platebních, kreditních a předplacených karet,
- výpis bankovního účtu,
- logovací soubory s uvedením přesných časů připojení, IP adres, ze kterých došlo k připojení k bankovnímu účtu,
- popis prováděných činností,
- datum, čas, příjemce, znění zaslaných SMS a autorizačních zpráv (včetně popisu potvrzovaných činností)
- seznam zařízení, kde bylo aktivováno mobilní bankovnictví/smartbanking,
- identifikátor SEID (slouží k identifikaci zařízení, které byly použity při bezkontaktních platbách).

Rozsah zjišťovaných informací se může lišit podle postavení majitele účtu a činností, které byly provedeny.

Nebankovní sektor

Za nebankovní sektor považujeme finanční instituce, které obchodují s penězi, ale nejsou bankami, tedy nemají bankovní licenci ani bankovní dohled. Informace od těchto subjektů tedy nepodléhají bankovnímu tajemství a policejní orgán je může vyžadovat samostatně bez státního zástupce, i bez souhlasu oprávněného majitele účtu.

Setkáváme se nejčastěji s využitím služeb:

- služby převodu peněz,
- kryptoměnová burza,
- služby card-to-card: převod peněz mezi debetními, kreditními nebo předplacenými kartami.

Služby převodu peněz jsou využívány zejména pro jejich okamžitost a možnost sjednání on-line. Tyto vlastnosti pachatelé zneužívají k založení účtů u služby převodu peněz pod falešnou identitou.

Služby převodu peněz, které jsou zneužívány podvodníky, nemají ve většině případů sídlo nebo zastoupení na území České republiky a pro získání informací je nutná žádost do zahraničí.

Zjišťujeme podobné informace jako u účtů v bankovním sektoru:

- identifikace účtu: číslo účtu, datum založení, majitel a disponent, další identifikační a registrační údaje,
- výpis účtu,
- logovací soubory s uvedením přesných časů připojení, IP adres, ze kterých došlo k připojení k účtu,
- seznam zařízení, které bylo využito při používání služby,
- identifikátor SEID (slouží k identifikaci zařízení, které byly použity při bezkontaktních platbách).

Konkrétní příklad ilustrující problematické aspekty sledování finančních toků. Finanční prostředky poškozeného směřovaly k zahraničnímu obchodníkovi na nákup kryptoměny. Účet u obchodníka byl sice ověřen na základě zaslaných osobních dokladů, ale jednalo se o upravené (padělané) doklady jiné osoby. Nakoupená kryptoměna poté směřovala na adresu u asijské kryptoměnové burzy, kde byl držitel adresy ověřen pouze na základě identifikátoru u služby instant messaging, která nespolupracuje s orgány činnými v trestním řízení.

Analýza atributů

U internetových podvodů je více než u jiných druhů trestných činů důležitá analýza atributů trestného činu. Atributem rozumíme typický znak nebo vlastnost, který nám zakládá domněnku, že pokud se objevuje u jednání se shodným způsobem provedení, tak za ní může stát stejný pachatel. Analýza atributů byla provedena ve 100 % případů.

Rozlišujeme jednoznačné atributy nebo nepřímé atributy.

Jednoznačný atribut – zakládá důvod pro vedení společného řízení o všech útocích pokračujícího trestného činu.

Nepřímý atribut – více nepřímých atributů může zakládat důvod pro vedení společného řízení o všech útocích pokračujícího trestného činu.

Co je chápáno jako jednoznačný atribut, nám ukazuje kriminalistická praxe a vždy záleží na způsobu provedení. Stejný atribut může být chápán u jednoho způsobu provedení podvodu jako jednoznačný a jiného způsobu již ne.

Mezi atributy pro společné řízení můžeme řadit:

- osoba pachatele,
- identifikátory komunikace: telefonní číslo, jednoznačný identifikátor u instant messaging (pozor na zobrazené display name, které není jednoznačným identifikátorem), ostatní komunikační aplikace, e-mailová adresa apod.,
- identifikátory toků finančních prostředků: číslo bankovního účtu, adresa kryptopeněženky, osoba legalizátora,
- identifikátory zařízení: IMEI mobilních zařízení, číslo SEID, výrobní číslo,
- IP adresa,
- webový odkaz, doména,
- soubory zasílané pachatelem: osobní doklady, různé fotografie, kupní smlouvy apod.,
- specifický způsob provedení,
- registrační a identifikační údaje.

