

POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Katedra managementu a informatiky

**Koncepce policejního vzdělávání
v oblasti kybernetické trestné činnosti
a zvýšení počítačové gramotnosti
policistů v Plzeňském kraji**

Diplomová práce

**Concept of police education in the field of cybercrime and improvement of
computer literacy of police officers in the Pilsen region**

Master thesis

VEDOUCÍ PRÁCE

PhDr. Mgr. Eliška Jonášová Ph.D.

AUTOR PRÁCE

Bc. Jakub Knap

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 Plzni dne 11. 03. 2024

Jakub Knap

Poděkování:

Tímto bych chtěl ze srdce poděkovat své rodině, která mě ve studiu podporovala, všem neúnavným čtenářům pomáhajících mi při korekci a v neposlední řadě PhDr. Mgr. Elišce Jonášové, PhD., která jako vedoucí mé diplomové práce věnovala čas a úsilí k tomu, aby byla práce zpracována na mnou zvolené téma v co možná nejkvalitnější podobě.

ANOTACE

Diplomová práce pojednává o koncepci policejního vzdělávání v oblasti kybernetické trestné činnosti a zvýšení počítačové gramotnosti policistů v Plzeňském kraji. Diplomová práce je členěna do čtyř samostatných kapitol. První kapitola vymezuje základní pojmy v oblasti kybernetické trestné činnosti a počítačové gramotnosti. Druhá kapitola pojednává o současném stavu znalostí v oblasti kybernetické trestné činnosti a počítačové gramotnosti v Plzeňském kraji. Třetí kapitola pak představuje vytvořenou koncepci policejního vzdělávání ve výše uvedených oblastech, přičemž koncepce je rozdělena na části školení, řízené modelové situace a předem připravené úkoly v oblasti počítačové gramotnosti. Čtvrtá kapitola vyhodnocuje vypracované dotazníkové šetření.

KLÍČOVÁ SLOVA

Kyberkriminalita * vyšetřování kyberkriminality * počítačová gramotnost * vzdělávání * kyberprostor * kybernetické trestné činy * vyšetřování kybernetických trestných činů * koncepce policejního vzdělávání

ANNOTATION

The master thesis deals with the concept of police education in the field of cybercrime and improvement of computer literacy of police officers in the Pilsen region. The thesis is divided into four separate chapters. The first chapter defines basic terms in the field of cybercrime and computer literacy. The second chapter discusses the current state of knowledge in the field of cybercrime and computer literacy in the Pilsen region. The third chapter introduces the developed concept of police education in the aforementioned areas with the concept divided into training components, modelled scenarios, and pre-prepared tasks in the field of computer literacy. The fourth chapter evaluates the conducted questionnaire survey.

KEYWORDS

Cybercrime * cybercrime investigation * computer literacy * education *
cyberspace * cybercriminal offenses * investigation of cybercriminal offenses *
concept of police education

Obsah

Úvod.....	9
Cíle a metodika	16
1. Vymezení hlavních pojmů	19
1.1. Kybernetická trestná činnost.....	19
1.1.1. Kybernetická kriminalita.....	20
1.1.2. Ostatní kriminalita páchaná v kyberprostoru.....	20
1.1.3. Informační a komunikační technologie	21
1.1.4. Malware a phishing.....	21
1.1.5. Sociální inženýrství.....	22
1.1.6. Spoofing	23
1.1.7. Darkweb	24
1.1.8. Botnet	24
1.1.9. DoS a DDoS útoky.....	25
1.1.10. Kyberstalking	25
1.1.11. Kybergrooming	25
1.1.12. Sexting.....	26
1.1.13. Stopa a důkaz.....	27
1.1.14. Online platební metody.....	28
1.1.15. OSINT a WEBINT.....	28
1.2. Počítačová gramotnost	29
1.2.1. Výpočetní technika	29
1.2.2. Software	30
1.2.3. Hardware	31
1.2.4. Počítačová síť.....	32
1.2.5. NAT	34
1.2.6. Protokol, internetový protokol, IP adresa a port.....	34

1.2.7	Internetový prohlížeč a cookies	36
1.2.8	Internet Service Provider (ISP)	37
1.2.9	Elektronická pošta, e-mailová adresa a e-mailová zpráva	38
1.2.10	Sociální síť	40
1.2.11	Logovací soubory	41
1.2.12	EXIF data	41
1.2.13	IoT	42
1.2.14	NAS	43
1.2.15	Hash	43
1.2.16	Vzdálená správa počítače	44
1.2.17	Umělá inteligence	45
2.	Kybernetická trestná činnost a počítačová gramotnost policistů v Plzeňském kraji – současný stav znalostí a způsoby získávání informací	47
2.1.	Způsoby získávání informací a zkušeností v oblasti kybernetické trestné činnosti a zvyšování počítačové gramotnosti v současné době – Policisté sloužící do 3 let.....	54
2.2.	Způsoby získávání informací a zkušeností v oblasti kybernetické trestné činnosti a zvyšování počítačové gramotnosti v současné době – Policisté sloužící více jak 3 roky	55
3.	Koncepce policejního vzdělávání v oblasti kybernetické trestné činnosti a počítačové gramotnosti	58
3.1.	Školení.....	59
3.2.	Řízené modelové situace.....	66
3.3.	Předem připravené úkoly v oblasti počítačové gramotnosti	69
4.	Výzkum	72
4.1.	Výzkumný vzorek respondentů	73
4.2.	Odpovědi respondentů k výzkumné otázce č. 1	78
4.3.	Odpovědi respondentů k výzkumné otázce č. 2	81

4.4.	Odpovědi respondentů k výzkumné otázce č. 3	84
4.5.	Odpovědi respondentů k výzkumné otázce č. 4, č. 5 a č. 6	86
4.6.	Odpovědi respondentů k výzkumné otázce č. 7	89
4.7.	Odpovědi respondentů k výzkumné otázce č. 8	91
4.8.	Odpovědi respondentů k výzkumné otázce č. 9 a č. 10.....	91
	Závěr.....	94
	Seznam použité literatury.....	97
	Seznam grafů.....	104
	Seznam obrázků	106
	Seznam příloh.....	114

Úvod

Téma mé diplomové práce "Koncepte policejního vzdělávání v oblasti kybernetické trestné činnosti a zvýšení počítačové gramotnosti policistů v Plzeňském kraji" jsem si vybral s ohledem na skutečnost, že v rámci vyšetřování této trestné činnosti se pohybuji prakticky od roku 2011. V rámci mých zkušeností se běžně setkávám s tím, že většina policistů na území Plzeňského kraje je obeznámena se základy šetření, prověřování a vyšetřování kybernetické trestné činnosti, pod kterou si představují téměř výhradně podvodná jednání. Bohužel však většina z informací, které i k této problematice mají, je velmi povrchní a vyplývající zejména z nejrůznějších koordinačních přípisů, případně ze zkušeností z dob minulých. Dle mého názoru jak policisté základních článků, tak policisté zařazení na útvarech služby kriminální policie a vyšetřování¹, nemají často čas a někdy ani zájem o získávání a rozšiřování svých znalostí v oblasti kybernetické trestné činnosti, a to i přes skutečnost, kdy výpočetní technika je v dnešní době nepopíratelně důležitým aspektem života ve společnosti. Moderní technologie nás všechny obklopují způsobem, který si ještě před několika málo desetiletími nedokázal téměř nikdo představit, snad vyjma George Orwella ve svém díle 1984 sepsaném v roce 1949.

Domnívám se, že pro samotné pochopení kybernetické trestné činnosti, je třeba současně zvýšit počítačovou gramotnost policistů, přičemž nemám pochyb o tom, že policisté umí velmi dobře využívat informační systémy Policie České republiky.² Avšak pro samotné šetření tohoto typu trestné činnosti je třeba umět efektivně využívat také další softwarové vybavení jako např. tabulkový software³, poštovního klienta⁴, specializovaný software vyvíjený policisty⁵ apod. Za nutnost pokládám znalost základní používané terminologie v oboru⁶, stejně tak pochopení možností rozvíjející se umělé inteligence. V diplomové práci se pokusím definování základní pojmy a jejich vysvětlení. Již samotné toto definování

¹ Dále jen SKPV

² Dále jen Policie ČR

³ Např. Microsoft Excel

⁴ Např. Microsoft Outlook

⁵ Např. softwarové nástroje vývojáře Cubex, případně software vyvíjený ze strany Útvaru zvláštních činností služby kriminální policie a vyšetřování

⁶ Např. NAT, port, IP adresa, FTP, SMTP, POP3, IMAP

a vysvětlení pojmů beru jako počátek vzdělávání v oblasti kybernetické trestné činnosti, jelikož se domnívám, že bez těchto, pro mě elementárních, znalostí nemůže policista složitou problematiku týkající se kybernetické trestné činnosti pochopit.

Obecně je velkým problémem kybernetické kriminality a ostatní kriminality páchané v kyberprostoru latentní kriminalita. I přes tuto skutečnost však počet registrované kybernetické kriminality a ostatní kriminality páchané v kyberprostoru každoročně v České republice roste, kdy v roce 2022 tato kriminalita tvořila 10,2 % z celkové registrované kriminality (18554 skutků). To meziročně znamenalo nárůst přes 94,9 %.⁷ V roce 2023 tato kriminalita tvořila 10,8 % z celkové registrované kriminality (19592 skutků).⁸

Pokud bychom se pak bavili pouze o Plzeňském kraji, pak v roce 2018 bylo spácháno 236 skutků, v roce 2019 291 skutků, v roce 2020 302 skutků, v roce 2021 479 skutků, v roce 2022 pak 887 skutků a v roce 2023 945 skutků⁹. Z uvedených dat je jednoznačně vidět soustavný nárůst uvedené kriminality na území Plzeňského kraje. Skutkově je nárůst v jednotlivých letech také markantní. Co se týče počtu skutků, pak je jejich zařazování (zejména v oblasti ostatní kriminality páchané v kyberprostoru) velmi problematické. Uvedených 945 skutků je totiž statistika kriminality spáchané internetem a počítačovými sítěmi. Pokud bychom se podívali na kybernetickou trestnou činnost jako celek, pak, dle tiskové konference ze dne 06. 02. 2024, bylo spácháno celkem 1357 skutků kybernetické trestné činnosti, oproti 1364 v roce 2022, 781 v roce 2021 a 482 v roce 2020¹⁰. Z uvedených statistik tedy vyplývá, že od roku 2020 do roku 2023 se kybernetická trestná činnost ztrojnásobila, což je velmi markantní nárůst.

⁷ MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022*. Online. In: Policie České republiky, 13. 01. 2023. Dostupné z: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx>. [cit. 2024-02-04].

⁸ MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2023*. Online. In: Policie České republiky, 12. 01. 2024. Dostupné z: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx>. [cit. 2024-02-04].

⁹ MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2023*. Online. In: Policie České republiky, 12. 01. 2024. Dostupné z: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx>. [cit. 2024-02-04].

¹⁰ Policie České republiky – KŘP Plzeňského kraje. *Statistické ukazatele za rok 2023*. Online. In: Policie České republiky. Dostupné z: <https://www.policie.cz/clanek/statisticke-ukazatele-za-rok-2023.aspx>. [cit. 2024-02-10].

Jednoznačně největší podíl z uvedené trestné činnosti zabírají podvody, kterých v roce 2023 bylo na území Plzeňského kraje spácháno celkem 603 skutků. Pomyslné druhé místo pak obsadily souhrnně skutky neoprávněný přístup a poškození záznamů v počítačovém systému, opatření a přechovávání přístupového zařízení a hesla, a to v celkem 105 případech. Dalším v pořadí by pak byl trestný čin neoprávněné opatření, padělání a pozměnění platebního prostředku v 75 skutcích.

Z dat týkajících se podílu kriminality spáchané na internetu na celkové kriminalitě v letech 2022 a 2023 vyplývá, že tento podíl vzrostl z 9 % v roce 2022 na 10 % v roce 2023¹¹.

Dalším důvodem, proč je vzdělávání se v této oblasti podle mě velmi důležité, jsou škody, které jsou v souvislosti s kybernetickou kriminalitou a zejména ostatní kriminalitou páchanou v kyberprostoru způsobovány. Česká bankovní asociace ve své zprávě ze dne 30. 01. 2024 uvádí: „*Počet útoků na klienty bank se meziročně ztrojnásobil. Celkové škody jsou víc než 1,3 miliardy korun.*“¹²

Podle dat dostupných mi z informačního systému ETŘ dosáhla škoda způsobena prověřovanou kybernetickou trestnou činností na území plzeňského kraje v roce 2023 výše 185587333,-Kč. V uvedené částce jsou však obsaženy, vyjma jednání mající charakter trestného činu, také jednání přestupková, kterých bylo v Plzeňském kraji řešeno v roce 2023 celkem 637.

Samotnou kapitolou dané problematiky je objasněnost dané kriminality. Bohužel k tomuto mi nejsou dostupná data pouze v Plzeňském kraji, ale statistika objasněných skutků spáchaných internetem a ostatními sítěmi na území celé České republiky byla v roce 2022 15,1 %. Toto byl od roku 2016 nejnižší podíl objasněnosti na této kriminalitě, když v roce 2021 to bylo 24,8 %, v roce 2020 30,5 %, v roce 2019 37,1 %, v roce 2018 47,8 %, v roce 2017 49,2 % a v roce 2016 pak byla objasněnost více než 50 %, celkem 51,3 %¹³. Zde je ale třeba mít také na paměti, že v roce 2016 bylo spácháno „pouze“ 4990 skutků.

¹¹ MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2023*. Online. In: Policie České republiky, 12. 01. 2024. Dostupné z: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx>. [cit. 2024-02-04].

¹² Česká bankovní asociace. *Češi a kyberbezpečnost*. Online. In: Česká bankovní asociace, 30. 01. 2024. Dostupné z: <https://cbaonline.cz/cesi-a-kyberbezpecnost-2024>. [cit. 2024-02-05].

¹³ VINČÁLEK, Jakub. *Jak se vyvíjí objasněnost trestných činů v kyberprostoru?*. Online. In: Statistika & My Magazín Českého statistického úřadu. 16.05.2023. Dostupné z:

Z uvedených statistik pak jednoznačně vyplývá, že přes zvyšování podílu kybernetické kriminality na celkové kriminalitě a současně stoupající počet registrovaných skutků je jejich objasněnost rok od roku nižší. Jaké jsou konkrétní důvody snižování objasněnosti, se můžeme pouze domnívat, dle mého názoru jsou jimi:

1. policisté nemají takový vhled do oblasti kybernetické trestné činnosti, jaký by pro prověřování a vyšetřování této kriminality měli mít, s čímž souvisí také skutečnost, že Policie ČR má velmi málo specialistů zabývajících se tímto druhem kriminality,
2. specialisté na kybernetickou trestnou činnost v řadách Policie ČR velmi často nevedou celé trestní řízení v jeho komplexu, ale jsou povolávání k řešení jen dílčích úkonů, případně k poskytnutí rady,
3. pachatelé se učí ze svých dřívějších chyb zjištěných na základě nahlédnutí do spisových materiálů a informací z rozhodnutí policejního orgánu, čímž se zdokonalují v páčání této trestné činnosti,
4. kybernetická trestná činnost se stala za poslední léta velmi výdělečnou, kdy bez nutnosti jakéhokoliv osobního jednání s poškozeným je způsobována velmi vysoká škoda,
5. pachatelům postačuje nalezení vhodného způsobu provedení, kdy tento způsob provedení jen s občasnou obměnou je používán pachateli v řádech měsíců a let.

S ohledem na zřízení pracovní skupiny KYBER rozkazem ředitele Krajského ředitelství policie Plzeňského kraje¹⁴¹⁵, jejímž jsem vedoucím, která má za úkol mj. rozvoj znalostí členů pracovní skupiny a předávání nabytých znalostí dále, bylo vztaženo uvedené téma právě na Plzeňský kraj, kde také uvedené poznatky a zjištění budu schopen aplikovat v praxi. Poznatky a zjištění budou výsledkem dotazníkového šetření, kdy vzorek dotazníku bude přiložen k této diplomové práci jako příloha. Dle vlastních zkušeností se domnívám, že v současné době u Policie

<https://www.statistikaamy.cz/2023/05/16/jak-se-vyvi-objasnenost-trestnych-cinu-v-kyberprostoru>. [cit. 2024-02-10].

¹⁴ Krajské ředitelství policie Plzeňského kraje dále jen KŘPP

¹⁵ 108 ROZKAZ ředitele Krajského ředitelství policie Plzeňského kraje ze dne 12. října 2023, kterým se zřizuje pracovní skupina KYBER. 12. 10. 2023. Dostupné z: <http://esiar.pcr.cz/kniha/siar>. [cit. 2024-02-10].

ČR je velmi velký zájem o osoby, které se v prostředí kybernetické trestné činnosti jsou schopny pohybovat, kvalifikovaně vést trestní řízení, jsou schopny určitým způsobem inovativně přemýšlet, aplikovat ustanovení zákona č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění účinném ke dni 04. 02. 2024¹⁶ a zákona č. 40/2009 Sb., trestní zákoník, ve znění účinném ke dni 04. 02. 2024¹⁷ způsobem, který dříve nikoho nenapadl, nikdo jej daným způsobem neaplikoval nebo tento způsob kolegové odsuzovali, zjednodušeně řečeno je v rámci nejrůznějších článků Policie ČR zájem o osoby, které přemýšlí ne zcela běžným způsobem.

V současné době je policejní vzdělávání v této oblasti velmi roztržité a neexistuje žádný program dostupný všem policistům, který by tuto oblast zahrnoval komplexně jak z teoretického, tak z praktického hlediska. Tato skutečnost kopíruje současný stav u Policie ČR, kdy tato ve svých interních dokumentech dělí kybernetickou trestnou činnost na kybernetickou kriminalitu a ostatní kriminalitu páchanou v kyberprostoru. Každá z uvedených částí kybernetické trestné činnosti má svého garanta, stejně tak mají však své garanty technické úkony, další garanti jsou pro zahraničí, emergency (bezodkladné) vyžadování aj. Vedle uvedených garantů pak stojí Útvar policejního vzdělávání a služební přípravy Policie ČR. *„Útvarem policejního vzdělávání a služební přípravy jsou zabezpečovány zejména následující činnosti:*

- *stanovuje koncepci policejního vzdělávání, služební přípravy a policejního sportu*
- *stanovuje a aplikuje systém odborného vzdělávání příslušníků policie a zaměstnanců*
- *vykonává analytickou, plánovací, metodickou, kontrolní a koordinační činnost pro oblast policejního vzdělávání, služební přípravy a policejního sportu*
- *metodicky vede a koordinuje činnost školních policejních středisek a odborů služební přípravy krajských ředitelství policie při zajišťování policejního vzdělávání a služební přípravy*

¹⁶ Dále jen trestní řád.

¹⁷ Dále jen trestní zákoník.

- *metodicky vede a koordinuje policejní sport, organizuje policejní mistrovství a mezinárodní soutěže*
- *připravuje, schvaluje a realizuje vzdělávací programy a vzdělávací projekty a komplexně zabezpečuje policejní vzdělávání*
- *zajišťuje služební přípravu, včetně prověrek ze služební přípravy policistů*
- *spolupracuje s Ministerstvem vnitra, s vyššími a středními policejními školami Ministerstva vnitra, Policejní akademií České republiky v Praze a dalšími organizačními složkami státu, ke kterým Ministerstvo vnitra vykonává zřizovatelské funkce, při zajišťování policejního vzdělávání realizované v těchto školách*
- *zajišťuje za policii mezinárodní policejní vzdělávání a spolupracuje s Ministerstvem vnitra při prosazování zájmů policie v mezinárodních vzdělávacích agenturách*
- *připravuje projekty spolufinancované zejména z mimorozpočtových zdrojů v oblasti policejního vzdělávání, služební přípravy a policejního sportu“¹⁸*

Gestor technického zajišťování a zkoumání je v rámci přípravného řízení Kriminalistický ústav Policie České republiky¹⁹, který v současné době připravuje IT specialisty – techniky – v rámci Vzdělávacího programu Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat. Gestor kybernetické kriminality je Národní centrála proti terorismu, extremismu a kybernetické kriminalitě SKPV²⁰. Za ostatní kriminalitu páchanou v kyberprostoru je pak gestorem Úřad služby kriminální policie a vyšetřování²¹. Oproti tomu Národní centrála proti organizovanému zločinu SKPV²² je jako gestor nad problematikou virtuálních měn. Zcela samostatně pak stojí Útvar zvláštních činností služby kriminální policie²³, který zastřešuje část týkající se telefonních operátorů, poskytovatelů internetového připojení, poskytovatelů zahraničních komunikačních služeb, provozovatelů e-mailových portálů apod. Z výše

¹⁸ Policie České republiky. *Útvar policejního vzdělávání a služební přípravy*. Online. In: Policie České republiky. Dostupné z: <https://www.policie.cz/clanek/utvar-policejního-vzdelavani-a-sluzebni-pripravy.aspx>. [cit. 2024-02-11].

¹⁹ Dále jen KÚP

²⁰ Dále jen NCTEKK

²¹ Dále jen ÚSKPV

²² Dále jen NCOZ

²³ Dále jen ÚZČ

uvedeného je tak patrné, že v případě dostatečně připraveného policisty, který se chce kvalifikovaně zabývat šetřením kybernetické trestné činnosti, je třeba, aby měl alespoň elementární znalosti ve všech výše zmíněných oblastech. Nad to lze konstatovat, že žádný z výše uvedených článků v současné době neprovádí školení nesespecializovaných policistů či systematické doškolování policistů specializovaných (vyjma KÚP). Problematika proškolení běžných policistů v rámci šetření kybernetické trestné činnosti zařazených na obvodních a místních odděleních, na odděleních hospodářské kriminality, obecné kriminality a analytiky a kybernetické kriminality leží zcela na odborech kybernetické kriminality krajských ředitelství Policie ČR. V současné době sice v rámci základních odborných příprav²⁴ (kterými musí projít všichni nově nastoupivší policisté) či specializačních příprav existuje určitá časová dotace týkající se kybernetické trestné činnosti, ale tato je velmi nedostatečná. Dle současných informací se však v oblasti policejního vzdělávání pomyslně „blýská na lepší časy“, kdy ze strany Úřadu služby kriminální policie a vyšetřování by měl být připravován několikastupňový vzdělávací program formou webinářů.²⁵

Právě z výše nastíněných důvodů se domnívám, že vypracování koncepce policejního vzdělávání v oblasti kybernetické trestné činnosti a zvýšení počítačové gramotnosti policistů v Plzeňském kraji může být velmi přínosné, i s ohledem na skutečnost, že centrálně ze strany Policie ČR mi není v současné době žádný komplexní vzdělávací program týkající se kybernetické trestné činnosti znám a už vůbec ne formou modelových situací, které budu chtít nastítnit v praktické části této diplomové práce.

²⁴ Dále i jen ZOP

²⁵ Informace aktuální ke konci měsíce ledna 2024

Cíle a metodika

Hlavním cílem této diplomové práce je na základě rešerše odborné literatury a za pomoci metod deskripce a klasifikace zhodnotit aktuální stav vzdělávání policistů v oblasti kybernetické trestné činnosti a počítačové gramotnosti, vymezení hlavních pojmů v rámci kybernetické trestné činnosti a počítačové gramotnosti.

K dosažení účelu definovaného hlavním cílem je práce rozdělena na teoretickou část, která obsahuje 4 dílčí cíle, a praktickou část, která se zabývá výzkumnými otázkami.

Dílčí cíle teoretické části práce jsou:

1. Na základě rešerše odborné literatury definovat pojem kybernetická trestná činnost.
2. Definovat pojem počítačová gramotnost.
3. Definovat hlavní pojmy týkající se kybernetické trestné činnosti.
4. Definovat hlavní pojmy týkající se počítačové gramotnosti.
5. Zjištění současného stavu znalostí policistů KŘPP v oblasti kybernetické trestné činnosti a počítačové gramotnosti.

K naplnění dílčího cíle týkajícího se současného stavu znalostí policistů KŘPP v oblasti kybernetické trestné činnosti a počítačové gramotnosti slouží mj. výzkumné otázky položené v rámci realizovaného výzkumu:

- Jak hodnotíte znalosti předávané v rámci základních odborných příprav (dále jen ZOP) týkající se kybernetické trestné činnosti a ostatní kriminality páchané v kyberprostoru?
- Jak hodnotíte znalosti předávané v rámci ZOP týkající se počítačové gramotnosti (schopnost používat účelově a účinně počítač a jinou výpočetní techniku)?
- Kolik školení po ZOP týkajících se kybernetické trestné činnosti či počítačové gramotnosti jste díky PČR absolvovali?
- Jak hodnotíte znalosti předávané v rámci školení týkajících se kybernetické trestné činnosti?
- Jaké zaměření uvedená školení týkající se kybernetické trestné měla?
- Jak hodnotíte znalosti předávané v rámci školení týkající se počítačové gramotnosti?

- Měli jste možnost se v rámci služebního poměru účastnit jakéhokoliv školení týkající se kybernetické trestné činnosti či počítačové gramotnosti?

Hlavním cílem praktické části práce je vytvoření koncepce rozvoje policistů se zaměřením na kybernetickou trestnou činnost, počítačovou gramotnost a předávání znalostí policistům v rámci plzeňského kraje, kdy k dosažení tohoto cíle budou nápomocny zejména 3 výzkumné otázky položené v rámci realizovaného výzkumu:

- Jakou formu vzdělávání v uvedené oblasti preferujete?
- Vyhovovalo by Vám školení formou řízených modelových situací v oblasti kybernetické trestné činnosti?
- Vyhovovalo by Vám školení formou řešení předem připravených úkolů v oblasti počítačové gramotnosti?

Uvedené cíle, stejně jako celá diplomová práce, budou autorem velmi pravděpodobně aplikovány do praxe, a to s ohledem na profesní působení autora, zejména jakožto vedoucího již zmíněné pracovní skupiny.

V rámci plnění všech cílů diplomové práce byly užity informace zjištěné z publikace *Pokročilé metody vědecké práce* profesora Molnára, která byly inspirací v rámci užitých vědeckých postupů, které jsou obsaženy v práci.

Teoretická oblast této diplomové práce je tvořena deskriptivním přístupem s empirickým výzkumem-

Exploratorní výzkum za využití neexperimentální metody průzkumu prostřednictvím dotazníkového šetření bude tvořit kostru výzkumné části této diplomové práce. Výzkumné otázky v dotazníku jsou strukturovány a pokládány tak, aby poskytly ucelené odpovědi na položené dotazy, kdy otázky byly tvořeny v souladu s profesorem Molnárem uváděnou všeobecnou a prověřenou pravdou: *„otázka správně položená je z poloviny zodpovězená“*²⁶. Stejně tak jednotlivé hypotézy byly tvořeny dle metodologie uváděné profesorem Molnárem.

Dotazníkové výstupy budou zpracovatelem vyhodnoceny prostřednictvím statistických metod. Za tímto účelem budou připravena data pro statistickou analýzu prostřednictvím sešitu Excel ve formátu XLSX. Ve vyhodnocení

²⁶ MOLNÁR, Zdeněk, MILDEROVÁ, Stanislava, ŘEZANKOVÁ, Hana, BRIXÍ, Radim a KALINA Jaroslav. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting, 2012. Věda pro praxi (Profess Consulting). ISBN 978-80-7259-064-3, str. 33

(výzkumných otázek) budu pracovat s kvantitativními typy proměnných, jelikož na základě získaných dat bude možné určit, kolik účastníků v každé výzkumné otázce odpovědělo, jakým způsobem a jejich případné vzájemné srovnání.

Dotazníkové výstupy budou zpracovatelem diplomové práce vyhodnoceny a následně prostřednictvím aplikování induktivního přístupu logické metody budou příslušná data využita k vytvoření hypotéz. Je však třeba mít na paměti, že *„Závěry induktivních myšlenkových pochodů jsou vždy ovlivněny subjektivními postoji (zkušenostmi, znalostmi) a mají proto omezenou platnost.“*²⁷

Vzhledem ke vztažení tématu pouze na oblast v územní působnosti KŘPP, bude třeba v samotném počátku vybrat reprezentativní vzorek policistů právě sloužících v působnosti KŘPP, což však bude mít za následek maximální možnou validitu a reliabilitu k danému tématu, kdy za úspěch pisatel bude považovat obdržení více jak 50 odpovědí (zejména s ohledem na vymezenou působnost policistů). Avšak i v rámci tohoto vzorku policistů bude vyvinuta snaha k získání respondentů z různých organizačních článků podléhajících KŘPP a s různým pracovním zaměřením. Vzhledem k předpokladu induktivního přístupu a získání dostatečného počtu statistických údajů následně předpokládám aplikaci smíšeného výzkumu, kdy se domnívám, že smíšený výzkum mi dopomůže i k očištění spolehlivých informací od nespolehlivých a získat tak validní a objektivní obraz.

²⁷ MOLNÁR, Zdeněk, MILDEROVÁ, Stanislava, ŘEZANKOVÁ, Hana, BRXÍ, Radim a KALINA Jaroslav. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting, 2012. Věda pro praxi (Profess Consulting). ISBN 978-80-7259-064-3, str. 43

1. Vymezení hlavních pojmů

Pro samotné pochopení kybernetické trestné činnosti, o které bude v této diplomové práci psáno, je třeba vymezit si základní pojmy, které budou pisatelem používány. Jde o zejména o pojmy jako botnet, cookies, darkweb, DoS a DDoS útoky, důkaz, elektronická pošta, e-mailová adresa, e-mailová zpráva, EXIF data, hardware, hash, informační a komunikační technologie, internet service provider, internetový prohlížeč, internetový protokol, IoT, IP adresa, kybergrooming, kybernetická trestná činnost, kyberstalking, logovací soubory, malware, NAS, NAT, online platební metody, ostatní kriminalita páchaná v kyberprostoru, phishing, počítačová síť, port, protokol, sexting, sociální inženýrství, sociální síť, software, spoofing, stopa, umělá inteligence, výpočetní technika, vzdálená správa počítače. Cílem této práce není vysvětlovat či rozebírat obligatorní a fakultativní znaky skutkové podstaty jednotlivých trestných činů, kdy se domnívám, že toto jsou záležitosti, které policisté znají a chápou ze základní odborné přípravy, kterou musí všichni absolvovat. Stejně tak zde nebudou definovány notoriety, tedy obecně známé pojmy, které nelze vykládat různými způsoby, ale jsou zcela jednoznačné (např. data, internet, GPS, operační systém). Dále je třeba upozornit na skutečnost, že některé pojmy uvedené v jednotlivých vymezeních se mohou prolínat s následujícími či předchozími.

1.1. Kybernetická trestná činnost

Existuje několik nejrůznějších vymezení pojmů kybernetická trestná činnost, stejně tak jako existuje několik různých označení této činnosti. Různá označení a vymezení vyplývají z jednotlivých děl a také z jednotlivých právních norem. Pokud bychom se bavili o samotném označení, pak se ve světě, ale i v České republice, stále ještě můžeme setkat (ostatně jak uvádí také Kolouch ve své publikaci CyberCrime) s označením internetová kriminalita, „*informační, informatická, elektronická kriminalita, softwarová trestná činnost, počítačová trestná činnost, počítačová kriminalita, kybernetická trestná činnost,*

*kyberkriminalita aj.*²⁸ Všechna uvedená označení se mnohdy berou jako synonyma k pojmu kybernetická trestná činnost.

Úmluva o počítačové kriminalitě tuto definuje jako „činy namířené proti důvěrnosti, integritě a dostupnosti počítačových systémů, sítí a počítačových dat, i proti zneužití těchto systémů, sítí a dat.“²⁹ Pokyn policejního prezidenta č. 103 ze dne 28. května 2013 o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení ve znění aktuálním ke dni 11. 09. 2023³⁰ dělí kybernetickou trestnou činnost na dvě části – kybernetickou kriminalitu a ostatní kriminalitu páchanou v kyberprostoru.

1.1.1. Kybernetická kriminalita

Kybernetická kriminalita je v PPP č. 103/2013 definována jako „*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*“³¹. Z této definice pak jednoznačně vyplývá, že se bude jednat o takové skutky, jako jsou útoky DoS a DDoS, útoky malwarem, převzetí účtů na sociálních sítích, neoprávněné přístupy k počítačovým systémům aj.

1.1.2. Ostatní kriminalita páchaná v kyberprostoru

Definice této kriminality dle PPP č. 103/2013 je „*kriminalita páchaná za výrazného využití informačních a komunikačních technologií, přičemž hlavním objektem útoku je zejména život, zdraví, majetek, svoboda, lidská důstojnost a mravnost*“³². Mezi typické a aktuální trestné činy patřící do skupiny této kriminality pak zařazujeme podvodná jednání prostřednictvím nákupních portálů, vylákání informací k bankovním účtům či platebním kartám, vydávání se za pracovníka

²⁸ KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-18-8, str. 31.

²⁹ Council of Europe. *Úmluva o počítačové kriminalitě*. Online. In: Council of Europe, 04. 01. 2013. Dostupné z: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900016804931c0>. [cit. 2023-09-10].

³⁰ Dále také jen PPP č. 103/2013

³¹ 103 POKYN policejního prezidenta ze dne 28. května 2013, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení. 28. 05. 2013. Str. 3. Dostupné z: <http://esiar.pcr.cz/kniha/siar>. [cit. 2023-09-10].

³² 103 POKYN policejního prezidenta ze dne 28. května 2013, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení. 28. 05. 2013. Str. 3. Dostupné z: <http://esiar.pcr.cz/kniha/siar>. [cit. 2023-09-10].

banky a následné podvodné vylákání financí, lze sem zařazovat také trestné činy související s dětskou pornografií páchanou prostřednictvím sítě internet apod.

1.1.3. Informační a komunikační technologie

Mezi informační a komunikační technologie řadíme „*technologie, systémy, aktivity a procesy, které se podílejí na zobrazení, zpracování, skladování a přenosu informací a dat elektronickou cestou*“³³. Pro informační a komunikační technologie se také používá zkratka ICT či IKT. Mezi tyto technologie řadíme softwarové a hardwarové vybavení a počítačové sítě (lokální síť, internet apod.).

1.1.4. Malware a phishing

Malware je „*Software vytvořený s nekalým úmyslem, který obsahuje funkce nebo nástroje, které mohou přímo nebo nepřímo způsobit škodu uživateli anebo počítačovému systému. Mezi škodlivý software patří počítačové viry, trojské koně, červy, špionážní software, atd.*“³⁴ Mezi malware patří mj. policejní viry³⁵ (viz. Obrázek č. 1), vyděračské viry³⁶ (viz. Obrázek č. 2), trojské koně³⁷, spyware³⁸, keyloggery³⁹ aj.

Pishingem rozumíme „*Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup*

³³ Český statistický úřad. 20. *INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE*. Online. In: Český statistický úřad, 18. 02. 2011. Dostupné z: <https://www.czso.cz/documents/10180/25385875/19874229+000110c20.pdf/08cfdb7a-a8c6-4fc4-83a8-4ee94258aab2?version=1.0>. [cit. 2023-09-11].

³⁴ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 187. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2023-09-11].

³⁵ Virus, který po spuštění operačního systému zobrazuje na obrazovce hlášení, že počítač uživatele byl uzamčen z důvodu přechovávání či distribuce dětské pornografie (či další trestné činnosti), kdy pro jeho odemčení je třeba uhradit „pokutu“ uvedeným způsobem.

³⁶ Virus, jenž po úspěšné nauce postupně zašifruje data v programátorem určeném pořadí, kdy po úspěšném zašifrování se na obrazovce operačního systému zobrazí hlášení o tom, že došlo k zašifrování dat a k jeho odšifrování je třeba uhradit určený poplatek, který zpravidla v čase stoupá a po určené době jej již nelze uhradit.

³⁷ Virus, který předstírá jakýkoliv zvolený důvěryhodný soubor tak, aby si jej uživatel nainstaloval či umístil do paměti svého počítače, kdy tento soubor následně vykonává programátorem zvolenou akci.

³⁸ Virus, který po své infiltraci cílového zařízení skrytě sbírá informace (typicky uživatelská jména a hesla), které následně v předem stanovených intervalech (či konstantně) odesílá tyto informace původci viru. Též označován jako špionážní software.

³⁹ Software zaznamenávající veškeré stisknuté klávesy na klávesnici napadeného systému, které jsou následně zaslány pachateli.

k datům atd.). Vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Může jít například o padělaný dotaz banky, jejíchž služeb uživatel využívá, se žádostí o zaslání čísla účtu a PIN pro kontrolu (použití dialogového okna, předstírajícího, že je oknem banky – tzv. spoofing). Tímto způsobem se snaží přistupující osoby přesvědčit, že jsou na známé adrese, jejímuž zabezpečení důvěřují (stránky elektronických obchodů atd.). Tak bývají rovněž velice často zcizována například čísla kreditních karet a jejich PIN.⁴⁰

Existuje velké množství jednotlivých druhů phishingu, mezi které patří e-mail phishing⁴¹, spear phishing⁴², whaling⁴³, CEO fraud⁴⁴, vishing⁴⁵, smishing⁴⁶, page hijacking⁴⁷, catfishing⁴⁸.

1.1.5 Sociální inženýrství

Výkladový slovník kybernetické bezpečnosti k sociálnímu inženýrství uvádí: „Účelová manipulace lidí s cílem přimět je k provedení určité akce nebo k vyzrazení důvěrné informace.“⁴⁹ Sociální inženýrství velmi často využívá lidské naivity či nezkušenosti. Cílem útočníka je zde zjištění požadovaných informací či

⁴⁰ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 122. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2023-09-11].

⁴¹ Dalo by se říci, že se jedná o část tzv. spamových e-mailových zpráv, které jsou rozesílány hromadně, bez jakéhokoliv zacílení.

⁴² Útok, ve kterém pachatel využívá již doposud zjištěné informace o jeho oběti, kdy následně cílí na získání dalších informací. Zjištěné informace typicky pachatel vlastní z předchozích phishingových kampaní.

⁴³ Phishing, který cílí na vedení společností, typicky jednatele, prokuristy apod.

⁴⁴ Účetní osobu (či osobu v obdobném postavení) kontaktuje zpravidla e-mailem pachatel tvářící se jako jednatel (či osoba v obdobném postavení) se žádostí o zaslání platby na konkrétní bankovní účet.

⁴⁵ Voice phishing, tedy phishingový útok prováděný cestou telefonního hovoru.

⁴⁶ SMS phishing, tedy phishingový útok prováděný cestou SMS zpráv.

⁴⁷ Vytvoření kopie původní stránky a např. zaplacení její propagace na vyhledávačích.