Dalším problematickým aspektem je zakládání účtů u bankovních i nebankovních institucí tzv. „finančními mulami“ a následné několikanásobné přeposlání finančních prostředků, které znesnadňuje nebo přímo znemožňuje jejich dohledání.

Doba rozhodnutí ve věci

Provedený výzkum zkoumal i dobu, která trvala od oznámení do rozhodnutí ve věci nebo sdělení obvinění. U ukončených případů se nejčastěji jednalo o případy, kde bylo takové rozhodnutí vydáno do 6 měsíců.

Praxe nám však ukazuje, že vyšetřování může trvat i několik let, a to zejména s ohledem na počet dílčích skutků pokračujícího trestného činu podvod.

4.8 Zvláštnosti zapojení veřejnosti do vyšetřování

Zkušenosti ukazují, že zapojení veřejnosti do vyšetřování, je na značně nízké úrovni. Svým způsobem je to logické, protože neexistuje žádné lokální místo, kde byl trestný čin spáchán. Poškození jsou z celého území státu nebo i ze zahraničí. Pachatel trestnou činnost páchá v soukromí a není pod dohledem veřejnosti.

Zapojení veřejnosti je ovšem nesmírně důležité, dalo by se říct klíčové u preventivních programů, které mají veřejnost vzdělávat. Osoba, která si je vědoma rizik a podvodných technik, se nestane obětí internetového podvodu. Příklad informačního letáku umístěného Krajským ředitelstvím policie Zlínského kraje u vkladového bitcoinmatu ve městě Zlíně je uveden v příloze (Příloha 2).

4.9 Aktuální problémy praxe při vyšetřování internetových podvodů

U internetových podvodů je možno rozdělit problémy praxe do těchto bodů:

1. zahraniční přesah,
2. bankovní služby, služby převodu peněz, kryptoměna,
3. rozsah páchané trestné činnosti, slučování skutků,
4. falšování identity on-line,
5. technologická úroveň znalostí u oběti a její osobnostní rysy,
6. technologická úroveň znalostí u orgánů činných v trestním řízení.

Zahraniční přesah

Zahraniční přesah omezuje možnosti vyšetřovatele rychle a pružně reagovat na nastalou vyšetřovací situaci. Vyžadování důkazních informací ze zahraničí provedené jednou z forem mezinárodní justiční spolupráce (právní pomoc, evropský vyšetřovací příkaz) je časově náročné. Množství dějů, které se odehrávají on-line a na které je nutné okamžitě reagovat je nepřeberné množství. Možnosti spolupráce policejních orgánů z jiných členských států jsou omezené zejména s ohledem na použití takových informací jako důkazu. Tato možnost je sice upravena v § 20 zákona č. 104/2013 Sb., o mezinárodní justiční spolupráci ve věcech trestních, ale praxe nám ukazuje, že není v členských nebo přidružených státech příliš akceptována. Výhoda policejní spolupráce je zejména v rychlosti získaných informací.

Další kapitolou zahraničního přesahu je nemožnost získat informace ze zemí se špatnou vymahatelností práva nebo zemí, se kterými není spolupráce upravena mezinárodními smlouvami.

Příklady problematických aspektů informací získaných ze zahraničí:

- výpověď majitele účtu v zahraničí můžeme jen obtížně ověřit, dát ji do širších souvislosti s jeho kriminální minulostí nebo jej operativně rozpracovat,
- zjištění o koncovém přípojném bodu podle IP adresy – zde je nutné provést šetření nejenom k účastníkovi smlouvy o připojení, ale i všem osobám, které připojení využívají.

Tyto úkony můžeme očekávat u organizované zločinecké skupiny s mezinárodním přesahem, ale u tisíců jednotlivých případů, kde se takový prvek objeví, je jejich použití problematické

Protiopatření: důslednost vyšetřovatele při zjišťování informací ze zahraničí.

Bankovní služby, služby převodu peněz, kryptoměna

Sledování finančních toků peněz od poškozeného k pachateli je problematické z několika důvodů:

- založení bankovního účtu, služby na falešnou identitu,
- využívání velké sítě osob legalizující finanční prostředky, nebo osob do legalizace nevědomě zapojených (pachatelem ovládnutý bankovní účet poškozeného),
- vytváření dlouhých řetězců pro přesuny finančních prostředků,
- anonymita kryptoměny,
- zapojení zahraničních bankovních ústavů a poskytovatelů služeb.