⁴⁸ Pachatel na síti internet vystupuje pod jím smyšlenou identitou za účelem kontaktování dalších osob apod.

⁴⁹ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 172. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2024-02-04].

provedení určité akce ze strany oběti bez toho, aby musel prolamovat jakékoliv zabezpečení, zjišťovat uživatelská jména či hesla. Místo toho pachatel navodí situaci, kdy mu všechny požadované informace sdělí oběť sama dobrovolně a většinou ještě ráda, případně tyto informace získá díky nainstalování škodlivého softwaru na zařízení oběti. ENISA⁵⁰ k sociálnímu inženýrství uvádí, že na techniky sociálního inženýrství lze nahlížet ze dvou úhlů. Prvním je prostřednictvím psychologické manipulace dosáhnout k získání dalšího přístupu k požadovanému systému (např. vydávat se za ředitele společnosti s cílem nalákat účetní osobu k procházení škodlivých internetových stránek, díky čemuž dojde k instalaci malwaru na počítač účetní osoby). Druhým je prostřednictvím informačních technologií, jakožto podpory psychologické manipulace, dosáhnout cíle mimo oblast informačních technologií (např. získání bankovních informací prostřednictvím phishingové kampaně a následné odcizení financí).⁵¹

1.1.6 Spoofing

Spoofing bývá označován jako samostatný podvod, jehož účelem je zamaskování e-mailové adresy, zobrazovaného jména, telefonního čísla, textové zprávy nebo adresy URL za účelem přesvědčení poškozeného, že tento komunikuje s důvěryhodným zdrojem.⁵² V České republice je však spoofing nejčastěji součástí předem připravené podvodné kampaně, a to jak ve formě kontaktování ze strany falešného bankéře⁵³, tak také ze strany podvodných investičních portálů na síti internet. Spoofing v tomto případě představuje prakticky ze 100% napodobení telefonního čísla známé instituce (České národní banky, České spořitelny, AirBank, ale třeba také Policie ČR aj.) z důvodu ubezpečení cíle o regulérnosti pachatelem sdělovaného postupu. Pachatel se typicky snaží získat od cíle veškeré jeho úspory (případně sjednat půjčku u bankovní instituce cíle, založit nové bankovní účty aj.), které následně pod nejrůznější legendou cíl vkládá

⁵⁰ European Union Agency for Cybersecurity – Agentura Evropské unie pro kybernetickou bezpečnost

⁵¹ ENISA. *What is "Social Engineering"?*. Online. In: ENISA. Dostupné z: <https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering>. [cit. 2024-02-04].

⁵² FOLGER, Jean. *What Is Spoofing? How Scam Works and How To Protect Yourself*. Online. In: Investopedia, 2022, 07.09.2022. Dostupné z: <https://www.investopedia.com/terms/s/spoofing.asp>. [cit. 2024-02-03].

⁵³ Jedna ze – v současné době rozšířených forem – vishingu.

do automatu na virtuální měny. V Příloze č. 1 jsou ukázány jedny z nejčastějších současných vishingových legend používaných ze strany pachatelů.

1.1.7 Darkweb

Darkwebem se nazývá neveřejná část internetu, pro jejíž zpřístupnění je třeba specifického softwarového vybavení (např. Tor Browser) stejně tak, jako je třeba znát konkrétní URL případně IP adresu serveru. Darkweb je část tzv. Deepwebu⁵⁴, která je v současné době známa zejména díky jejímu spojení s páčáním trestné činnosti. Darkweb funguje prostřednictvím tzv. darknetu, tedy šifrované počítačové sítě, která je založena na specifických protokolech integrujících anonymizační funkce. Darknet je tedy založen na tom, aby byl anonymní.⁵⁵

1.1.8 Botnet

„Software, který slouží ke vzdálenému ovládnutí botů, které běží na infikovaných počítačích, a zajišťuje, že cracker má přístup k výpočetnímu výkonu mnoha strojů současně. Umožňuje provádět nezákonnou činnost ve velkém měřítku – zejména útoky DDoS a distribuci spamu.“⁵⁶ V posledních letech nebývá do sítě botnetů zařazena již jen klasická výpočetní technika jako stolní počítače, notebooky a mobilní telefony, ale do této sítě bývají čím dál častěji zařazovány také prvky IoT. Se stále rostoucím počtem používané výpočetní techniky rostou také velikosti jednotlivých botnetů, kdy v současné době lze na darkwebu objednat botnetovou síť pocházející z konkrétní země (např. z České republiky) tak, aby jednotliví provozovatelé služeb, na které předmětný botnet bude útočit, nemohli jednoduše odklonit provoz počítačové sítě dle země původu přístupů. Toto dříve byla velmi častá obrana proti tomuto typu útoku, kdy české internetové stránky odmítaly provoz z IP adres patřících do rozsahu cizích zemí (většinou vyjma Slovenské republiky).

⁵⁴ Deepweb je neindexovaná část internetu, která není běžnými vyhledávací dostupná, jedná se např. o různá fóra, firemní sítě apod.

⁵⁵ BHASKER, Das. *Darknet vs. Dark Web vs. Deep Web vs. Surface Web — The Difference*. Online. In: TechLog360, 16.03.2022. Dostupné z: <https://techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/>. [cit. 2023-10-05].

⁵⁶ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 39. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2023-09-11].

1.1.9 DoS a DDoS útoky

DoS útok ("denial of service") lze chápat jako potlačení určité služby. Jako cíl tohoto útoku má pachatel úplné vyřazení předmětné služby, případně snížení její kvality či výkonu. Nejčastěji pachatelé používají k takovému jednání opakující se požadavky, které musí systém vykonat. Díky velkému počtu takových úkonů v krátkých časových intervalech dojde k omezení výkonu nebo až k jeho celkovému zahlcení a vypnutí (přehřátí apod.).

Rozdíl mezi DoS a DDoS útokem je ve zdroji útoku, přičemž v případě DoS je jeden zdroj útoku a v případě DDoS ("distributed denial of service") jich je více. To fakticky znamená, že pachatel má pod svojí (alespoň dočasnou) kontrolou větší počet výpočetní techniky, která provádí více či méně koordinovaný útok.⁵⁷

1.1.10 Kyberstalking

Jak již název vypovídá, tak kyberstalking je nebezpečné pronásledování páchané prostřednictvím informačních a komunikačních technologií. Útočník typicky prostřednictvím těchto technologií dlouhodobě a opakovaně kontaktuje svoji oběť, kontaktování stupňuje a tímto jednáním se snaží o vyvolání pocitu strachu o soukromí, zdraví nebo život oběti. Typickými formami je obtěžování prostřednictvím elektronických zpráv (prostřednictvím nejrůznějších platform jako WhatsApp, Messenger, e-mailové zprávy aj.), ale také se setkáváme s formou příspěvků na sociálních sítích. Kyberstalking nelze vždy automaticky, i přes jeho neblahé účinky, kriminalizovat. Aby byl tento čin trestným, musí splňovat podmínky uvedené v § 354 trestního zákoníku. Motivy mohou být nejrůznější, od samotného obtěžování oběti, přes nucení, aby oběť něco konala, až po „obyčejné“ ukázání vlastní síly či postavení v kolektivu.⁵⁸

1.1.11 Kybergrooming

Kybergroomingem rozumíme navázání kontaktu dospělého s dítětem prostřednictvím informačních a komunikačních technologií, získání si důvěry oběti a její následná manipulace za účelem osobního setkání a sexuálního zneužití dítěte. S rozvojem nejrůznějších komunikačních aplikací a sociálních sítí dochází

⁵⁷ KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-18-8, str. 295-296.

⁵⁸ INTERNETEM BEZPEČNĚ. *Kyberstalking*. Online. In: INTERNETEM BEZPEČNĚ. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/>. [cit. 2024-02-04].

k jednoduššímu navázání kontaktu pachatele s dítětem. Dalším aspektem je skutečnost, že dítě si zřídka chrání své soukromí na jím užívaných sociálních sítích a dává tímto způsobem pachateli do rukou velké množství informací, které následně ke svému jednání může využít. Pachatel užívá velké množství smyšlených profilů na sociálních sítích, kdy se často vydává za osoby obdobného věku jako je jeho oběť, většinou opačného pohlaví. Po chvíli, kdy si pachatel s dítětem „nevinně“ dopisuje, přichází na řadu ujišťování, že jen pachateli záleží na dítěti, že jej chápe apod. Po získání si důvěry typicky dochází ze strany pachatele k získání intimních materiálů (většinou fotografií či videí) dítěte. Následuje fáze vydírání, kdy pachatel požaduje po oběti zaslání dalších intimních materiálů nebo požaduje rovnou osobní schůzku, a to pod výhrůžkou rozeslání již získaných materiálů blízkým kontaktům dítěte. Pachatel této činnosti vyniká velkou trpělivostí, kdy k získání důvěry dítěte je třeba mnohdy několik týdnů. Častým problémem u této činnosti je stud dítěte, které se s tímto problémem nesvěřuje primárně svým rodičům (či jakékoliv jiné dospělé osobě), ale v případě, že již někomu o tomto jednání řekne, pak jsou to typicky jeho kamarádi či vrstevníci. Díky tomu se dostává do stavu, kdy se domnívá, že z uvedeného jednání není jiná cesta než splnit podmínky pachatele.⁵⁹

1.1.12 Sexting

Jedná se o zasílání zpráv, fotografií, videosouborů či zvukových nahrávek se sexuálním podtextem prostřednictvím informačních a komunikačních technologií. Tento obsah, zasílaný primárně v rámci vztahu dvou (i více) osob, může být následně zneužit k nátlaku na osobu nebo k jejímu dalšímu poškození. U tohoto druhu komunikování je třeba si uvědomit všechna rizika spojená s touto činností. Setkáváme se také s případy, kdy na jedné straně sextingu je osoba, která si pouze zpestřuje vlastní život a osobu na druhé straně nijak nezná, ale i přes tuto skutečnost jí zašle vlastní intimní fotografie či videa, které jsou následně využity v rámci nejrůznějšího vydírání a také kybergroomingu.

⁵⁹ INTERNETEM BEZPEČNĚ. *Kybergrooming*. Online. In: INTERNETEM BEZPEČNĚ. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/>. [cit. 2024-02-04].

Se sextingem můžeme spojovat také platformy jako Onlyfans⁶⁰, Fansly⁶¹ či Fancetro⁶². Na těchto platformách neřídka kdy „umělci“ vkládají své intimní fotografie či videa, dopisují si se svými „fanoušky“ a inkasují za toto nemalé finanční částky.

V případě zveřejnění fotografií či videosouborů osob mladších 18 let se může jednat o naplnění skutkové podstaty trestného činu dle trestního zákoníku (typicky výroba a jiné nakládání s dětskou pornografií či zneužití dítěte k výrobě pornografie).

1.1.13 Stopa a důkaz

Kriminalistickou stopou rozumíme *jakoukoliv změnu příčinně souvislou s kriminalisticky relevantní událostí, která existuje nejméně od doby jejího vzniku do zajištění, která je současnými kriminalistickými metodami a prostředky vyhodnotitelná*.⁶³ Základní rozdělení stop je na paměťové a materiální. Paměťovými stopami rozumíme stopy zanechané ve vědomí člověka, typicky jde o zapamatování si určité události či její části. Materiální stopy vznikají působením pachatele či jím používaného předmětu na konkrétní objekt. Pro šetření na úseku kybernetické trestné činnosti a ostatní kriminality páchané v kyberprostoru pro nás budou stěžejní zejména stopy digitální.

Digitální stopou rozumíme „1. digitální informace nebo jakákoli data přenesená nebo uložená za použití počítačového systému; digitální stopa se zpravidla nachází na magnetickém, optickém nebo polovodičovém médiu nebo v prostředí datových sítí, 2. hmotný nosič digitální informace.“⁶⁴ Z uvedeného jasně vyplývá, že samotné médium (neboli hmotný nosič digitální informace) je také samotnou stopou. V praxi se totiž setkáváme se situací, kdy nejprve zajišťujeme médium, které následně vyhodnotíme, ohledáme apod. V takových případech je tedy digitální stopa a její hmotný nosič součástí jedna druhého.

⁶⁰ <https://onlyfans.com>

⁶¹ <https://fansly.com>

⁶² <https://fancetro.com>

⁶³ MUSIL, Jan, KONRÁD, Zdeněk a SUCHÁNEK, Jaroslav. *Kriminalistika*. 2. přepracované a doplněné vyd., Praha, C.H.Beck, 2004. ISBN 80-7179-878-9, str. 78.

⁶⁴ ČÁP, Jan plk. v. v. Mgr. *100 Bezpečnostní teorie a praxe 1/2022 informace – Zajišťování, zpřístupňování a vyhodnocování digitálních stop*. Online. PDF. In: Policejní akademie ČR, 06. 04. 2022. Dostupné z: <https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf>. [cit. 2023-11-23].

Trestně-právní teorie obecně uvádí, že jako důkaz může být v trestním řízení použito vše, co může přispět k objasnění věci. Zde bych rád doplnil, že důkaz však musí být procesně správně zajištěn. Za důkaz v trestním řízení považujeme zejména výslech svědka, výslech obviněného, znalecké posudky, protokol o ohledání, věci zajištěné dle § 78 trestního řádu. Avšak nejedená se o taxativní výčet.

1.1.14 Online platební metody

V současné době si každý člověk nakupující prostřednictvím internetu (či prostřednictvím této sítě provádějící jakoukoliv finanční transakci) může vybrat z velké nabídky online platebních metod. Ne každý provozovatel poskytuje stejnou škálu online platebních metod, ale mezi nejčastěji používané patří online bankovní převod, platba platební kartou, mobilní platby, platba prostřednictvím QR kódu, platba prostřednictvím služeb GooglePay (Google Peněženka), ApplePay, a samozřejmě také platby prostřednictvím platebních bran jako jsou GoPay, Comgate, PayU a PayPal. Mezi výhody těchto plateb patří zejména rychlost jejich připsání protistraně. Mezi jejich nevýhody však patří jejich velmi obtížné zablokování ze strany orgánů činných v trestním řízení, a to zejména s ohledem na již uvedenou rychlost připsání.

Další možnost skýtají kryptoměny. „*Kryptoměna je souborný název pro měny neregulované centrálními bankami. Kryptoměně se říká také crypto, cryptocurrency, kryptoměna nebo virtuální měna.*“⁶⁵ V současné době jich existuje již více jak 8 000⁶⁶. Mezi nejznámější měny řadíme Bitcoin, Ethereum, Tether USDt, BNB, Solana, Ripple, Dogecoin. Většina kryptoměn nemá pevně daný kurz, ale jsou velmi volatilní. Najdou se však i měny, které jsou závislé na kurzu fiat měny, např. jako Tether USDt, který je přímo závislý na kurzu USD. Kryptoměny jsou v dnešní době často používány jako výnos k páčání trestné činnosti, ale také jako investice.

1.1.15 OSINT a WEBINT

Termínem OSINT (Open Source Intelligence) rozumíme analýzu otevřených zdrojů. V této oblasti se jedná o shromáždění jednotlivých materiálů

⁶⁵ Česká spořitelna. *Co je kryptoměna*. Online. In: Česká spořitelna. Dostupné z: <https://www.csas.cz/cs/financni-slovník/kryptomeny>. [cit. 2024-02-23].

⁶⁶ Dle aplikace dostupné pro mobilní telefony CoinsData.io - <https://coinsdata.io>

k vyhledávanému tématu či osobě, a to jak na sociálních sítích, v novinových člancích, nejrůznějších internetových diskusích, tak ale také ve volně či internetem dostupných rejstřících. Největším zdrojem v dnešní době bývá právě internet, kdy veškeré materiály následně opatříme hodnocením věrohodnosti zdroje, případně dalšími poznámkami a nevěrohodné informace z následné analýzy odstraníme.⁶⁷

1.2 Počítačová gramotnost

Pojmem počítačová gramotnost je velmi nový, kdy tento chápeme jako schopnosti používat účelově a účinně jak počítač, tak mobilní telefon, tablet, případně další výpočetní techniku, ale také i např. počítačové sítě. Do tohoto používání začleňují jak správné využívání hardwaru, tak také správné používání softwaru. Z tohoto je vidno, že počítačová gramotnost velmi úzce souvisí s informačními a komunikačními technologiemi, které musí uživatel využívat v rozsahu, který mu umožní zjednodušení úkolu, či jeho zdárné vyřešení.

V současné době existuje certifikovaný projekt s názvem ICDL Europe, který ve svém popisu uvádí, že se zaměřuje na zavádění a zvyšování digitální kompetence v pracovním procesu, ve vzdělávání a ve společnosti.⁶⁸ Tento projekt „prostřednictvím mezinárodně jednotných sylabů definuje vzdělávací obsah, který odráží aktuální potřeby trhu práce a běžného života jedince ve společnosti, a to zejména v oblasti přenositelných digitálních znalostí a dovedností, a současně nabízí mezinárodně uznávanou, standardizovanou, objektivní a nezávislou metodu ověřování výsledků vzdělávání (tzv. ECDL zkoušky).“⁶⁹ Uvedený projekt tak vlastně unifikuje určitou úroveň počítačové gramotnosti v dané době.

1.2.1 Výpočetní technika

Jako výpočetní techniku v dnešní době chápeme hlavně stolní počítače a notebooky. Patří sem však i tablet, mobilní telefony, nejrůznější herní konzole, NAS a dokonce také chytré televize či lednice, kamery či chytré hodinky. Slovník

⁶⁷ NAJJAR, Shebab. *WEBINT in Action | Real-World Applications and Use Cases*. Online. In: Medium, 04. 05. 2023. Dostupné z: <https://osintteam.blog/webint-in-action-real-world-applications-and-use-cases-1c052530698b>. [cit. 2024-02-11].

⁶⁸ ICDL Europe. *About us*. Online. In: ICDL Europe. Dostupné z: <https://icdleurope.org/about-us/>. [cit. 2023-09-11].

⁶⁹ ECDL PROFILE. *O konceptu ECDL/ICDL*. Online. In: ECDL PROFILE. Dostupné z: https://www.ecdl.cz/o_projektu.php. [cit. 2023-09-11].

výpočetní techniky k této uvádí: „*Od poloviny 20.století však výpočetní techniku chápeme především v kontextu počítačů, resp. jejich jednotlivých částí, které slouží k početním operacím. Takovým výpočetním zařízením může být například router, server, pracovní stanice nebo přístupový bod bezdrátové sítě.*“⁷⁰ Prakticky můžeme říci, že v dnešní době jsme výpočetní technikou obklopeni na každém kroku.

1.2.2 Software

Jako software označujeme veškeré programové vybavení dané výpočetní techniky. Uvedené programy jsou typicky určeny k vykonávání konkrétních úloh, případně umožňují zpracování dat. Podle Jirásk a spol. jej můžeme dělit na systémový software, aplikační software a firmware. Do systémového softwaru typicky řadíme jednotlivé operační systémy, a to ať v jejich grafické podobě (např. Microsoft Windows, Google Android, iOS), tak také v jejich negrafické (dalo by se téměř říci textové) podobě (např. MS DOS, některé distribuce Linuxu). Tento systémový software umožňuje uživateli ovládat konkrétní kus výpočetní techniky bez toho, aby měl k dispozici jakýkoliv další software. Bez systémového softwaru nejsme také schopni používat aplikační software. Do aplikačního softwaru řadíme jednoduché aplikace (např. program na vypnutí či uspání počítače – PowerOff), ale také komplexnější programy (např. kancelářské balíky, grafické editory⁷¹). Mezi aplikační software řadíme také ovladače. Ovladač je program umožňující komunikaci mezi operačním systémem a hardwarovou komponentou. Bez ovladače by danou hardwarovou komponentu nemohl operační systém správně používat. Firmwarem je oproti tomu ovládací program konkrétního kusu hardwaru. Bez tohoto by hardware nepracoval správně, či vůbec. Firmware obsahují např. základní desky, harddisky, procesory, ale také kalkulačky, digitální fotoaparáty apod. Je úzce spjat s konkrétním hardwarem, a provádí pouze základní úkoly dané hardwarové komponenty. Mohlo by se zdát, že firmware a ovladač jsou téměř to samé a měli bychom je řadit do totožné skupiny softwaru, ale rozdíl mezi firmwarem a ovladačem je v tom, že firmware umožňuje pouze základní úkoly,

⁷⁰ Infoz.cz Slovník cizích slov. *Slovník výpočetní techniky*. Online. In: Infoz.cz slovník cizích slov. Dostupné z: <https://www.infoz.cz/slovník-vypocetni-techniky/>. [cit. 2023-11-17].

⁷¹ Grafický editor je software umožňující zpracovávání a upravování fotografií a dalších grafických souborů.

kdežto ovladač je software umožňující komunikaci s konkrétním operačním systémem (a nezdá se, že se správným ovladačem jsme schopni daný kus hardwaru využít lépe a účelně – např. u grafických karet je toto velmi markantní).⁷²

1.2.3 Hardware

Jakékoliv jednotlivé technické vybavení daného kusu výpočetní techniky či jeho část. Mezi hardware řadíme např.:

- paměť RAM, neboli operační paměť – *„paměť určená pro čtení i zápis, po přerušení dodávky elektrického proudu se obsah dat vymaže“*⁷³, musíme mít na paměti, že dodávka elektrického proudu může být přerušena do této paměti každým vypnutím počítače,
- procesor – *„Elektronický obvod, který provádí operace na některém externím zdroji dat, obvykle paměti nebo jiném datovém toku. Termín je často používán k odkazování na centrální procesor v systému, ale typické počítačové systémy kombinují řadu specializovaných „procesorů.“ Z dnešního pohledu pojem "Mikroprocesor" označuje to samé.“*⁷⁴
- Základní deska – *„Spojuje všechny ostatní komponenty, zprostředkovává napájení, umožňuje přenosy dat. Některé části jsou na ní pevně uchyceny (procesor, paměti, grafická karta) a jiné jsou s ní spojeny pomocí kabelů (harddisky, DVD mechanika apod.).“*⁷⁵
- Grafická karta – *„Zařízení, které je zpravidla uvnitř počítače v podobě zásuvné karty (i když dnes je často integrována přímo na základní desce) a slouží ke grafickým výpočtům a vytváření grafického výstupu na monitor. Existují i grafické karty umožňující vstup, taková funkce se nazývá VIVO.“*⁷⁶

⁷² JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 172-173. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2023-09-11].

⁷³ IT Slovník. *Co je to RAM?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/ram>. [cit. 2024-02-23].

⁷⁴ IT Slovník. *Co je to procesor?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/procesor>. [cit. 2024-02-23].

⁷⁵ IT Slovník. *Co je to Základní deska?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/zakladni-deska>. [cit. 2024-02-23].

⁷⁶ IT Slovník. *Co je to Grafická karta?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/graficka-karta>. [cit. 2024-02-23].

- Pevný disk - *"Často též "harddisk" - magnetické zařízení fungující na principu magnetického zápisu používané v počítači k trvalému uchování většího množství dat."*⁷⁷
- Chipset - *"Neboli čipová sada je označení sadu integrovaných obvodů, které jsou navrženy pro společnou spolupráci. Obvykle jsou prodávány jako jeden produkt. Příkladem může být procesor a podpůrné obvody na základní desce (severní a jižní můstek)."*⁷⁸
- Baterie,
- ale také jednotlivé periferie⁷⁹ jako například monitor, klávesnice, webová kamera, snímač otisků prstů, externí paměťové úložiště, modem atd.

U síťového hardwaru pro nás může být důležitá také MAC adresa. *„Adresa MAC je jedinečný identifikátor, který přiřadil výrobce danému kousku síťového hardwaru (jako jsou karty Wi-Fi nebo Ethernet). MAC je zkratka z Media Access Control a cílem je jednoznačná identifikace konkrétního zařízení. Adresa MAC sestává ze sady šesti dvojic znaků (šestnáctkových číslic), oddělených dvojtečkami. Příkladem adresy MAC může být 00:1B:44:11:3A:B7.“*⁸⁰ U MAC adresy musíme mít na paměti, že v některých případech tuto můžeme změnit.

1.2.4 Počítačová síť

Kolouch ve své knize CyberCrime uvádí, že existuje množství definic toho, co je počítačová síť. Jako nejjednodušší, a pro tuto práci zcela dostačující jsem zvolil definici, která uvádí, že počítačová síť chápeme jako *„soubor (množinu) počítačových systémů, které jsou navzájem propojeny a mezi nimiž dochází k výměně dat či informací.“*⁸¹ Domnívám se, že pro samotné pochopení počítačové sítě pak není zcela důležité znát jednotlivé dělení počítačové sítě jako takové, avšak je třeba umět se orientovat nejméně v některých druzích, jako jsou LAN (a s ní související privátní síť), P2P, veřejnou síť a VPN.

⁷⁷ IT Slovník. *Co je to Pevný disk?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/pevny-disk>. [cit. 2024-02-23].

⁷⁸ IT Slovník. *Co je to chipset?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/chipset>. [cit. 2024-02-23].

⁷⁹ Zařízení připojující se k počítači (dříve kabelem, dnes také bezdrátově).

⁸⁰ MCCANCE, Shaun, CAMPBELL, Jim, HILL, Michael a GERASIMOVA, Ekaterina. *Co je to MAC adresa*. Online. In: GNOME HELP. Dostupné z: <https://help.gnome.org/users/gnome-help/stable/net-macaddress.html.cs>. [cit. 2024-02-11].

⁸¹ KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-18-8, str. 67.

LAN (Local Area Network) je místní síť, typicky se může jednat o podnikovou síť (například intranet u Policie ČR), se kterou jsme se setkávali dříve v rámci domácností při hraní počítačových sítí u tzv. LAN party (hráči nejsou připojeni prostřednictvím sítě internet, ale napřímo prostřednictvím síťového zařízení – např. switch – a síťového kabelu). LAN se v dnešní době používá také v rámci spojení jednotlivých kusů výpočetní techniky prostřednictvím Wi-Fi routeru. LAN používá privátní IP adresy (např. 192.168.1.1., 192.168.1.2), které jsou ručně či automaticky (nejčastěji routerem) nastaveny v jednotlivých zařízeních. V případě, že tato privátní síť chce využívat připojení do sítě internet, musí používat překlad síťových adres (tzv. NAT).

P2P (Peer-to-Peer) je síť, kdy jednotlivá zařízení jsou spojena přímo mezi sebou (často prostřednictvím síťového kabelu, Bluetooth spojení či NFC⁸²) a tímto způsobem spolu komunikují.

Veřejnou sítí je síť, která je „otevřena nejširší veřejnosti, které nabízí své služby spočívající v přenosu dat. Uživatelem takovéto sítě se skutečně může stát kdokoli, kdo o to má zájem a je ochoten za to zaplatit, resp. přistoupit na podmínky toho, kdo takovou síť provozuje. Provozovatelem přitom bývá takový subjekt, který svou datovou sítí nepoužívá – vlastní ji a provozuje především proto, aby její služby mohl poskytovat na komerční bázi jiným subjektům.“⁸³

VPN (Virtual Private Network) je zkratka pro virtuální privátní síť. Jedná se o privátní počítačovou síť, „která dovolí připojit vzdálené uživatele do cílené LAN přes Internet. Bezpečnost se řeší pomocí šifrovaného tunelu mezi dvěma body (nebo jedním a několika). Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů.“⁸⁴

⁸² Near Field Communication již ze svého názvu znamená, že se jedná o komunikaci na krátkou vzdálenost. Konkrétně se jedná o komunikaci mezi zařízeními na vzdálenost 4 cm. Obě zařízení, která spolu komunikují musí být vybavena tzv. NFC čipem. V současné době je NFC využíváno zejména k bezkontaktním platbám prostřednictvím mobilních telefonů, hodinek apod.

⁸³ PETERKA, Jiří. *Terminologie datových sítí*. Online. In: eARCHIV, březen 2000. Dostupné z: <http://www.earchiv.cz/b00/b0003002.php3>. [cit. 2024-01-29].

⁸⁴ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 204. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2023-09-11].

1.2.5 NAT

Jedná se o zkratku vyjadřující překlad síťových adres (Network Address Translation). „*Mechanismus umožňující přístup více počítačů z lokální sítě do Internetu pod jedinou veřejnou IP adresou. Počítače z lokální sítě mají přiděleny tzv. privátní IP adresy. Hraniční prvek takové lokální sítě zajišťuje překlad privátních IP adres na veřejnou.*“⁸⁵ Překlad síťových adres primárně vznikl v důsledku velmi rychle se blížícího vyčerpání IP adres verze 4, kdy tímto způsobem narostl možný počet připojených zařízení do sítě internet. I v současné době je tento překlad velmi často využíván, ať již u provozovatelů mobilních sítí⁸⁶, nebo také u poskytovatelů internetového připojení⁸⁷.

1.2.6 Protokol, internetový protokol, IP adresa a port

„*Protokolem v IT se rozumí standard dvou zařízení (nejčastěji mezi dvěma servery neboli počítači), na kterém se dohodli daní výrobci, že zařízení budou takto fungovat. Jedná se tedy o nalezení vhodné interoperability⁸⁸ pro jejich vzájemnou komunikaci. Interoperabilní protokoly poté řídí komunikaci mezi elektronickými prvky sítě a vše další, co obecně ke komunikaci serverů patří. Protokoly mohou být tvořeny libovolně, hardwarově i softwarově. Zřejmě nejznámějším protokolem je TCP/IP, který zajišťuje vhodnou síťovou komunikaci a v širším měřítku i Internet, tak jak ho uživatelé dobře znají. V rodině protokolů TCP/IP je dále např. IP neboli internetový protokol, TCP komunikační protokol či UDP. V rámci podstatných služeb a funkcí samotného Internetu se dále hojně používají například aplikační protokol HTTP či pro elektronickou poštu nezbytné protokoly POP3 a IMAP. Všechny existující protokoly disponují standardizovaným číslem síťového portu, na kterém vykonávají svou činnost.*“⁸⁹

⁸⁵ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 147-148. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2023-09-11].

⁸⁶ Např. O2, Vodafone či T-Mobile a další virtuální operátoři

⁸⁷ Např. O2, Vodafone, T-Mobile či další lokální poskytovatelé jako PilsFree, Mraknet apod.

⁸⁸ Schopnost odlišných systémů mezi sebou spolupracovat.

⁸⁹ SPRÁVA SÍTĚ slovník pojmů. *Co je to protokol*. Online. In: SPRÁVA SÍTĚ slovník pojmů. Dostupné z: <https://www.sprava-site.eu/protokol/>. [cit. 2024-02-02].

„Hypertext transfer protocol (HTTP) Aplikační protokol pro distribuované, kolaborativní, multimediální informační systémy. HTTP je základem datových přenosů pro celosvětovou síť WWW. Hypertext transfer protocol secure (HTTPS) Široce používaný komunikační protokol pro bezpečnou komunikaci přes počítačovou síť, zvláště široce používán na Internetu. Technicky se nejedná o protokol jako takový, spíše je výsledkem prostého vrstvení protokolu HTTP na protokol SSL/TLS⁹⁰ a tak dodává standardní komunikaci HTTP ještě bezpečnostní možnosti.“⁹¹

Pro účely této práce zmíním ještě File transfer protocol (FTP), kdy se jedná o protokol pro přenos souborů mezi serverem a uživatelem.

Internetový protokol (IP) je soubor pravidel a konvencí, „pomocí kterého spolu komunikují všechna zařízení na internetu“.⁹²

Kdežto IP adresa identifikuje konkrétní zařízení v síti. Aktuálně jsou využívány dvě verze IP adresy, a to verze 4 (IPv4) a verze 6 (IPv6). IPv4 je tvořen celkem čtyřmi troj číselnými sekvencemi navzájem oddělenými tečkami, přičemž nejvyšší číslo v sekvenci může dosahovat hodnoty 255. Jakmile se objeví ve kterékoliv sekvenci hodnota vyšší než 255 pak nedává smysl a nelze se prostřednictvím tohoto připojit do sítě internet. Stejně tak musíme mít na paměti, že část rozsahu z IPv4 byla ponechána k využití privátním sítím (viz. Příloha č. 2) a další část byla rezervována pro speciální účely (viz. Příloha č. 3). Proto je třeba si vždy IP adresu ověřit u oficiálního zdroje, kterým je pro Evropu subjekt RIPE NCC.⁹³ IPv6 je tvořen celkem osmi čtyřmístnými sekvencemi navzájem oddělenými dvojtečkami, kdy jednotlivé sekvence mohou obsahovat písmena i číslice. Dále nesmíme

⁹⁰ SSL a TLS jsou protokoly poskytující zabezpečení komunikace šifrováním a autentizací vzájemně komunikujících stran.

⁹¹ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 73-74. Dostupné z Národního úřadu pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podperne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2024-02-02].

⁹² JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 83. Dostupné z Národního úřadu pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podperne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2023-09-11].

⁹³ www.ripe.net

zapomínat, že IP adresy lze zapsat s vynecháním číslovky 0 na desítkové a stovkové pozici, např. IPv4 128.028.000.255 lze zapsat jako 128.28.0.255; u IPv6 lze číslovku 0 vynechat zcela, např. 2001:0db8:85a3:0000:0000:8a2e:0370:7334 lze zapsat 2001:0db8:85a3::8a2e:0370:7334. S IP adresou také velmi blízce souvisí termín DNS (Domain Name System). Tento nám zjednodušuje návštěvy oblíbených internetových portálů a adres, které z IP adresy překládá na slovní vyjádření. Např. IP adresa portálu www.seznam.cz byla dne 11. 02. 2024 ve 13:24 hodin 77.75.77.222. Pokud bychom toto ukázali na příkladu, tak ve chvíli, kdy by neexistoval DNS, pak bychom do adresního řádku internetového prohlížeče museli zadávat konkrétní IP adresu pro přístup na tuto stránku, avšak díky DNS zde napíšeme jen www.seznam.cz (případně seznam.cz) a DNS nás automaticky přesměruje na správnou IP adresu.

Port se „*používá při komunikaci pomocí protokolů TCP či UDP. Definuje jednotlivé síťové aplikace běžící v rámci jednoho počítače. Může nabývat hodnot v rozmezí 0–65535. Například webové stránky jsou obvykle dostupné na portu 80, server pro odesílání mailové pošty na portu 25, ftp server na portu 21. Tyto hodnoty je možné změnit a u některých síťových služeb správci někdy záměrně nastavují jiná než běžně používaná čísla portů kvůli zmatení případného útočníka.*“⁹⁴

1.2.7 Internetový prohlížeč a cookies

Internetovým prohlížečem je jakýkoliv software, který nám po zadání příslušné URL⁹⁵ adresy zobrazí její obsah. V současné době existuje velké množství internetových prohlížečů, např. Microsoft Edge, Mozilla Firefox, Safari, Chrome, Opera apod. Mezi internetové prohlížeče řadíme i specializovaný prohlížeč Tor Browser. Internetové prohlížeče můžeme v rámci prověřování trestné činnosti využívat k ustanovení osoby, která danou výpočetní techniku v konkrétní době užívala, a to zejména díky informacím obsaženým v historii internetových

⁹⁴ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 130-131. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2024-02-02].

⁹⁵ Uniform resource locator – Zdrojový identifikátor popisující umístění zdroje a protokolu k jeho správnému načtení. Příkladem URL je třeba www.seznam.cz

prohlížečů. K internetovému prohlížeči, respektive spíše k internetové stránce, se váže také pojem HTML. Jedná se o zkratku Hypertext Markup Language a jedná se o jazyk pro tvorbu internetových stránek a internetových aplikací.

Tor Browser je specializovaný internetový prohlížeč, který umožňuje přístup (vyjma standardních stránek, které zobrazují i ostatní internetové prohlížeče) ke stránkám dostupným na Darkwebu. Tento prohlížeč při jeho správném nastavení umožňuje také zcela anonymní procházení internetu. Uživatel tohoto prohlížeče přistupuje k příslušným stránkám způsobem, že je dotaz k vyvolání stránky přesměrován mezi množstvím dalších klientů Tor sítě (viz. Obrázek č. 3). K velké nevýhodě tohoto prohlížeče patří zejména jeho velká doba načítání stránek (= velká latence).

S internetovým prohlížečem úzce souvisejí také tzv. cookies. Cookies jsou „*Data předaná mezi HTTP serverem a prohlížečem za účelem uchování stavové informace na straně klienta, která může být později vyzvednuta a využita http serverem. Cookie se dnes nejčastěji používá pro rozpoznání uživatele, který již aplikaci dříve navštívil, nebo pro ukládání uživatelského nastavení webové aplikace. Dnes jsou často diskutovány v souvislosti se sledováním pohybu a zvyklostí uživatelů některými weby.*“⁹⁶

1.2.8 Internet Service Provider (ISP)

ISP poskytují jednotlivé služby v rámci internetu. V dřívější době se za ISP považovali pouze poskytovatelé internetového připojení a zajišťující tedy koncovým uživatelům konektivitu. V současné době však zahrnuje další fyzické a právnické osoby (poskytovatele služby) poskytující další služby v prostředí internetu jako jsou cloudová úložiště, e-mailové schránky, sociální sítě, VoIP aj. V ČR se legislativně používá pojem poskytovatel služby informační společnosti. Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů⁹⁷ uvádí, že službou informační společnosti je „*jakákoliv služba poskytovaná elektronickými prostředky na individuální žádost uživatele podanou*

⁹⁶ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 44. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2024-02-02].

⁹⁷ Dále jen zákon o některých službách informačních společnosti

*elektronickými prostředky, poskytovaná zpravidla za úplaty; služba je poskytnuta elektronickými prostředky, pokud je odeslána prostřednictvím sítě elektronických komunikací a vyzvednuta uživatelem z elektronického zařízení pro ukládání dat*⁹⁸ a elektronickými prostředky jsou „zejména síť elektronických komunikací, elektronická komunikační zařízení, automatické volací a komunikační systémy, telekomunikační koncová zařízení a elektronická pošta“⁹⁹. Uživatelem pak může být jakákoliv fyzická či právnická osoba využívající službu informační společnosti.

1.2.9 Elektronická pošta, e-mailová adresa a e-mailová zpráva

Zákon o některých službách informačních společností uvádí, že elektronickou poštou je *„textová, hlasová, zvuková nebo obrazová zpráva poslaná prostřednictvím veřejné sítě elektronických komunikací, která může být uložena v síti nebo v koncovém zařízení uživatele, dokud ji uživatel nevyzvedne*¹⁰⁰.