Protiopatření:

- důslednost vyšetřovatele při prověřování všech finančních toků,
- důslednost vyšetřovatele při prověřování všech osob zapojených do legalizace, protože tyto osoby někdo kontaktoval, dal jim instrukce a ony zase finanční prostředky někam převádí nebo někomu předávají.

Tento přístup vyžaduje trpělivost, systematickou práci s daty a případně i nasazení operativně pátracích prostředků.

Rozsah páchané trestné činnosti, slučování skutků

Problematickým aspektem u některých popsaných způsobů jednání pachatele je velké množství poškozených. Případy jsou přijímány napříč celým územím České republiky a zpočátku není ani jasné, že se jedná o rozsáhlou trestnou činnost. U internetových podvodů je více než u jiných druhů trestných činů důležitá analýza atributů trestného činu, podrobně již popsáno v kapitole 4.7. V některých případech je obtížné stanovit, který policejní orgán je příslušný ve věci vést společné řízení a dochází k přeposílání a vracení spisů a sporům o příslušnost. Tyto postupy ve svém důsledku omezují ofenzívnost vyšetřování, protože jsou případy takříkajíc pořád někde na cestě.

Protiopatření: v případě detekce případu s větším počtem poškozených vydání koordinačního přípisu, který jasně stanoví, který policejní orgán bude věc vyšetřovat a jaké jsou před sloučením věci požadavky na provedení úkonů.

Falšování identity on-line

V současné době neexistuje identifikátor, který by jednoznačně určoval osobu, která činnost na internetu provedla. I když jsou přijímána různá opatření, která mají přispět k tomu, aby byla nade vši pochybnost zřejmá on-line identita, vždy tu bude člověk, který svou identitu spravuje a může ji tedy po vhodné manipulaci pachateli poskytnout. To nám prokázal provedený výzkum u jednotlivých druhů podvodných jednání, kdy poškození umožnili ovládnout své bankovní účty a vůči bance poté vystupovali pachatelé jako oprávněné osoby.

Protiopatření: edukace celé společnosti, tak aby rozuměla technologiím a ochraně své on-line identity.

Technologická úroveň znalostí u oběti a její osobnostní rysy

Technologická úroveň znalostí oběti se projevuje zejména u těch způsobů jednání pachatele, kde by bez součinnosti oběti nedošlo ke spáchání trestného činu. Poškození v mnoha případech nevěděli, že svojí činností umožňují pachateli ovládnout svůj bankovní účet. Dalším důležitým aspektem jsou osobnostní rysy oběti jako je: přílišná důvěřivost až lehkomyslnost, vidina rychlého a snadného zisku.

Protiopatření: edukace celé společnosti, tak aby rozuměla technologiím (např. fungování on-line bankovnictví) a nepřetržité mediální upozorňování na rizika internetových podvodů.

Technologická úroveň znalostí u orgánů činných v trestním řízení

Obsahovou analýzou bylo zjištěno, že u některých případů nebyly provedeny úkony, které se nabízely a které být provedeny měly. Dále byly zjištěny případy, kde nebyly správně vyhodnoceny a interpretovány získané informace.

Protiopatření: edukace orgánů činných v trestním řízení, za účelem zvýšení technologické úrovně jejich znalostí, tak aby rozuměli způsobům, jak získat informace pro odhalení pachatele a jak jim správně porozumět.

ZÁVĚR

Cílem této diplomové práce bylo popsat a stanovit typický model kriminalistické metodiky vyšetřování internetových podvodů. Domnívám se, že s ohledem na rozsah diplomové práce bylo požadovaného cíle dosaženo a byly splněny všechny požadavky, které jsou na zpracování takové metodiky kladeny.

První kapitolu diplomové práce jsem věnoval teorii metodik vyšetřování. Za využití odborné literatury jsem popsal teoretické základy, funkci, systém a strukturu vyšetřování, typovou kriminalistickou charakteristiku a zásady metodiky vyšetřování. Ve druhé kapitole jsem vymezil základní pojmy, které jsou důležité pro pochopení předkládaných informací a velkou část jsem věnoval popisu jednotlivých způsobů jednání pachatele při páchání internetových podvodů.

Výzkumnou část jsem věnoval rozsáhlému terénnímu šetření věnovanému obsahové analýze vyšetřovacích spisů u případů internetových podvodů, které byly spáchány v období od 1.1.2022 do 31.12.2022 na teritoriu Krajského ředitelství policie Zlínského kraje. Počáteční kritéria výzkumného souboru splňovalo 654 případů. K vymezení kriminalistické charakteristiky u znaku způsobu jednání pachatele, bylo analyzováno 647 případů. Bylo zjištěno celkem 8 typických způsobů jednání a to: reverzní inzertní podvod, inzertní podvod, investiční podvody, phishing, výplata falešného zisku, SCAM419, falešný bankéř a jiné podvody. Na zjištění dalších znaků kriminalistické charakteristiky byl vybrán vzorek 80 případů. Pro mnohé čtenáře bude jistě překvapením, že klasický inzertní podvod, který je spojený s nabídkou zboží k prodeji byl zastoupen pouze v 17 % případů. Jedná se o jediný typ podvodu, kde se objasněnost blíží k celorepublikovému průměru všech objasněných trestných činů a dosahuje 37 %. Mimo podvody definované jako „jiné“, kde je objasněnost 11 %, je u všech ostatních způsobů objasněnost 0 %. Zapojení zahraničního prvku bylo zjištěno u 67 případů a úskalí spojená s vyšetřováním takové situace se promítla do zjištění, že byl objasněn pouze 1 případ, který měl zahraniční přesah.

Za zásadní zjištění považuji to, že cílem pachatelů není jako v minulosti pouze připravit poškozené o finanční prostředky zaslané poškozeným v určité výši, ale připravit poškozeného o všechny jeho dostupné finanční prostředky včetně těch, které nečerpal, protože jsou uloženy v předschválených úvěrech. Taková trestná činnost má v některých případech devastující dopad na život poškozených, protože nejenom, že

přišli o celoživotní úspory, ale ještě musí splácet pachatelem uzavřené úvěry. Provedený výzkum se zabýval i dalšími komponenty struktury metodik vyšetřování, které byly podrobeny důkladné obsahové analýze a prezentování zjištěných výsledků.

Poslední kapitola je věnována popisu a stanovení typického modelu kriminalistické metodiky vyšetřování internetových podvodů. V této části práce jsem propojil část teoretickou a empirickou a došlo ke spojení kriminalistické vědy s praxí. Práce je zpracována tak, aby obsáhla jednotlivé komponenty z teorie struktury vyšetřování. Byla doplněna o zjištění z terénního šetření a o vlastní zkušenosti, které jsem nabyl mnohaletou praxí. Dále se zabývám zapojením veřejnosti do vyšetřování, kdy její úlohu spatřujeme především v její edukaci, aby byla informována o nejčastějších tricích podvodníků, což má mít za následek snížení počtu trestných činů. Závěrem popisuji aktuální problémy praxe a navrhuji protiopatření ke zlepšení stavu.

Jsem si vědom toho, že terénní šetření bylo provedeno na úrovni jednoho ze 14 krajských ředitelství policie České republiky, a proto je zde prostor předkládané výsledky dále verifikovat celorepublikovým šetřením prováděným po více let.

Není to tak dávno, kdy k vyšetřování internetových podvodů postačovala s jistou dávkou nadsázky znalost trestního zákoníku, trestního řádu, zákona o elektronických komunikacích, porozumění základním pojmům jako je IP adresa a s tím spojená schopnost potřebné informace umět vyžádat, správně jim porozumět a využít je k objasnění věci. Pro praktické vyšetřování případu to znamenalo: vyžádat informace od provozovatele českého inzertního portálu, vyžádat bankovní informace (většinou přímá platba poškozený – pachatel), zjistit další poškozené, zjistit informace k IP adrese, a to vše především na území ČR.

Postupem doby se, ale začala situace měnit. Mezi hlavní faktory změny můžeme řadit: nárůst počtu používaných technologií a jejich uživatelů (např. on-line banking), nárůst počtu spáchaných trestných činů, anonymizace pohybu na internetu, falšování identity on-line, zapojení zahraničního prvku, poskytování nebankovních finančních služeb, možnost sjednání bankovních i ostatních účtů on-line, využívání virtuálních měn, zastírání původu peněz opakovanými převody mezi bankovními účty či mezi službami nebankovních finančních služeb, zapojení celého řetězce osob legalizující výnosy z trestné činnosti apod.