Mezi elektronickou poštou můžeme zařadit také datovou zprávu. Zákon o elektronických úkonech a autorizované konverzi dokumentů definuje datovou schránku jako: *„elektronické úložiště, které je určeno k doručování orgány veřejné moci, provádění úkonů vůči orgánům veřejné moci, dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob*“¹⁰¹

Pokud se budeme bavit o e-mailové adrese a e-mailové zprávě, pak v rámci výkladů a judikatury je pro policisty stěžejní názor, který vyjádřilo Trestní kolegium Nejvyššího soudu České republiky se ve svém stanovisku sp. zn. Tpjn 300/2012. *„Tzv. e-mailová adresa představuje elektronickou službu spočívající v elektronické poště, která je definována jako telekomunikační služba instalovaná převážně na standardních počítačových sítích, určena k přenosu zpráv mezi počítačovými pracovišti, k ukládání těchto zpráv do paměťových schránek, k třídění*

⁹⁸ Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). Online. Dostupné z: <https://www.zakonyprolidi.cz/cs/2004-480>. [cit. 2024-02-02].

⁹⁹ Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). Online. Dostupné z: <https://www.zakonyprolidi.cz/cs/2004-480>. [cit. 2024-02-02].

¹⁰⁰ Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). Online. Dostupné z: <https://www.zakonyprolidi.cz/cs/2004-480>. [cit. 2024-02-02].

¹⁰¹ Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů. Online. Dostupné z: <https://www.zakonyprolidi.cz/cs/2008-300#p2>. [cit. 2024-02-02].

a předzpracování zpráv.“¹⁰² „Zprávou se rozumí jakákoliv informace, která se vyměňuje nebo přenáší mezi konečným počtem účastníků nebo uživatelů, pokud ji jde přiřadit k určitému účastníkovi nebo uživateli, který tuto informaci přijímá (§ 89 odst. 2 zák. č. 127/2005 Sb.).“¹⁰³ „Vedle toho je možno ještě uvést, že ve výše uvedeném smyslu by bylo možno považovat elektronickou poštu (e-mail) za určitou část jinak veřejně přístupné počítačové sítě (tedy tzv. podsít), která veřejně přístupná není.“¹⁰⁴

E-mailová adresa je pak např. petr.novak@axapela.cz. E-mailovou zprávu tvoří hlavička zprávy, tělo zprávy a případně přílohy ke zprávě.

Hlavička zprávy obsahuje odesilatele zprávy, příjemce zprávy, předmět zprávy, datum a čas odeslání zprávy a údaje o poštovních serverech. Hlavička je částečně viditelná ve většině poštovních aplikací (ať internetových, tak lokálních), kdy ale pro její kompletní zobrazení musíme zobrazit zdrojový kód zprávy. Ve zdrojovém kódu zprávy pak vidíme, jak předmětná zpráva putovala z jednoho poštovního serveru ke druhému a zřídka kdy zde můžeme také vidět IP adresu uživatele, který příslušnou zprávu odeslal. Tělem zprávy rozumíme konkrétní obsah sdělení uvedený ve zprávě (ale tento může také zcela absentovat). Přílohami jsou např. obrázek přiložený jako soubor ke konkrétní e-mailové zprávě. E-mailovou poštu můžeme používat jak prostřednictvím webových rozhraní konkrétního poskytovatele, tak také prostřednictvím poštovního klienta, jako je např. Mozilla Thunderbird. Při nastavování poštovního klienta však musíme znát několik pojmů. Konkrétně se jedná o 3 protokoly:

- SMTP (Simple Mail Transfer Protocol) – „internetový protokol určený pro přenos zpráv elektronické pošty. Popisuje komunikaci mezi poštovními servery.“¹⁰⁵

¹⁰² Rozhodnutí Nejvyššího soudu Tpjn 300/2012, ze dne 30. 1. 2013. Online. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/510D3BBA2FD98693C1257B2B0054DA9B?open-Document&Highlight=0. [cit. 06. 12. 2023].

¹⁰³ Rozhodnutí Nejvyššího soudu Tpjn 300/2012, ze dne 30. 1. 2013. Online. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/510D3BBA2FD98693C1257B2B0054DA9B?open-Document&Highlight=0. [cit. 06. 12. 2023].

¹⁰⁴ Rozhodnutí Nejvyššího soudu Tpjn 300/2012, ze dne 30. 1. 2013. Online. Dostupné z: http://www.nsoud.cz/Judikatura/judikatura_ns.nsf/WebSearch/510D3BBA2FD98693C1257B2B0054DA9B?open-Document&Highlight=0. [cit. 06. 12. 2023].

¹⁰⁵ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF.Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 166. Dostupné z Národní úřad

- POP3 (Post Office Protocol) – „název pro aktuální verzi internetového protokolu, který neustále stahuje nové e-mailové zprávy ze vzdáleného serveru. Po přijetí všech zpráv jsou následně na vzdáleném serveru zprávy smazány, což je hlavní rozdíl oproti protokolu IMAP, kde kopie zůstávají do té doby, dokud je samotný uživatel fyzicky nesmaže.“¹⁰⁶
- IMAP (Internet Message Access Protocol) – „je určen pro vzdálený přístup k uživatelské e-mailové poště přes poskytnutí služby e-mailového klienta. Jeho hlavní odlišení od serveru POP3 je to, že veškeré došlé e-maily nejsou v momentě jejich stažení automaticky smazány, ale naopak se uchovávají kopie.“¹⁰⁷

1.2.10 Sociální síť

Mohlo by se zdát, že je pojem sociální síť v současné době již brán jako notorieta, ale s ohledem na zkušenosti jsem se rozhodl zde zařadit i tento pojem. Běžně bereme jako sociální sítě pojmy jako Facebook, SnapChat, Instagram, ale velké množství osob si neuvědomuje, že pod pojem sociální síť patří také komunikátory jako WhatsApp, Signal či Meet. Sociální síť je služba, prostřednictvím které můžeme komunikovat, sdílet informace a data. Společné pro sociální sítě je pak vytvoření profilu, prostřednictvím kterého následně komunikujeme. Uvedený profil může být spjat s e-mailovou adresou, telefonním číslem případně jiným již zaregistrovaným profilem. Encyklopedie Britannica pak sociální síť definuje jako „online komunitu jednotlivců, kteří si vyměňují zprávy, sdílejí informace a v některých případech spolupracují na společných aktivitách. Sociální sítě a sociální média jsou překrývající se pojmy, ale sociální sítě jsou obvykle chápány jako uživatelé, kteří mezi sebou vytvářejí komunity, zatímco sociální média jsou spíše o používání stránek sociálních sítí a souvisejících platforem k budování publika“¹⁰⁸.

pro kybernetickou a informační bezpečnost:
https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2024-02-02].

¹⁰⁶ SPRÁVA SÍTĚ slovník pojmů. *Co je to POP3*. Online. In: SPRÁVA SÍTĚ slovník pojmů. Dostupné z: <https://www.sprava-site.eu/pop3/>. [cit. 2024-02-02].

¹⁰⁷ SPRÁVA SÍTĚ slovník pojmů. *Co je IMAP*. Online. In: SPRÁVA SÍTĚ slovník pojmů. Dostupné z: <https://www.sprava-site.eu/pop3/>. [cit. 2024-03-06].

¹⁰⁸ RAY, Michael. *social network computing*. Online. In: Encyklopedie Britannica, 09. 01. 2024. Dostupné z: <https://www.britannica.com/technology/social-network>. [cit. 2024-02-02].

1.2.11 Logovací soubory

Jirásek je ve své publikaci definuje jako „*Soubor obsahující informace o aktivitách subjektů v systému, přístup k tomuto souboru je řízen.*“¹⁰⁹ Pro policejní praxi v oblasti kybernetické trestné činnosti jsou logovací soubory jednou z nejdůležitějších „studnicí informací“. Logovací soubory mohou vznikat závisle, ale i nezávisle, na přání uživatele výpočetní techniky. V těchto se typicky zapisuje informace o IP adrese, přihlášeném uživateli a provedené akci. Může také obsahovat informace o použitém portu. Takové informace jsou pak velmi často využitelné alespoň pro zúžení okruhu podezřelých osob, v některých případech dokonce k ustanovení konkrétního zájmového koncového zařízení. Pro představu je v Příloze č. 4 přiložen náhled části logovacího souboru mého domácího NAS od společnosti Asus. Je také mít na paměti, že logovací soubory mohou být povrženy nebo záměrně změněny pachatelem či dokonce smazány.

1.2.12 EXIF data

„*EXIF (Exchangeable image file format) data jsou data, které vkládají do souborů digitální fotoaparáty. EXIF je formát dat, respektive metadat, která slouží jako nositelé informací. Do běžných souborových formátů, jako je JPEG, TIFF či RIFF, je automaticky vkládají digitální fotoaparáty a moderní kamery. Tato metadata obsahují konkrétní informace o daném fotoaparátu, místě pořízení fotografie a další důležité poznatky. Konkrétně se jedná o značku a model fotoaparátu, datum a čas pořízení snímku, nastavení fotoaparátu (citlivost, jas, použití či nepoužití blesku, zaostření apod.), náhled snímku, místo pořízení snímku (skrze GPS družice) a případné autorovy poznámky.*“¹¹⁰ EXIF data mohou být pro policistu velmi užitečné s ohledem na skutečnost, že v těchto lze nalézt informace o konkrétním zařízení (jako jsou sériové číslo, typ aj.), které vyfotografovalo zájmovou fotografii. Stejně tak je možné v něm nalézt GPS souřadnice, kde došlo k vyfotografování (či poslední zaznamenanou pozici fotografujícího zařízení) dané

¹⁰⁹ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 174. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost: https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2024-02-02].

¹¹⁰ IT SLOVNÍK.cz. *Co znamená zkratka EXIF?* Online. In: IT SLOVNÍK.cz. Dostupné z: <https://it-slovník.cz/pojem/exif>. [cit. 2024-02-03].

fotografie. Je třeba si opět uvědomit, že uvedené informace jsou velmi snadno změnitelné a nelze je tak brát jako nezměnitelné. Jsou upotřebitelné zejména s ohledem na další zjištěné informace, případně ve chvíli, kdy se nám podaří zajistit fotoaparát, a chceme se pokusit zjistit, zda to opravdu není zařízení, které zájmovou fotografii provedlo. V obrazové příloze je pod Obrázek č. 4 a Obrázek č. 5 uvedený náhled EXIF dat z fotografického editor Zoner Photo Studio X. Dále je třeba si uvědomit, že pro zobrazení kompletních EXIF dat nám nepostačí jejich zobrazení ve standardním prohlížeči fotografií integrovaným do operačního systému Microsoft Windows, ale je vhodné stáhnout si program přímo zobrazující EXIF data případně jakýkoliv fotografický editor. Jako Obrázek č. 6 a Obrázek č. 7 je zobrazen náhled vlastností dostupný standardně v systému Microsoft Windows totožného obrázku ke komparaci zjištěných informací. Stejně tak je nutné mít na paměti, že většina (ne-li všechny) běžně používaných sociálních sítí tato EXIF data při nahrání fotografií na servery mažou.

1.2.13 IoT

Internet věcí (Internet of Things - IoT) je síť vzájemně propojených zařízení, jenž si mezi vyměňují data mezi sebou a cloudem. Tato zařízení jsou obvykle vybaveny senzory a softwarem, ale mohou obsahovat mechanické a digitální součásti. Data jsou přenášena prostřednictvím počítačové sítě bez jakéhokoliv zásahu člověka (vyjma prvotní konfigurace). Do této kategorie může spadat jak srdeční monitor či biočip, tak také automobilové senzory (např. tlak v pneumatikách), ale také klidně lednice, mikrovlnná trouba či okno. Prakticky sem můžeme řadit jakékoliv zařízení, kterému můžeme přiřadit IP adresu a je schopno přenášet data prostřednictvím počítačové sítě. V současné době je IoT využíván ve velké míře v rámci tzv. chytré domácnosti. Tato domácnost se většinou sestává z několika samostatných prvků zařazených do jedné obslužné a řídicí aplikace. V rámci chytré domácnosti je obslužná aplikace schopna vyvětrat otevřením oken v nastavení čas (nastavenou teplotou nebo vlhkostí), zatopit, upozornit na zaplněný odpadkový koš, uvařit oblíbený druh kávy apod. Samozřejmě s každou technologií, která je připojena k internetu (zejména s ohledem na to, abychom mohli svoji domácnost online sledovat), přichází riziko napadení jednotlivých prvků. V dnešní době jsou jednotlivé prvky IoT velmi často napadeny při využití v rámci botnetu k dalším útokům. I v případě IoT musíme mít na paměti (byť to mnohdy může být

nepravděpodobné), že jakékoliv zařízení, které má vlastní obslužnou aplikaci a současně je toto zařízení připojené k internetu, má s největší pravděpodobností možnost provedení logování a díky tomu jsme z takového zařízení v případě potřeby schopni získat také logovací soubory.¹¹¹

1.2.14 NAS

NAS je zkratkou pro Network Attached Storage. Již ze samotného překladu je patrné, že se jedná o úložiště připojené k síti (počítačové). Samozřejmostí je pak také to, že musí obsahovat úložiště. V současné době je ukládací prostor řešen pevným diskem, stále častěji se však setkáváme s obsaženým SSD diskem¹¹². Ještě do nedávné doby byly NAS zařízení spíše záležitostí společností či podnikatelů, ale s rozvojem a zpřístupňováním jednotlivých zařízení široké veřejnosti, se i NAS dostává stále častěji do běžných domácností. NAS je primárně určen k zálohování či archivování uživatelsky důležitých dat a informací. NAS může, ale nemusí, být připojen k síti internet, kdy v případě připojení k internetu je zde riziko napadení tohoto zařízení ze strany pachatele, který tak může získat citlivé informace o uživateli či napadené společnosti, případně tato data zašifrovat či jakkoliv jinak kompromitovat. Výhodou tohoto systému je přístup na jedno zařízení ze strany prakticky neomezeného počtu uživatelů, a to i současně. Data si pak uživatelé mohou, dle nastavení, zpřístupnit jen vlastní, cizí či kombinací uvedeného. Stejně tak je možné toto zařízení používat jako úložiště záznamů z bezpečnostních či domácích kamer.

1.2.15 Hash

Jirásek ve své publikaci uvádí definici hash funkce jako „*Jednosměrná matematická transformace vstupních dat (textu) do souboru (otisk, hash). Matematicky je prakticky nereálné získat z otisku zpět vstupní data. Tato funkce je využívána v aplikacích zabezpečení dat (například autentizace, digitální podpis, kontrola integrity). Porušení bezpečnosti hash funkce je označováno jako kolize.*“¹¹³ Prakticky tedy hash ověřuje integritu obsahu souboru, ze kterého je

¹¹¹ GILLIS, Alexander S. *internet of things (IoT)*. Online. In: TechTarget, srpen 2023. Dostupné z: <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>. [cit. 2024-02-03].

¹¹² Solid state drive

¹¹³ JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Online, PDF. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0, str. 70. Dostupné z Národní úřad pro kybernetickou a informační bezpečnost:

vypočítán. V praxi to znamená, že v případě textového souboru postačuje změna jednoho znaku či přidání jedné mezery a hash, který je vypočítán z daných textových souborů, bude zcela jiný. Naproti tomu pokud totožný soubor pouze přejmenujeme, bez toho, abychom v jeho obsahu cokoliv jiného měnili, tak hash, vypočítaný ze souboru s původním názvem, bude totožný, jako hash vypočítaný ze souboru se změněným názvem. Hashovací funkce se v současné době využívá při předkládání či vydávání věcí v rámci trestních řízení, kdy touto funkcí ověřujeme, že ze strany policisty (či kohokoliv jiného) nedošlo k zásahu do obsahu dat, která byla vydána. V současné době doporučujeme vypočítat hash pomocí 2 různých algoritmů¹¹⁴.

1.2.16 Vzdálená správa počítače

Vzdálená správa počítače je již dlouhá léta využívána v komerční sféře, kdy pro pracovníky IT oddělení je mnohem rychlejší (a většinou také snadnější) vyřešit problém s počítačovou stanicí přímo ze své kanceláře připojením se k zájmovému počítači prostřednictvím počítačové sítě a následně na svém počítači tento počítač obsluhovat. Prakticky toto funguje tak, že vzdálený počítač obsluhujeme prostřednictvím hardwaru na vlastní stanici. Operační systém Microsoft Windows má za tímto účelem v moderních systémech implementovanou funkcionalitu „Připojení ke vzdálené ploše“. Připojení se pak uskutečňuje díky povolenému „Remote Desktop Protocol“, tedy protokolu umožňujícímu toto připojení. V nedávné době byla zranitelnost tohoto protokolu hojně využívána pachatelí k přístupu do pracovních stanic společností a jejich následnému zašifrování ransomwarem.

Další možností, jak vzdáleně spravovat počítač je specializovaný software, např. TeamViewer Remote¹¹⁵, AnyDesk¹¹⁶, SupRemo¹¹⁷ aj.

Problém spočívající ve vzdálené správě počítače je ten, že osoba, která provádí tuto vzdálenou správu počítače má typicky neomezený přístup ke spravovanému počítači, takže je schopna si zkopírovat uložená data, ale také je schopna spustit

https://www.nukib.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf. [cit. 2024-02-03].

¹¹⁴ Těmito jsou např. MD5, SHA1, SHA256, SHA512, SHA3_512 aj.

¹¹⁵ <https://www.teamviewer.com/en/>

¹¹⁶ <https://anydesk.com/en>

¹¹⁷ <https://www.supremocontrol.com>

jakýkoliv nainstalovaný program či tento sama nainstalovat. Nebezpečí tkví také v internetovém prohlížeči, kdy uživatelé (pro vlastní pohodlí) mají u jimi užívaných internetových stránek často uloženy přihlašovací údaje. Tohoto dnes pachatelé využívají v rámci již zmíněných phishingových kampaní, kdy po připojení se k počítači a internetovému bankovníctví převádí finanční prostředky na jimi ovládané bankovní účty, virtuální peněženky, zřizují nové bankovní účty prostřednictvím internetu, bankovní identity¹¹⁸, identity občana¹¹⁹ apod.

Uvedená vzdálená správa počítače však není podporována pouze na stolní počítače či notebooky, ale také na mobilní telefony a tablety. I u těchto je třeba si uvědomit, že se ve své podstatě jedná o počítače primárně určené ke komunikování s okolím.

1.2.17 Umělá inteligence

Internetová odnož encyklopedie Britannica k umělé inteligenci uvádí, že je to schopnost stroje vykonávat úkoly, o kterých se předpokládá, že k jejich splnění a řešení je třeba lidská inteligence. Ranným příkladem může být hraní šachů, překládání jazyků či řešení matematických vzorců. V současné době však tyto příklady jsou dalece překonány a považují se v oblasti umělé inteligence jako triviální, zejména ve srovnání s vizuálním rozpoznáváním vzorů, komplexním rozhodováním či používáním přirozeného jazyka. Umělá inteligence tak v současné době znamená, že se dokáže učit, dokáže uvažovat, řešit problémy, dokáže vnímat a používat jazyk.

Nyní tedy umělou inteligenci chápeme jako schopnost neuronových sítí přebírat další vrstvy a pracovat na složitějších problémech. Umělá inteligence se aktuálně dokáže učit strojově (autonomně prostřednictvím implementovaného softwaru), a to i bez dozoru (objevovat prvky v datech bez počátečních dotazů).