Výše uvedené faktory mají vliv na množství dat, které je zapotřebí správně řadit, rozumět jim a chápat je v širších souvislostech případu. K získání dat je nutné znát správné postupy, které se dříve nepoužívaly (např. Google, služby spol. Meta). Je nutné chápat fungování rozličných služeb komunikačních, finančních nebo také fungování kryptoměny, kde často mizí výnosy z trestné činnosti.

To vše klade na vyšetřovatele nové požadavky na znalosti analytické technologické a právní.

Problematika internetových podvodů je problematikou dynamicky se rozvíjející a je potřeba, abychom byli na její úskalí připraveni například vytvořením této metodiky vyšetřování internetových podvodů.

Věřím, že touto prací jsem přispěl k lepšímu pochopení toho, co všechno si lze představit pod internetovými podvody a že vypracovaná metodika přispěje k lepším výsledkům při odhalování a vyšetřování trestné činnosti na úseku internetových podvodů.

SEZNAM POUŽITÉ LITERATURY

Monografie

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.

GŘIVNA, Tomáš, Radim POLČÁK et al. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. ISBN 978-80-903786-7-4.

JELÍNEK, Jiří a kolektiv. *Trestní právo hmotné. Obecná část. Zvláštní část*. 8. aktualiz. vyd. Praha: Nakladatelství Leges, 2022. ISBN 978-80-7502-576-0.

JIROVSKÝ, Václav. *Kybernetická kriminalita*. Praha: Grada Publishing, 2007. ISBN 978-80-247-1561-2.

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.

KOLOUCH, Jan, Pavel BAŠTA a kol. *Cybersecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4.

KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika. Teorie, metodologie a metody kriminalistické techniky*. 2. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-869-3.

MITNICK, Kevin a William SIMON. *Umění klamu*. Gliwice: Nakladatelství Helion, 2002. ISBN 83-7361-210-6.

MUSIL, Jan, Zdeněk KONRÁD a Jaroslav SUCHÁNEK. *Kriminalistika*. Praha: C. H. Beck, 2001. ISBN 80-7179-362-0.

MUSIL, Jan, Zdeněk KONRÁD a Jaroslav SUCHÁNEK. *Kriminalistika*. 2. přeprac. a dopl. vyd. Praha: C. H. Beck, 2004. ISBN 80-7179-878-9.

NĚMEC, Miroslav et. al. *Teorie a metodologie kriminalistiky pro magisterské studium – I. díl. Aktuální problémy kriminalistické teorie*. Praha: ABOOK, 2018. ISBN 978-80-906974-1-6.

NĚMEC, Miroslav et. al. *Teorie a metodologie kriminalistiky pro magisterské studium – II. díl. Aktuální problémy kriminalistické praxe*. Praha: ABOOK, 2019. ISBN 978-80-906974-2-3.

NOVOTNÝ, František, Josef SOUČEK et al. *Trestní právo hmotné*. 3. rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-291-2.

PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. 2. aktualiz. a rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. rozš a aktualiz. vyd. Plzeň: Nakladatelství a vydavatelství Aleš Čeněk, 2022. ISBN 978-80-7380-849-5.

STRAUS, Jiří, Viktor PORADA a kol. *Teorie, metody a metodologie kriminalistiky.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2017. ISBN 978-80-7380-666-8.

ŠÁMAL, Pavel, Tomáš GŘIVNA, Lukáš BOHUSLSV, Oto NOVOTNÝ, Jiří HERCEG et al. *Trestní právo hmotné*. 9. vyd. Praha: Wolters Kluwer ČR, 2022. ISBN 978-80-7598-764-8.

E – monografie

ABU-TAIEH, Evon, Abdelkrim El MOUATASIM a Issam H. AL HADID. *Cyberspace* [online]. Velká Británie: IntechOpen, 2020. [cit. 27.2.2024]. ISBN: 978-1-78985-858-7. Dostupné z: https://www.google.cz/books/edition/Cyberspace/eqf8DwAAQBAJ?hl=cs&gbpv=1.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 5. dopl. a uprav. vyd. Praha: Česká pobočka AFCEA a Centrum kybernetické bezpečnosti, 2022. [cit. 28.10.2023]. ISBN: 978-80-908388-4-0. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf.

YAR, Majid a Kevin F. Steinmetz. *Cybercrime and Society* [online]. Velká Británie: SAGE Publications, 2019. [cit. 27.2.2024]. ISBN: 9781526481658. Dostupné z:https://www.google.cz/books/edition/Cybercrime_and_Society/_nN7DwAAQBAJ?hl=cs&gbpv=1.

Časopisecké články

RAK, Roman a Viktor PORADA. Digitální stopy v kriminalistice a forenzních vědách. *Soudní inženýrství* [online]. 2005, roč. 16, č. 1. [cit. 19.11.2023]. Dostupné z: https://www.sinz.cz/archiv/docs/si-2005-01-3-23.pdf.

RAK, Roman a Viktor PORADA. Vlastnosti digitálních stop a jejich dopady na forenzní šetření. *Soudní inženýrství* [online]. 2005, roč. 16, č. 4. [cit. 19.11.2023]. Dostupné z: https://www.sinz.cz/archiv/docs/si-2005-04-183-192.pdf.

VINČÁLEK, Jakub. Jak se vyvíjí objasněnost trestných činů v kyberprostoru. *STATISTIKA&MY* [online]. 2023, roč. 13, č. 5. [cit. 10.02.2024]. Dostupné z: https://www.statistikaamy.cz/wp-content/uploads/2023/05/18042305.pdf.

Zákonná úprava a IAŘ (interní akty řízení)

POKYN policejního prezidenta č. 100/2018, *o kriminalistickotechnické činnosti* v posledním znění.

POKYN policejního prezidenta č. 103/2013, *o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení* v posledním znění.

Vyhláška č. 357/2012 Sb., *o uchovávání, předávání a likvidaci provozních a lokalizačních údajů* v posledním znění.

Zákon č. 141/1961 Sb., *o trestním řízení soudním* (*trestní řád)* v posledním znění.

Zákon č. 127/2005 Sb. *o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích)* v posledním znění.

Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění.

Zákon č. 104/2013 Sb., *o mezinárodní justiční spolupráci ve věcech trestních* v posledním znění.

Zákon č. 250/2016 Sb., *o odpovědnosti za přestupky a řízení o nich* v posledním znění.

Zákon č. 251/2016 Sb., *o některých přestupcích* v posledním znění.

ZÁVAZNÝ POKYN policejního prezidenta č. 174/2011, *k provádění finančního šetření v trestním řízení* v posledním znění.

Webové stránky a elektronické zdroje

ABC LINUXU, 2005. *MAC adresa* [online]. [cit. 15.02.2024]. Dostupné z: https://www.abclinuxu.cz/slovnik/mac-adresa.

Česká bankovní asociace, 2024. *Češi a kyberbezpečnost 2024* [online]. [cit. 10.12.2023]. Dostupné z: https://cbaonline.cz/cesi-a-kyberbezpecnost-2024.

ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2022. Osoby v ČR používající internet, 2022: Tabulka 2.1. In: *Využívání informačních a komunikačních technologií v domácnostech a mezi osobami za období 2022* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/documents/10180/164606768/06200422.pdf/1c5c22c0-8941-4670-9698-e949482b0c35?version=1.3.

ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2023. Věc: Výpis ze statistického zjišťování [online]. [cit. 10.12.2023]. Dostupné z: https://www.czso.cz/documents/10180/132433649/Inflace_2000_2023.pdf.

ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2023. Účastníci hlasové služby v pevné síti v Česku: Tab. A1. In: *Informační společnost v číslech – 2023 - Česká republika a EU* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/documents/10180/191186455/06100423.pdf/879a3104-e54c-4f4e-b768-b0bd057ac006?version=1.3.

ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2023. Účastníci hlasové služby v mobilní síti v Česku: Tab. A2. In: *Informační společnost v číslech – 2023 - Česká republika a EU* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/documents/10180/191186455/06100423.pdf/879a3104-e54c-4f4e-b768-b0bd057ac006?version=1.3.

ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2023. Osoby v Česku používající mobilní telefon; 2022: Tab. C1. In: *Informační společnost v číslech – 2023 - Česká republika a EU* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/documents/10180/191186455/06100423.pdf/879a3104-e54c-4f4e-b768-b0bd057ac006?version=1.3.

ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2022. Osoby v ČR komunikující přes internet s ostatními, 2022: Tabulka 5.1. In: *Využívání informačních a komunikačních technologií v domácnostech a mezi osobami za období 2022* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/documents/10180/164606768/06200422.pdf/1c5c22c0-8941-4670-9698-e949482b0c35?version=1.3.