Díky strojovému učení a umělé inteligenci jsou dnes např. automobilové společnosti schopny vyvíjet autonomní vozidla. Stejně tak díky umělé inteligenci a její možnosti zpracování přirozeného jazyka jsou schopny počítače zpracovávat a analyzovat jazyk podobně jako lidé. Jedním z populárních jazykových modelů

¹¹⁸ Jednoduchý a bezpečný způsob pro přihlašování a ověřování totožnosti na internetu. Využijete ji nejen v bance, ale hlavně na úřadech nebo u soukromých firem.

¹¹⁹ Identita občana slouží pro bezpečné a jednoduché přihlašování do různých portálů státní a veřejné správy. Zahrnuje například Mobilní klíč eGovernmentu, NIA ID, bankovní identitu i jiné identifikační prostředky, kterými při přihlášení spolehlivě prokážete svoji totožnost.

umělé inteligence jsou GPT-3, GPT-3.5 a GPT-4, jenž jsou základem pro software ChatGPT¹²⁰. Pro lepší představu v Příloze č. 5 uvádím 2 příklady vytvořených textů prostřednictvím jazykového modelu GPT-3.5 Mezi jazykové modely umělé inteligence řadíme také chatboty zákaznických služeb na různých portálech, ale také software vyvinutý pro tvorbu obrázků jako jsou DALL-E¹²¹ a Midjourney¹²² či novinka Sora¹²³ umožňující vytváření videosekvencí (protože zadání těchto programů je písemné, nezáleží na formě výstupu). Umělá inteligence je spojena také s virtuálními asistenty jako jsou Alexa od Amazonu, Siri od Applu či Cortana od Microsoftu, ale u těchto je v současné době problém jazyk, ve kterém jsou schopny operovat, přičemž čeština mezi tyto jazyky nepatří a některé nejsou v České republice ani dostupné.¹²⁴

¹²⁰ <https://chat.openai.com/>

¹²¹ <https://openai.com/dall-e-3>

¹²² www.midjourney.com/

¹²³ <https://openai.com/sora>

¹²⁴ COPELAND, B.J. *artificial intelligence*. Online. In: Encyklopédia Britannica, 18. 11. 2023. Dostupné z: <https://www.britannica.com/technology/artificial-intelligence>. [cit. 2024-02-02].

2. Kybernetická trestná činnost a počítačová gramotnost policistů v Plzeňském kraji – současný stav znalostí a způsoby získávání informací

S ohledem na mé služební zařazení jakožto vyšetřovatele kybernetické kriminality na KŘPP je součástí mé práce také provádění kontrol spisových materiálů zpracovávaných územními odbory a Městským ředitelstvím Policie Plzeň – město¹²⁵ týkajících se kybernetické trestné činnosti. Stejně tak jsem jedním z 11 policistů, kteří jsou v rámci celé působnosti KŘPP veleni do dosažitelnosti jakožto kyber specialisté. Díky tomuto se domnívám, že mám ucelený pohled zejména na stávající stav znalostí policistů v oblasti kybernetické kriminality. Současný stav znalostí policistů KŘPP v oblasti kybernetické kriminality není zcela valný, jejich znalosti jsou velmi povrchní, vyplývající z dříve zjištěných skutečností. Bohužel většina z policistů nereflektuje změny, které během doby jejich služby nastaly a mnohdy ani bez dodatečných školení tyto změny nemají možnost zaregistrovat. Právě kvůli těmto problémům původně vznikla pracovní skupina KYBER v rámci KŘPP. Bohužel i po vzniku uvedené pracovní skupiny, ve které jsou a byli členy zástupci všech ÚO/MŘP v působnosti KŘPP, docházelo k nedostatečnému přenosu informací a zkušeností mezi policisty. S ohledem na tuto skutečnost jsem se rozhodl vypracovat tuto diplomovou práci, která by mi v práci s policisty napříč KŘPP měla pomoci v nastavení systému školení, avšak i v jiné rovině než jen v trestně právní, kdy tuto, jak jsem ostatně již výše zmínil, by policisté měli mít více než kvalitně zažito z předchozího profesního vzdělávání.

V souvislosti se zpracováním mé diplomové práce, jsem oslovil Útvar policejního vzdělávání a služební přípravy Policie ČR¹²⁶ za účelem zjištění informací o současném stavu vzdělávání policistů, a to jak nově nastoupivších, tak také déle sloužících. Na základě tohoto jsem zjistil, že v rámci intranetové sítě¹²⁷ Policie ČR je k dispozici databáze (ve formě intranetových stránek) obsahující oficiální

¹²⁵ Dále jen ÚO/MŘP

¹²⁶ Dále jen ÚPVSP

¹²⁷ Intranet je v informatice označení pro část počítačové sítě, která používá stejné technologie jako Internet (protokoly TCP/IP, přenosový protokol HTTP atp.). Na rozdíl od Internetu je však intranet privátní, což znamená, že jeho využívání je omezeno na skupinu uživatelů typicky pracovníky konkrétní společnosti či školy.

aktuální vzdělávací programy zastřešené tímto útvarem. Vzdělávací programy, ve kterých jsem zjistil jakoukoliv část týkající se mnou popisované kybernetické trestné činnosti, případně počítačové gramotnosti, jsou rozepsány níže, kdy se jedná o:

- Základní odborná příprava příslušníků Policie ČR – společné minimum bez specializace (univerzální ZOP) blended learning
- VZDĚLÁVACÍ PROGRAM Dítě v trestním řízení
- VZDĚLÁVACÍ PROGRAM Specializační kurz MS EXCEL – základní kurz
- VZDĚLÁVACÍ PROGRAM Specializační kurz MS EXCEL – pro pokročilé
- VZDĚLÁVACÍ PROGRAM SKPV – profesní specializace vyšetřování
- VZDĚLÁVACÍ PROGRAM SKPV – profesní specializace odhalování
- VZDĚLÁVACÍ PROGRAM kvalifikačního kurzu Hospodářská kriminalita
- VZDĚLÁVACÍ PROGRAM Kriminální zpravodajská analýza
- VZDĚLÁVACÍ PROGRAM Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat
- VZDĚLÁVACÍ PROGRAM Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat – prolongace

ÚPVSP však není jedinou cestou, jakým způsobem se mohou noví či delší dobu sloužící policisté v uvedených oblastech vzdělávat. Samostatnou kapitolou by bylo sebevzdělávání policistů, avšak s touto alternativou nebude a ani nemůže být v souvislosti s touto prací počítáno, zejména s ohledem na již zmíněnou neochotu policistů v této oblasti. Další možností je pořádání instrukčně metodických zaměstnání¹²⁸ ze strany KŘPP, ÚSKPV, NCOZ, NCTEKK a KÚP. ÚZČ pak sice IMZ pořádají, avšak na tyto většinou není zván široký okruh policistů, což je pochopitelné s ohledem na charakteristiku tohoto útvaru, proto se o tomto nebudu níže zmiňovat. KÚP pořádá primárně kurzy pro policejní specialisty zařazené na odborech kriminalistické techniky a expertíz¹²⁹. Pokud se podíváme blíže na IMZ pořádané ÚSKPV, NCOZ a NCTEKK v této oblasti, pak zjistíme, že tyto kurzy jsou pořádány celorepublikově, kdy na dané kurzy je možné typicky nominovat celkem 2-3 policisty za každé krajské ředitelství. Díky existenci odborů analytiky

¹²⁸ Dále jen IMZ.

¹²⁹ Dále jen OKTE.

a kybernetické kriminality¹³⁰ na každém z krajských ředitelství, jsou v drtivé většině na uvedené IMZ nominováni policisté právě těchto článků. Navíc ke znalostem v oblasti kybernetické trestné činnosti směrem k policistům zařazených do článků vnější služby je třeba si uvědomit, že ne každý takový policista je zpracovatelem spisových materiálů či policistou přijímajícím trestní oznámení, a proto o takové školení nemusí mít tolik policistů z této oblasti zájem.

Z historického hlediska lze konstatovat, že sama Policie ČR až od roku 2011 sleduje počet trestných činů spáchaných v kyberprostoru¹³¹, kdy do této doby sledován nebyl a nemůžeme tak předpokládat, že by kybernetická trestná činnost byla do této doby vůbec předmětem jakýchkoliv školení či ZOP.

S ohledem na uvedenou skutečnost a vlastní zkušenosti, mohu říci, že pokud bychom se bavili o policistovi zařazeném na jakémkoliv článku vnější služby, stejně jako o policistech zařazených na člancích SKPV, pro tyto bylo do roku 2019 velmi obtížné absolvovat jakékoliv specializační školení zabývající se čistě kybernetickou trestnou činností, které by bylo zajišťováno ze strany Policie ČR. Stejně tak mi není znám žádný IMZ, který by byl ze strany NCOZ, NCTEKK, ÚSKPV či KÚP primárně určen pro policisty zařazených pod vnější službou. Na tyto pořádané IMZ mohou být někteří policisté zváni, avšak dle mých zkušeností se primárně těchto IMZ účastní policisté zařazení u SKPV. Znám mi je pouze školení týkající se kybernetické trestné činnosti, které bylo přednášeno na Policejní akademii České republiky v Praze, kdy v době mého absolvování bylo 3denní posazené do teoretické roviny a dále byla možnost 1denního soustředění s praktickými ukázkami.

Další možností byly a jsou IMZ pořádané ze strany OAKK, případně odděleními analytiky a kybernetické kriminality jednotlivých ÚO/MŘP, kdy však tyto nejsou nijak centrálně určeny, stejně jako není stanoveno jejich zaměření. OAKK KŘPP od roku 2017 pořádala každoročně pravidelný IMZ zaměřený na oblast kybernetické trestné činnosti určený výhradně pro policisty z SKPV ÚO/MŘP. Program těchto pravidelných IMZ je různorodý, kdy za uvedenou dobu byly obsahem přednášky na témata:

¹³⁰ Dále jen OAKK

¹³¹ Policie České republiky. *Kyberkriminalita*. Online. In: Policie České republiky. Dostupné z: <https://www.policie.cz/clanek/kyberkriminalita.aspx>. [cit. 2024-02-20].

- Obligatorní každoroční témata byla:
 - diskuse nad problematickými otázkami z praxe,
 - rozbor zvláštností při vyšetřování;
- 2017
 - znalecké zkoumání PC, mobilních telefonů, obrazových souborů,
 - zajišťování výpočetní techniky,
 - využívání výpočetní techniky při páchání kybernetické kriminality,
 - nové trendy kybernetické kriminality na internetu,
 - vyžadování informací dle § 88a trestního řádu po linii ÚZČ,
- 2018
 - GDPR¹³² v souvislosti s šetřením kybernetické trestné činnosti,
 - Facebook
 - zjištění existence účtu,
 - zjištění ID profilu,
 - vyhledávání informací o zájmovém profilu,
 - pokročilé vyhledávání,
 - soukromí účtu, soukromí ve skupinách,
 - viry na Facebooku,
 - stažení archivu profilu – záložka bezpečnost,
 - zmrazení profilu cestou NCOZ,
 - vyžádání informací k profilu od Facebooku,
 - představení skriptů pro zajištění dat z profilů,
 - emergency případy,
 - novinky na Facebooku;
- 2019
 - představení oddělení kybernetické kriminality KŘPP,
 - spolupráce s Odborem informačních a komunikačních technologií¹³³, OKTE, Odborem analytiky KŘPP,
 - vyžadování „datafreezingu“ u zahraničních společností,
 - používání forenzních nástrojů pro analýzu,

¹³² Obecné nařízení o ochraně osobních údajů.

¹³³ Dále jen OIKT.

- vyžadování informací dle §7b, telekomunikace + datové zprávy po linii ÚZČ;
- bohužel v letech 2020–2021 pořádání IMZ nebylo možné z důvodu probíhající pandemie COVID-19;
- 2022
 - zajišťování výpočetní techniky,
 - využívání výpočetní techniky při páchání kybernetické kriminality,
 - nové trendy kybernetické kriminality na internetu,
 - možnosti vyžadování „datafreezingu“¹³⁴ u zahraničních společností,
 - možnost získání provozních a lokalizačních údajů v rámci zjištěných zemí a požadavky na jejich vyžádání
 - způsoby vyhodnocování logovacích souborů ze strany analytiků + vhodné nástroje,
 - vyžadování informací dle § 7b trestního řádu, § 88a trestního řádu po linii ÚZČ,
 - vyžadování informací dle § 158d odst. 3 trestního řádu, § 88 trestního řádu po linii ÚZČ.

V roce 2022 se výše uvedený pravidelný IMZ transformoval na IMZ pracovní skupiny KYBER, ve které jsou zastoupeni policisté a policistky všech oddělení SKPV napříč plzeňským krajem. Tímto způsobem jsme se pokusili předávat informace napříč KŘPP, kdy každý policista byl a je zodpovědný za předání informací získaných na základě pracovní skupiny oddělení, na kterém je služebně zařazen. V roce 2022 jsme tedy zorganizovali IMZ pracovní skupiny na téma úvod do problematiky kybernetické trestné činnosti, vyžadování datafreezingu u zahraničních společností, vyžadování informací dle § 7b trestního řádu, telekomunikace + datové zprávy po linii ÚZČ, vzhled do světa virtuálních měn. V roce 2023 pak proběhl návazný IMZ s tématy představení a praktická ukázka nových nástrojů vytvořených ÚZČ a zejména navazující přednáška na téma z roku 2022 vzhled do světa virtuálních měn – nové trendy, vyžadování informací od českých a zahraničních subjektů provozujících kryptosměnárny, právní a legislativní záležitosti problematiky virtuálních měn. Výhodou IMZ pro pracovní

¹³⁴ Zmražení dat u zahraničního poskytovatele.

skupinu, oproti předešlým IMZ z let 2017-2022, je stálost členů pracovní skupiny, takže jsme v současné době schopni vrstvit návazná a další témata a nemusíme se vracet k základním tématům, která by měli policisté a policistky z pracovní skupiny znát. V případě potřeby by také jednotliví členové měli být schopni provést školení základních útvarů či svých vlastních oddělení na již proškolená témata. Další výhodou pracovní skupiny je úzké zaměření jejích členů, kdy nezřídka kdy se tito účastní výukových školení ze strany CEPOL¹³⁵ a jsou i takto nabyté informace schopni předat dále.

Nad rámec výše uvedených IMZ jsme v roce 2018 pořádali speciální IMZ na téma Aspekty kybernetické trestné činnosti pro základní články v působnosti KŘPP. Tento IMZ byl individuálně zaměřen na činnost základních článků (články vnější služby), kdy obsahem byly:

- druhy kybernetické trestné činnosti, jejich podstata,
- současné trendy,
- postup policejních orgánů při přijímání trestního oznámení a následném prověřování,
- postupy při vyšetřování,
- důkazní prostředky,
- součinnost s jinými státními a nestátními organizacemi apod. se zaměřením na činnost základních článků.

Uvedený IMZ absolvovalo 110 policistů a policistek z jednotlivých obvodních oddělení policie¹³⁶.

Tento IMZ měl také své zrcadlo speciálně určené pro články SKPV KŘPP, kdy kopíroval výše uvedený program pro základní články, avšak byl doplněn o:

- problematiky případů internetových podvodů, podvodů prostřednictvím služeb PayPal, Blesk peněženky, ebay,
- obchodování s digitální peněžní měnou Bitcoin prostřednictvím open-source P2P platební sítě,
- problematika virtuální měny obecně,
- problematika sociálních sítí (Facebook, Twitter atd.),

¹³⁵ CEPOL je agentura Evropské unie, která podporuje spolupráci v oblasti prosazování práva prostřednictvím vzdělávání a výcviku, a to na evropské i mezinárodní úrovni.

¹³⁶ Dále jen OOP.

- zneužívání informací, dat a neoprávněné přístupy k počítačové síti,
- phishing.

Na tento IMZ byli, nad rámec policistů z SKPV KŘPP, pozváni také zástupci Krajského státního zastupitelství v Plzni.

Oba tyto IMZ byly následovány dalším, který v dané době byl vyhodnocen jako velmi přínosný, kdy se jednalo o téma sociální sítě Facebook, přednáška obsahující informace ke zjištění existence účtu, zjištění ID profilu, vyhledávání informací o zájmovém profilu, pokročilé vyhledávání, soukromí účtu, soukromí ve skupinách, viry na Facebooku, stažení archivu profilu - záložka bezpečnost, zmrazení profilu cestou NCOZ, vyžádání informací k profilu od Facebooku, představení skriptů pro zajištění dat z profilů, emergency případy, novinky na Facebooku. Tento IMZ byl určen pro široké spektrum policistů a navštívilo jej opět více jak 110 policistů a policistek zařazených na jednotlivých OOP a SKPV KŘPP. V roce 2022 jsme pořádali další IMZ pro široké publikum policistů, který byl zaměřen na problematiku virtuálních měn, vymezení virtuální měny, vysvětlení základních pojmů, uvedení příkladů těchto měn a jejich specifik, jakým způsobem lze získávat informace o jednotlivých transakcích a jejich trasování prostřednictvím volně dostupných možností. Opět se jej účastnilo opět na 100 policistů a policistek z různých OOP a SKPV KŘPP.

Školení týkající se počítačové gramotnosti, jsou mi i po provedení výzkumu pro tuto diplomovou práci, známy prakticky pouze týkající se používání tabulkového procesoru Microsoft Excel. K počítačové gramotnosti je třeba říci, že již před více jak 10 lety byly přinejmenším pro policisty SKPV dostupné specializační kurzy (obdoby VZDĚLÁVACÍ PROGRAM SKPV – profesní specializace vyšetřování a VZDĚLÁVACÍ PROGRAM SKPV – profesní specializace odhalování), ve kterých účastníci zpracovávali vybrané druhy protokolů na výpočetní technice, učili se používat program ASPI pro vyhledávání zákonů, jejich aktuálních i historických znění, stejně jako pro vyhledávání judikatury, dále se zde učili řádně zpracovávat spisový materiál v systému ETR. Proto se domnívám, že většina policistů ovládá základní znalosti počítačové gramotnosti. V následujících kapitolách se budu věnovat programům pořádaným ÚPVSP.

2.1. Způsoby získávání informací a zkušeností v oblasti kybernetické trestné činnosti a zvyšování počítačové gramotnosti v současné době – Policisté sloužící do 3 let

Základem odborné přípravy policisty je program Základní odborná příprava příslušníků Policie ČR – společné minimum bez specializace (univerzální ZOP) blended learning. „Absolvent tohoto kurzu by měl mj. v uvedené oblasti umět zpracovávat administrativní úkony a využívat informační zdroje potřebné ke služební činnosti, kterými jsou např. IS ETR, ASPI, e-SIAŘ, IS Bedrunka a také by se měl vyznat v základních pojmech a principech v oblasti kybernetické kriminality a získané dovednosti uplatnit v praxi. Práce v IS ETR a vyhledávání právních norem a interních aktů řízení v informačních zdrojích je zpracovávána také prakticky. V uvedeném programu je na administrativní a informační technologie vyčleněna časová dotace v počtu 14 hodin. Na kybernetickou kriminalitu jsou pak vyčleněny další 2 hodiny, během kterých by policista – dle dostupných materiálů – měl pochopit charakteristiku protiprávního jednání páchaného v digitálním prostředí a prostřednictvím digitálních technologií, přičemž obsahem těchto 2 hodin je základní charakteristika digitálních stop a jejich zajištění a základní pravidla bezpečného pohybu v síti internet.“¹³⁷

Dítě v trestním řízení je program pro všechny absolventy základní odborné přípravy, kteří provádí úkony v řízení v trestních věcech mladistvých a nezletilých. Policie ČR tímto svým programem vytváří specialisty zabývající se dětmi – jak jako pachatelé, tak také jako poškozenými. V jedné ze svých částí tento program popisuje trestnou činnost dětí a páchané na dětech na internetu a sociálních sítích. Časová dotace této přednáškové části je 2 hodiny, kdy ale do této dotace patří ještě vymezení využití analytické činnosti při rozkrývání trestné činnosti ve virtuálním prostředí.¹³⁸

Specializační kurzy MS EXCEL jsou určeny pro všechny. U základního kurzu je jedinou podmínkou zvládnutí práce s operačním systémem MS WINDOWS. Kurz

¹³⁷ Základní odborná příprava příslušníků Policie ČR – společné minimum bez specializace (univerzální ZOP) blended learning, Kódové označení: P1/0038, Č. j. UPVSP-3208-1/ČJ-2020-910010. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].

¹³⁸ VZDĚLÁVACÍ PROGRAM Dítě v trestním řízení, kódové označení P3/0073, č.j. UPVSP-3250-6/ČJ-2019-910010. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].

pro pokročilé je pak pro zájemce, kteří mají znalosti na úrovni MS EXCEL. Tyto kurzy nejsou určeny jen policistům, ale také občanským zaměstnancům. Základní kurz naučí účastníky „základní znalosti a dovednosti při používání tabulkového editoru MS EXCEL. Naučí se vytvářet tabulky dle vlastních potřeb, provádět jednoduché výpočty a vytvářet výsledné dokumenty a grafy.“¹³⁹ Délka výuky tohoto kurzu je 14 hodin. Návazný kurz pro pokročilé pak učí „znalosti a dovednosti spojené s tvorbou, formátováním a používáním tabulkového kalkulátoru, a to na vyšší uživatelské úrovni. Umí využívat a provádět standardní matematické a logické operace s použitím základních vzorců a funkcí a umí pracovat s daty většího objemu, vyhledávat v nich a vytvářet potřebné výstupy.“¹⁴⁰ Délka výuky je totožná jako základního kurzu.

2.2. Způsoby získávání informací a zkušeností v oblasti kybernetické trestné činnosti a zvyšování počítačové gramotnosti v současné době – Policisté sloužící více jak 3 roky

Pro tyto policisty je také určen program dítě v trestním řízení, stejně tak specializační kurzy na MS Excel. Dále se také budu věnovat programům určeným pro SKPV, kdy v běžném případě není předpoklad toho, že by policista sloužící méně jak 3 roky byl zařazen do některého z článků SKPV.

Vzdělávací program SKPV – profesní specializace vyšetřování ve svých osnovách platných od 01.11.2021 má zahrnutu, vyjma části týkající se dítěte v trestním řízení (zahrnující pravděpodobně – dle osnov – totožné informace jako výše popsaný program) samostatnou oblast týkající se kybernetické kriminality. Celková dotace této sekce je 16 hodin, kdy absolvent „dodržuje zásady zajišťování výpočetní techniky a digitálních dat, provádí základní postupy při zajišťování informací (důkazů) na internetu v případech emergency, přijímá oznámení týkající se podezření ze spáchání trestné činnosti na internetu v souladu s trestním řádem

¹³⁹ VZDĚLÁVACÍ PROGRAM Specializační kurz MS EXCEL – základní kurz, kódové označení P2/0159, č.j. VO-503/2006. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivita/. [cit. 2023-10-30].

¹⁴⁰ VZDĚLÁVACÍ PROGRAM Specializační kurz MS EXCEL – pro pokročilé, kódové označení P2/0157, č.j. VO-504/2006. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivita/. [cit. 2023-10-30].

a interními akty“¹⁴¹ a s ohledem na vytváření některých základních protokolů a dokumentů absolvent tohoto také zvyšuje svoji počítačovou gramotnost, kdy „pracuje s výpočetní technikou a programovými aplikacemi, které využívá při plnění úkolů, používá vybrané informační a datové zdroje Policie ČR“.¹⁴² Uvedené informace týkající se kybernetické trestné činnosti jsou pak získány pouze v teoretické rovině, ale bohužel uvedený program nemá prostor pro praktická cvičení, což při celkové dotaci 292 vyučovacích hodin ani není prakticky možné, jelikož by tento program musel zásadně zvýšit svoji časovou dotaci.

Téměř vše výše popsané vztahující se k programu SKPV – profesní specializace vyšetřování platí také pro vzdělávací program SKPV – profesní specializace odhalování. Rozdíl je v menším penzu přednášek, které jsou v tomto programu směrem ke kybernetické trestné činnosti přednášeny, avšak časová dotace je oproti vyšetřování navýšena z 16 na 20 hodin.¹⁴³ Bohužel i přes toto navýšení není obsahem žádné praktické cvičení či modelový příklad. Dále pak téměř absentuje vzdělání směrem k počítačové gramotnosti.

Kvalifikační kurz Hospodářská kriminalita je určen pro příslušníky Policie ČR ustanovené na odborech a odděleních hospodářské kriminality v rámci krajských ředitelství Policie ČR (či ÚO/MŘ), kteří mají znalosti a dovednosti na úrovni základní odborné přípravy. V rámci tohoto šestitýdenního kurzu je dána 4hodinová dotace na oblast kyberkriminality a 2 hodiny na autorská práva (velmi často jsou zařazována do ostatní kriminality páchané v kyberprostoru).¹⁴⁴

V rámci programu kriminální zpravodajská analýza, který je určen pro příslušníky Policie ČR ustanovené na pracovištích kriminálních analýz krajských a městských ředitelství policie a územních odborech nebo na systematizovaném služebním místě analytik NCOZ SKPV nebo NPC SKPV, jsou 4 hodiny přednášky o OSINT, WEBINT a dalších pojmu z oblasti vytěžování otevřených zdrojů (mj. digitálních

¹⁴¹ VZDĚLÁVACÍ PROGRAM SKPV – profesní specializace vyšetřování, kódové označení P2/0312, č.j. UPVSP-3953-2/ČJ-2021-910010. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].

¹⁴² VZDĚLÁVACÍ PROGRAM SKPV – profesní specializace vyšetřování, kódové označení P2/0312, č.j. UPVSP-3953-2/ČJ-2021-910010. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].

¹⁴³ VZDĚLÁVACÍ PROGRAM SKPV – profesní specializace odhalování, kódové označení P2/0311b, č.j. UPVSP-3953-3/ČJ-2021-910010. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].

¹⁴⁴ VZDĚLÁVACÍ PROGRAM kvalifikačního kurzu Hospodářská kriminalita, kódové označení, č.j. PA-1968-1/-2016-820060. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].

stop na internetu), další 4 hodiny jsou věnovány přednášce, ale i praktickému cvičení, na téma internetová bezpečnost (obsahující WEBINT svépomocí a významné typy otevřených zdrojů, sociální sítě a diskusní fóra). Následně je dalších 58 vyučovacích hodin věnováno řešení modelového případu, ve kterém účastníci využívají získané dovednosti i v rámci praktického cvičení.¹⁴⁵

Program Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat a jeho prolongace je vysoce specializovaným programem, kterého se mohou účastnit policisté zařazení „na KŘP odboru analytiky a kybernetické kriminality, oddělení kybernetické kriminality a skupině kybernetické kriminality, u útvarů NCOZ SKPV, NPC SKPV, ÚSČ SKPV a ve znaleckých pracovištích KÚ PČR a OKTE na služebních místech, jejichž náplň služební činnosti je i zajišťování výpočetní techniky a digitálních dat pro účely jejich následného znaleckého zkoumání.“¹⁴⁶ Tento program se, pravděpodobně jako jediný, zabývá technickou oblastí v souvislosti s kybernetickou trestnou činností, a právě z těchto důvodů je určen primárně pro výše uvedené policisty. „Absolvent vzdělávacího programu za využití dostupných technických prostředků a kriminalistických metod používá v souladu s platnou právní úpravou nejnovější postupy v zajišťování výpočetní techniky a digitálních dat, včetně zajišťování virtuální měny a její následný převod oprávněnému subjektu.“¹⁴⁷ Časová dotace výuku tohoto programu je 86 hodin, přičemž 14 hodin je věnováno operačnímu systému Linux, 66 hodin zajišťování výpočetní techniky a digitálních dat a 6 hodin pak kriminalistické technice. Tento program velmi často také využívá při výuce praktická cvičení. Prolongační kurz je určen policistům, kteří zvládli předchozí kurz a končí jim platnost vydaného osvědčení. Časová dotace výuku prolongačního kurzu je 12 hodin.¹⁴⁸

¹⁴⁵ VZDĚLÁVACÍ PROGRAM Kriminální zpravodajská analýza, kódové označení P2/0188, č.j. UPVSP-675-10/ČJ-2018-9100KR. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivita/. [cit. 2023-10-30].

¹⁴⁶ VZDĚLÁVACÍ PROGRAM Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat, kódové označení P2/0279, č.j. UPVSP-/ČJ-4124-2/ČJ-2022-910010. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivita/. [cit. 2023-10-30].

¹⁴⁷ VZDĚLÁVACÍ PROGRAM Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat, kódové označení P2/0279, č.j. UPVSP-/ČJ-4124-2/ČJ-2022-910010. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivita/. [cit. 2023-10-30].

¹⁴⁸ VZDĚLÁVACÍ PROGRAM Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat – prolongace, kódové označení P2/0298, č.j. UPVSP-/ČJ-4124-3/ČJ-2022-910010. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivita/. [cit. 2023-10-30].

3. Koncepce policejního vzdělávání v oblasti kybernetické trestné činnosti a počítačové gramotnosti

K samotné koncepci policejního vzdělávání v oblasti kybernetické trestné činnosti je třeba si uvědomit, že co se týče trestně-právní roviny, pak na základě provedeného šetření (nikoliv výzkumu uvedeném v kapitole 4.) v rámci této diplomové práce, se domnívám, že policisté by měli mít dostatečně velký přehled o jednotlivých trestných činech, jejich obligatorních a fakultativních znacích.

S ohledem na tuto skutečnost, s přihlédnutím k výsledkům dotazníkového šetření, jsem se rozhodl, že vytvořím koncepci založenou na základě vydefinování základních pojmů, provedení návazných a samostatných školení prováděných ze strany specializovaných útvarů Policie ČR či na základě vlastních sil KŘPP a vytvořením řízených modelových situací či předem připravených úkolů v oblasti počítačové gramotnosti. Prvotní ideou pisatele bylo rozdělení školení dle zaměření na kybernetickou trestnou činnost a samostatně na počítačovou gramotnost, která by se následně dělila podle toho, zda účastníky mají být policisté zařazení do článků vnější služby či policisté zařazení do článků SKPV. Při zpracování samotné koncepce uvedených školení ale vytanulo, že tato školení se částečně překrývají či doplňují, stejně tak jen menší část je určena jen pro policisty z článků SKPV a větší část je společná pro všechny případně školené policisty. Zmínit je třeba také skutečnost, že byť v současných vzdělávacích programech jsou policisté, dle dostupných informací, seznamování se základy kybernetické trestné činnosti, tak se domnívám, že jejich časová dotace je pro hlubší pochopení nedostatečná. Předpokládaná časová dotace níže nastíněných samotných školení je více jak 120 hodin. Stejně tak musíme mít na paměti, že velký podíl v současné době sloužících policistů neměli ve svých tehdejších vzdělávacích programech žádné informace týkající se kybernetické trestné činnosti, kdy zejména u těchto je předpoklad užitečnosti uvedených školení a řízených modelových situací.

3.1. Školení

Uvedená školení, až na výjimky, budou totožná pro všechny policisty, tedy jak pro policisty z vnější služby, tak také pro policisty zařazené na člancích SKPV. Většina uvedených školení je koncipována tak, aby je mohli školit policisté zařazení na OAKK KŘPP, kdy odchylky budou sděleny ve stručném popisu školení. Časová dotace každého tematického celku je pak plánována maximálně na 6 hodin tak, aby mohly být ukázány prezentované informace také v praktických příkladech. Počet školených osob je v maximálním rozmezí 130 osob, což je kapacita kinosálu KŘPP, avšak není vyloučeno rozčlenění na menší celky z důvodu lepší interakce s posluchači, zejména u školení prezentovaných policisty KŘPP. Samotná školení budou koncipována do jednotlivých tematických celků, které se částečně budou doplňovat či překrývat, kdy se jedná o tematické celky s názvy:

- Základy kybernetické trestné činnosti
- Prvotní nezbytné úkony v souvislosti s kybernetickou trestnou činností
- Zajišťování důkazů dle TŘ
- Analýza – možnosti analýzy ze strany OAKK
- Anonymizace pohybu na síti internet
- E-maily
- Informace o webu + IP
- Kryptoměny I.
- Kryptoměny II.
- Kryptoměny III. pro techniky
- Možnosti finančního šetření v ČR a úkony u bankovních institucí
- Možnosti softwaru Europol + Freetools
- OKTE – možnosti spolupráce na úseku kybernetické trestné činnosti
- OSINT pro technicky zdatnější policisty
- OSINT základy pro SKPV – odhalování a analytiku
- Platební metody a vyhledání majetku v zahraničí
- Práce s obrázky
- Sociální sítě
- Spoofing v praxi pro SKPV – odhalování a vyšetřování
- Vyhledávání na internetu

- Vytvoření falešné identity pro SKPV – odhalování
- Vyžadování údajů od mezinárodních společností
- Zajímavosti pro technicky zdatnější policisty

Základem pro všechny policisty by mělo být školení **Základy kybernetické trestné činnosti**, které bude rozděleno podle účastníků na vnější službu a SKPV. V tomto školení budou účastníkům sděleny základní pojmy vztahující se k této trestné činnosti, dojde k vymezení kyberprostoru, budou uvedeny definice nejen dle trestního práva, ale také dle občanského zákoníku, Úmluvě o počítačové kriminalitě a v případě vnější služby také dle Zákona č. 250/2016 Sb., o odpovědnosti za přestupky a řízení o nich a dle Zákona č. 251/2016 Sb., o některých přestupcích. Akcentována budou také smluvní ujednání mezi uživateli jednotlivých sociálních sítí a služeb a ukázán fingerprint zařízení¹⁴⁹ v praxi.

Druhé školení má název **První nezbytné úkony v souvislosti s kybernetickou trestnou činností**, jež je primárně zaměřeno pro policisty, kteří přijímají a sepisují trestní oznámení. Toto školení bude děleno na úkony, které je třeba neodkladně provést v případě, kdy byla činem způsobena škoda, zejména směrem ke zjištění cesty finančních toků a nejméně pokusu o zajištění příslušných finančních prostředků, a to jak v rámci institucí sídlících na území České republiky, tak také u institucí zahraničních. Další část je zaměřena na činy, kde došlo k jakékoliv komunikaci s pachatelem prostřednictvím sítě internet. Zde bude nejdůležitějším úkonem zajištění komunikace s pachatelem, zjištění identifikačních údajů všech stran a následné provedení zálohy dostupnými metodami.

V pořadí třetím školením, které by měli policisté absolvovat, bude školení **Zajišťování důkazů dle trestního řízení**. Byť jsem si vědom skutečnosti, že uvedené informace obsažené v tomto školení, by měli policisté nejméně z článků SKPV dobře znát, tak s ohledem na stále se vyvíjející judikaturu v oblastech zejména záznamu o telekomunikačním provozu a sledování osob a věcí, se domnívám, že zařazení tohoto školení je více než vhodné. V současné době se

¹⁴⁹ Jedná se o identifikační metodu a následné určení konkrétního zařízení pomocí specifických informací, jako jsou informace o operačním systému, internetových prohlížečích, IP adrese, rozlišení obrazovky, sériových čísel hardwaru a další. Prakticky fingerprint zařízení slouží k obdobným účelům jako cookies.

jedná např. o rozhodnutí o možnosti vydání příkazu ke zjištění informací o záznamu o telekomunikačním provozu i do budoucna, za splnění určitých podmínek.

Další školení lze absolvovat v jakémkoliv časovém sledu, vyjma návazných školení, kterými jsou oblast Kryptoměny I.-III. A OSINT základy pro SKPV – odhalování a analytiku a OSINT pro technicky zdatnější policisty. Tato školení mají vzájemnou návaznost, která bude uvedena níže.

Analýza – možnosti analýzy ze strany OAKK je název bloku, ve kterém budou představeny současné možnosti provádění komplexních či dílčích analýz ze strany OAKK či oddělení analytiky a kybernetické kriminality (vztahová, časová, četnostní, obsahová, časoprostorová, srovnávací, telekomunikačního provozu, analýza toků), možnosti vyhodnocení velkého objemu dat, vizualizace zjištěných informací a vyhledávání směrem k sériové trestné činnosti.

Anonymizace pohybu na síti internet představí možnosti anonymního a bezpečného procházení sítě internet prostřednictvím specializovaných internetových prohlížečů, VPN, proxy serverů¹⁵⁰ a virtuálních systémů, ukážeme si jejich výhody a nevýhody.

Přednáška **E-maily** bude zaměřená na zpracování e-mailových zpráv, kdy budou vysvětleny důležité položky zdrojového kódu (hlavičky), práce s programem Emailovník, ukázána možnost extrahování e-mailových adres z konkrétní internetové stránky, nastíněna možnost hashování zajištěných zpráv. Policistům bude ukázáno a v praxi vyzkoušeno uložení celé e-mailové zprávy ve formátu EML prostřednictvím webového rozhraní nejčastějších poskytovatelů, stejně tak bude představena a vyzkoušena možnost tohoto uložení z nejčastějších e-mailových klientů. Na závěr bude ukázáno nastavení e-mailového klienta pro stažení většího počtu e-mailových zpráv.