ČESKÝ STATISTICKÝ ÚŘAD (ČSÚ), 2023. *Pohyb obyvatelstva - 1. pololetí 2023* [online]. [cit. 11.02.2024]. Dostupné z: https://www.czso.cz/csu/czso/cri/pohyb-obyvatelstva-1-pololeti-2023.

Český telekomunikační úřad. *Dělení služeb elektronických komunikací* [online]. [cit. 10.12.2023]. Dostupné z: https://www.ctu.cz/deleni-sluzeb-elektronickych-komunikaci.

GNOME HELP. *Co je MAC adresa?* [online]. [cit. 15.02.2024]. Dostupné z: https://help.gnome.org/users/gnome-help/stable/net-macaddress.html.cs

Kaspersky Lab. *What is Spoofing – Definition and Explanation* [online]. [cit. 20.2.2024]. Dostupné z: https://usa.kaspersky.com/resource-center/definitions/spoofing.

Kaspersky Lab. *What is Smishing and How to Defend Against it?* [online]. [cit. 20.2.2024]. Dostupné z: https://usa.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it.

KLOZOVÁ Miroslava, 2021. Podvod 419 alias “SCAM 419”– 2021. In: *INTERNETEM BEZPEČNĚ* [online]. [cit. 13.12.2023]. Dostupné z: https://www.internetembezpecne.cz/podvod-419-alias-scam-419/.

SEZNAM POUŽITÝCH GRAFŮ

SEZNAM POUŽITÝCH TABULEK

SEZNAM PŘÍLOH

PŘÍLOHY

Příloha č. 1: Výzkumné otázky

Způsob páchaní TČ

1. Jaké jsou nejčastější způsoby jednání pachatele?
2. Jaký komunikační prostředek pachatel použil?
3. Skrýval pachatel svou identitu, nebo jednal vlastním jménem?
4. Využil pachatel technických prostředků anonymizace komunikace?
5. Jaký byl vztah pachatele k použité technice?
6. Jaké bylo při podvodu postavení pachatele?
7. V kolika případech zaslal pachatel zásilku?
8. Jaký způsob platby nebo převodu peněz pachatel využil?
9. Jaký byl vztah oběti a pachatele?
10. Jaký počet případů byl spáchán ve spolupachatelství?

Kriminální situace

11. Jaký počet případů má zahraniční přesah?
12. Jaká je objasněnost u všech ukončených případů?

Osobností rysy pachatele trestného činu

13. Jaký je věk pachatele?
14. Jaké je pohlaví pachatele?
15. Jaká je typická obhajoba pachatele?
16. Jak často ovlivňoval pachatel svědky?
17. Měl pachatel předchozí kriminální zkušenost?
18. Byl pachatel v minulosti odsouzen za trestný čin podvod?
19. Jaké měl pachatel vzdělání?
20. Jaké měl pachatel zaměstnání?

Osobnostní rysy oběti trestného činu

21. Poškozeným je fyzická nebo právnická osoba?
22. Jaký je věk oběti?
23. Jaké je pohlaví oběti?
24. Jaké měla oběť zaměstnání?

Motiv činu

25. Jaký byl motiv činu?

Typické stopy a jiné soudní důkazy

26. Jaké kriminalistické stopy a jiné soudní důkazy byly zajišťovány?

Zvláštnosti předmětu vyšetřování

27. Byl podvod kvalifikován v souběhu s jiným trestným činem?
28. Jaké jiné trestné činy byly kvalifikovány společně s podvodem?
29. V kolika případech je případ dílčím skutkem pokračujícího trestného činu podvod?

Typické podněty a jejich zvláštnosti

30. Jak dlouho po činu oznámil poškozený skutek na policii?
31. Jaké podstatné informace poškozený o průběhu podvodu nesdělil?
32. Co bylo důvodem nesdělení informace?

Typické počáteční vyšetřovací situace

33. Je známa totožnost pachatele v počáteční etapě vyšetřování?
34. Je známo místo pobytu pachatele v počáteční etapě vyšetřování?

Zvláštnosti počátečních úkonů a opatření

35. Jaké byly provedeny počáteční úkony?

Zvláštnosti následných úkonů

36. Jaké byly provedeny následné úkony?
37. Jaká doba uplynula od oznámení po zahájení trestního stíhání či rozhodnutí ve věci?

Příloha č. 2 – Varování bitcoinmat Zlín

Zdroj: Krajské ředitelství policie České republiky