Informace o webu + IP je jedním z nejširších prezentovaných témat, kdy však samotné praktické šetření není časově tak náročné. Z tohoto důvodu by i v tomto případě neměla být výše uvedená časová dotace přesáhnutá. Nejprve se budeme věnovat informacím, které lze zjistit k doménám - jako je registrátor domény,

¹⁵⁰ Plní funkci komunikačního prostředníka mezi klientem a cílovým serverem. Proxy server překládá požadavky klienta vůči serveru, přebírá jeho odpověď, kterou zdárně doručuje zpět klientovi.

zjištění všech dostupných domén následných řádů, ukážeme si rozdíl mezi informacemi získanými o doménách s koncovkou .CZ, představíme nástroj na extrahování e-mailových adres z konkrétní internetové stránky, vysvětlíme fungování portálů na zjištění malwaru a škodlivého kódu na konkrétní internetové stránce, možnosti zjištění dřívějšího vzhledu internetových stránek a rozdíl ve vyžadování informací podle § 8 odst. 1 trestního řádu a podle § 88a trestního řádu, možnosti znepřístupnění webových stránek, kontaktování zahraničního poskytovatele, provedení zálohy internetové stránky a vytvoření protokolu o ohledání konkrétní stránky. Druhá část se bude zabývat možnostmi zjištění poskytovatele IP adresy (jak v Evropě, tak také mimo), v případě českého poskytovatele zjištění, zda je poskytovatelem dle zákona č. 127/2005 Sb., o elektronických komunikacích, uvedeme rámec informací zjistitelných na základě žádosti dle § 8 odst. 1 trestního řádu, na základě postupu dle § 88a trestního řádu a postup dle mezinárodní justiční spolupráci a Evropského vyšetřovacího příkazu. Školení **Kryptoměny I.** je prvním z celkem 3 samostatných školení, které však mají návaznost jedno na druhé, i když poslední školení, oproti předchozím, není určeno pro všechny policisty. Všechna tato školení budou prezentována specialisty z NCTEKK¹⁵¹, kteří s těmito mají velké zkušenosti. Jedná se o bývalé policisty NCOZ, se kterými máme dřívější velmi dobré zkušenosti. Kryptoměny I. má posluchačům objasnit, co to vlastně kryptoměna je, jakým způsobem se vyvíjela a jaká je její historie. Další část se věnuje nejznámější kryptoměně, kterou je Bitcoin následovaná blokem o AltCoinech¹⁵². Následovat budou základní informace o tom, jakým způsobem jsou využívány kryptoměny k trestné činnosti, jak vypadají kryptoměnové peněženky, jejich druhy, základ blockchainu a trasování prostřednictvím informací volně dostupných, od kterých volně přejdeme k možnostem anonymizování kryptoměn prostřednictvím tzv. mixérů až po obecné podmínky zajištění kryptoměn. Pro účastníky tohoto školení je pak připraveno návazné školení **Kryptoměny II.**, které přímo navazuje na první část, kterou rozšiřuje o znalosti vyžadování údajů od poskytovatelů služeb spojených s kryptoměnou, procesní metodiku zajišťování kryptoměn v trestním řízení, samotný praktický postup policejního orgánu při zajišťování kryptoměn v rámci

¹⁵¹ I přes skutečnost, že gestorem této oblasti je NCOZ

¹⁵² AltCoin = Alternativy Bitcoinu

trestního řízení včetně následného nakládání s kryptoměnou a o postup policejního orgánu s online směnárny kryptoměn. V rámci tohoto kurzu budou ukázány i praktické výstupy z jednotlivých zaslaných součinností směnárnám kryptoměn k ilustraci získaných údajů. Školení **Kryptoměny III. pro techniky** je návaznou specializovanou částí, které se budou účastnit pouze absolventi VZDĚLÁVACÍHO PROGRAMU Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat, kdy pouze tito policisté mají v rámci Policie ČR možnost převádět kryptoměnu ze zájmových peněženek do peněženek v dispozici státu. Tento exkurz je zařazen z důvodu ne zcela vysoké četnosti prováděných převodů ze strany uvedených policistů, přičemž tento kurz má napomoci oživení si dříve získaných dovedností v rámci uvedeného vzdělávacího programu. Pro tyto účely bude vytvořen zkušební uzavřený blockchain jen pro účely tohoto školení, na kterém bude docházet k simulovaným převodům nejpoužívanějších kryptoměn, ověření těchto převodů a bude kladen důraz na možná nebezpečí s převody související s ohledem na aktuální praxi.

Specialisté na finanční šetření z OHK KŘPP představí **Možnosti finančního šetření v ČR a úkony u bankovních institucí**, doplňující školení vysvětlující možnosti komplexního finančního šetření, jaké instituce jsou standardně dotazovány, jak vypadá výstup z provedeného finančního šetření, nastíní možnosti vyžadování spolupráce s Finančním analytickým úřadem v oblasti trestné činnosti a podá informace, které je možné získat u bankovních institucí a z centrální evidence účtů.

Možnosti softwaru Europol + Freetools představí možnosti využití softwaru vyvinutého pro orgány činné v trestním řízení napříč Evropskou unií, kdy budeme prezentovat v dané době vyzkoušené nástroje, jak pro OSINT analýzu, tak pro rozpoznávání osob na fotografiích dle vlastní databáze tváří, rozpoznávání osob na videích dle vložených fotografií, vyhledávání dětské pornografie v rámci zájmových dat, změnu čitelnosti registrační značky na základě matematických operací.

Ze strany specializovaného odboru KŘPP budou v rámci semináře **OKTE – možnosti spolupráce na úseku kybernetické trestné činnosti** předneseny možnosti znaleckého zkoumání a odborných vyjádření směrem k nejčastěji prověřované kybernetické trestné činnosti, přičemž se zaměříme na mobilní

zařízení a počítače (jak stolní, tak také notebooky). Dále budou představeny rozdíly v možnostech těchto zkoumání a vyjádření v případě nejčastějších operačních systémů pro mobilní telefony a počítače.

OSINT základy pro odhalování a analytiku má absolventům tohoto školení ukázat základní možnosti jeho využívání bez jakéhokoliv zastírání příslušnosti k Policii ČR a je tedy koncipováno jako určené pro jakéhokoliv policistu. K danému šetření budou předány informace o vyhledávání identit na síti internet, ukázáno komerční řešení Maltego, které by mělo být v blízké budoucnosti dostupné na každém krajském ředitelství policie. Dále budou představeny možnosti ověření existence e-mailové adresy, jakým způsobem vytvořit zájmovou identitu pro provedení šetření v otevřených zdrojích a ukázána pravidla vyhledávání v otevřených zdrojích – tedy samotné vyhodnocení zjištěných informací a jejich pravdivosti, a také dostupné OSINT databáze. Pro technicky zdatnější policisty, které předpokládám zejména u absolventů VZDĚLÁVACÍHO PROGRAMU Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat bude následovat kurz **OSINT pro technicky zdatnější policisty**, ve kterém budeme aplikovat anonymní procházení na internetu. K tomuto budeme potřebovat správně nastavit prostředí procházení internetu, kdy je možné využít několik metod, jako jsou virtualizované operační systémy k tomuto určené, využití VPN, proxy serverů, různých internetových prohlížečů a jejich doplňků, dále tyto seznámíme se způsoby ověření správného nastavení prostředí a vyhledávání.

Platební metody a vyhledání majetku v zahraničí je dalším ze školení s účastí specialistů, tentokrát z NCOZ zabývajících se dohledáváním majetku pocházejícího z trestné činnosti. V rámci této přednášky budou diskutovány možnosti zajištění finančních prostředků v zahraničí, možnosti spolupráce se subjekty jako jsou PayPal, Skrill, TransferGo, Revolut a možnosti dohledání majetku v zahraničí. Dále se budeme zabývat platebními kartami ve vztahu k jejich virtualizaci a tokenizaci, jako i ke zjištění plateb prostřednictvím Android Peněženky (Google Pay) a Apple Pay.

Dalším z plánovaných okruhů v rámci školení je **Práce s obrázky**. Policistům bude ilustrováno několik nástrojů dostupných na síti internet, které pomohou s doostřením fotografií, dále k vyhledání dalších obrázků vytvořených konkrétním fotoaparátem, přes vyhledání obličeje online a provedení online analýzy obrázku,

reverzního hledání obrázků až ke zjištění EXIF dat prostřednictvím prohlížeče XnView.

Kurz **Sociální sítě** ukáže účastníkům, jakým způsobem zjistit identifikační údaje k jejich uživatelům, ukáže možnosti zálohování zájmových příspěvků, zálohování kompletních profilů a případně stažení videí, a to u nejčastěji používaných sociálních sítí v České republice, se kterými se v rámci šetření kybernetické trestné činnosti setkáváme, jimiž jsou Facebook, Instagram, YouTube, WhatsApp. Ukážeme také, jakým způsobem vytvořit protokol o ohledání dané sociální sítě.

Spoofing v praxi pro SKPV – odhalování a vyšetřování vydefinuje, co to spoofing vlastně je, jakými způsoby jej můžeme provádět, jaká šetření k němu jsme schopni zajistit cestou ÚZČ, a to včetně praktické ukázky několika nástrojů k provedení spoofingu.

Vyhledávání na internetu je opět určeno pro široké publikum, kdy absolventům budou představeny nejrůznější možnosti vyhledávání dle zvolených parametrů k provedení přesnějšího a cílenějšího vyhledávání, stejně jako budou prezentovány rozdíly mezi mezinárodními vyhledávači jako je Google, DuckDuckGo, Yahoo, Yandex a případně další. Stejně tak bude ukázána možnost vyhledávání na základě obrázku prostřednictvím výše uvedených vyhledávačů.

Vytvoření falešné identity pro SKPV – odhalování je školení zaměřené výhradně pro operativní účely tak, aby policisté, kteří jej absolvují, byli schopni vystupovat na síti internet pod operativní legendou k monitorování trestné činnosti. Za tímto účelem budou účastníci naučeni k vytvoření nefunkčního čísla platební karty včetně všech dalších potřebných údajů, k vytvoření virtuálního telefonního čísla s možností číst SMS zprávy prostřednictvím sítě internet, automatizovaného vytvoření smyšlené identity včetně fotografie neexistující osoby a ověření existence zahraničních společností k prvotnímu šetření.

Následující školení bude provedeno s účastí specialistů z NCTEKK a ÚZČ.

Vyžadování údajů od mezinárodních společností představí možnosti získání informací od platebních bran, kryptosměnáren a sociálních sítí, včetně eventuality vyžádání informací v tzv. emergency případech, dále také možnosti provedení zmrazení dat v zahraničí a jejich následném vyžadování, včetně provedení úkonů cestou mezinárodní justiční spolupráce.

Zajímavosti pro technicky zdatnější policisty je, jak již název napovídá, určena pro policisty, kteří chtějí umět něco víc, než nabízí výše uvedená školení. V rámci tohoto se budeme bavit o možnostech zjištění IP adresy prostřednictvím obrázku, na který je třeba pouze „kliknout“, o možnosti virtualizace operačního systému Android na počítači, provedení zálohy webové stránky prostřednictvím softwaru, převod textu z různých jazyků bez využití internetu, převod formátů PDF do kopírovatelné podoby, jakož i o možnosti využívání umělé inteligence v rámci páchané trestné činnosti. V tomto školení bude také prostor pro rozebírání aktuálních technických trendů.

Jako Přílohu č. 7 přikládám pro lepší představu vytvořenou systematiku školení zachycenou v diagramu.

3.2. Řízené modelové situace

Při zkoumání různých metod a přístupů využitelných ke komplexnímu systému vzdělávání v oblasti kybernetické trestné činnosti jsem dospěl k závěru, v souladu s výsledky dotazníkového šetření uvedeného v kapitole 4.8. této diplomové práce, že vhodným doplněním teoreticky získaných informací jsou řízené modelové situace¹⁵³. ŘMS předpokládám o účasti maximálně 6 účastníků rozdělených do dvojic, kterým se bude věnovat 1–3 instruktoři, a to podle náročnosti dané ŘMS. Tito instruktoři budou mít k dispozici vytvořená výuková skripta, jenž budou mít základ ve skutečně zpracovaných spisových materiálech, skutečných žádostech a odpovědích jednotlivých subjektů, případně v příslušných zpracovaných formulářích. Daná skripta budou v níže uvedených oblastech, avšak předpokládám jejich obměnu v čase dle potřeb:

- neoprávněné opatření, padělání a pozměnění platebního prostředku,
- neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací,
- podvod prostřednictvím inzertních portálů (tzv. reverzní inzertní podvody),
- podvod prostřednictvím vishingu,
- sexuální nátlak prostřednictvím sítě internet,
- vydírání,

¹⁵³ Dále jen ŘMS

- výroba a jiné nakládání s dětskou pornografií.

Účelem zdejšího OAKK nebude provádění ŘMS se všemi policisty v působnosti KŘPP, avšak předání informací, jak uvedená ŘMS provádět, a to v rámci pracovní skupiny KYBER, kdy tito budou následně zodpovědní za vybrání vhodných policistů na jimi podléhajících článcích a jejich postupné proškolení.

Obsahem již zmíněných skript budou dokumenty, formuláře a datové soubory obsahující všechny potřebné informace k vedení trestního spisu od jeho počátku do fáze rozhodnutí ve věci, kdy samotné směřování „prověřování“ bude zcela na dané skupině účastníků. Zde je třeba upozornit na skutečnost, kdy k dispozici budou vzory vybraných formulářů tak, aby nedocházelo ke zbytečnému zdržení, avšak skupina bude mít k dispozici více formulářů, než v každé modelové situaci bude skutečně třeba. Toto bude z důvodu, aby policisté při každém kroku vyhodnotili, zda uvedený postup dle daného formuláře je třeba či nikoliv a z jakého důvodu. Instruktoři budou mít také k dispozici výukovou výpočetní techniku ve formě mobilních telefonů, flash disků, pevných disků, notebooků, tištěných dokumentů apod. Forma výukových doplňkových předmětů bude záviset na konkrétní ŘMS a instruktoři budou mít vždy totožné nástroje pro každou skupinu právě absolvující ŘMS. Tímto způsobem budou účastníkům vrstveny informace dosažitelné orgánům činných v trestním řízení a bude záležet pouze účastníků na jejich vyžádání, vyhodnocení a využití. Skripta budou vytvořena tak, aby účastníci byli schopni dostat se do fáze rozhodnutí ve věci, a to ať usneseními o odložení podle § 159a odst. 1 – odst. 5 trestního řádu, tak také usnesením o zahájení trestního stíhání podle § 160 odst. 1 trestního řádu. V každých skriptech bude na závěr uvedeno, jakého výsledku a z jakého důvodu by mělo být v rámci ŘMS dosaženo.

Rámcově lze uvést příklad jednoho z nejzávažnějších zločinů – sexuální nátlak na dítěti prostřednictvím sítě Instagram. Jako příklad přikládám Přílohu č. 8 - Systematika skript, ve které je graficky znázorněno, jakým způsobem budou skripta vytvářena v tomto trestném činu. Samotná skripta pak nejsou přílohou této práce, ale jsou zde představeny pouze jejich okruhy, jelikož uvedená skripta by si zasloužila samostatnou práci na dané téma.

Na počátku bude skupinám předán text trestního oznámení, který bude třeba vyhodnotit a rozhodnout, zda je možné a vhodné sepsat záznam o zahájení úkonů

trestního řízení (zjištění se bude ubírat k sedmi základním kriminalistickým otázkám). V případě, že tento záznam sepsat nebude možné, pak budou muset účastníci rozhodnout, zda lze zjistit další informace o dané činnosti a jakým způsobem. Pokud tyto zjistit nelze či v dané věci není spatřován trestný čin, pak bude třeba rozhodnout, jakým způsobem bude spisový materiál ukončen, kdy v Příloze č. 8 jsou jako možnosti v tomto kroku uvedeny sepsání založení věci ad acta případně postoupení přestupkového jednání příslušnému orgánu. V případě, kdy bude, i po získání dodatečných informací, ze strany účastníků vyhodnoceno, že mohlo dojít k naplnění skutkové podstaty jakéhokoliv trestného činu, pak budou muset dopsat příslušný připravený formulář, ve kterém určí právní kvalifikaci daného jednání, místo spáchání, osobu poškozeného a vymezí časové období spáchání skutku, to vše za předpokladu, že tyto informace budou znát.

Následovat bude vyhodnocení „spisového materiálu“, kdy prvotně účastníci po vzájemné dohodě, vypracují plán prověřování s vymezením, kdo jaké úkony bude činit. Zde bude dán důraz zejména na rychlost a efektivnost jednotlivých využití oprávnění, které trestní řád orgánům činným v trestním řízení skýtá s akcentem na neodkladné a neopakovatelné úkony a zajištění důkazních prostředků, které - např. vlivem postupu času – již nebudou následně k dispozici (jako např. údaje o telekomunikačním provozu, jímž bude končit zákonná lhůta uchování apod.). Stejně tak bude dán důraz na celkovou rychlost a efektivnost celého trestního řízení, jelikož u kybernetické trestné činnosti platí, že důkazní situace se může velmi rychle měnit, a to často díky vlivu osoby pachatele. V tomto konkrétním případě by mělo následovat získání informací od rodičů poškozené osoby, zajištění informací dostupných poškozené osobě na sociální síti internet a zjištění co nejvíce informací k pachateli. V podrobnostech bych odkázal na Přílohu č. 8, kdy jsou zde podrobně rozpracovány jednotlivé předpokládané úkony policejního orgánu, včetně možných reakcí, kdy podle tohoto konkrétního diagramu budou připravena právě skripta s plnými odpověďmi na případné dotazy účastníků, které budou upravovány instruktory na základě požadavku konkrétní skupiny. Předpokládám tedy, že ne každá skupina se zeptá totožným způsobem jako jiná, stejně tak předpokládám rozdílný rozsah zjišťovaných informací ze strany jednotlivých skupin. Po provedení dostatečných úkonů (dostatečnost bude posuzována vždy účastníky dané skupiny), bude úkolem rozhodnutí v dané věci.

Za tímto účelem bude vypracováno buď příslušné usnesení o odložení či zahájení trestního stíhání, případně bude rozhodnuto o odevzdání věci.

Úkolem instruktorů bude skutečná a velmi častá interakce s jimi přidělenou skupinou, kdy každé rozhodnutí skupiny bude detailně konzultováno právě s instruktory, kterým bude vysvětlováno, z jakého důvodu se skupina rozhodla pro dané řešení situace, proč zvolili ten konkrétní způsob zajištění stopy, zda je příslušný postup k získání stopy procesně správný a tedy následně použitelný v trestním řízení, jakým způsobem zvolit taktiku výslechu apod. Instruktor by, na základě vlastního posouzení, měl následně rozhodnout, zda bude do uvedeného řešení zasahovat a případně jakým způsobem. V ideálním případě by měl instruktor, v případě nesprávně vyhodnoceného či nedostatečně odůvodněného postupu, nasměrovat skupinu tak, aby vlastními úvahami nad dotazy instruktora, případně přehodnotili své rozhodnutí či jej doplnili, nebo aby na svém rozhodnutí trvali. V takových případech bude instruktor simulovat funkci porad se zkušenějšími kolegy či vedoucími policisty. Jsem si plně vědom skutečnosti obtížnosti výběru prvotních instruktorů, avšak trůfám si tvrdit, že uvedené prvotní ŘMS jsme schopni efektivně zvládnout vlastními silami na OAKK KŘPP.

3.3. Předem připravené úkoly v oblasti počítačové gramotnosti

K předem připraveným úkolům v oblasti počítačové gramotnosti budou využity výše uvedené ŘMS, kdy se domnívám, že toto bude zcela dostatečné. Z praxe lze říci, že většina policistů (trůfnu si tvrdit, že snad každý policista) zvládá základní úkony na počítači, stejně jako jeho základní obsluhu. Není mi znám žádný policista, který by neuměl pracovat s textovým procesorem Microsoft Word, IS ETŘ, nezvládal by základní ovládání operačního systému Microsoft Windows, nevyznal se ve vyhledávání interních aktů řízení prostřednictvím aplikace eSIÁŘ či nedokázal používat vyhledávání v jim dostupných evidencích.

Naproti tomu je však třeba říci, že v rámci ŘMS budou navozeny situace, kdy bude policista muset zjistit IP adresu počítače, se kterým zrovna pracuje. K této IP adrese bude muset zjistit poskytovatele internetového připojení, kterému by bylo možné adresovat žádost o součinnost. Získá informace o tom, jakým způsobem

lze, alespoň předběžně, zjistit, zda je internetová stránka, jež chce navštívit, bezpečná či obsahuje nějaký škodlivý či dokonce nebezpečný kód, kdo a kdy ji registroval, zda k této existují nějaké recenze či zda lze zjistit kontakt na administrátora stránky nebo jinou odpovědnou osobu. Dále budou mít za úkol nalézt starší obsah totožné internetové stránky.

Účastník ŘMS bude muset převést data získaná např. z logovacích souborů do tabulkového procesoru Microsoft Excel tak, aby následně byl schopen použít funkci filtrování, odebrání duplicit či seřadit jednotlivého sloupce. Další praktická cvičení budou zaměřena na zobrazení EXIF dat prostřednictvím prohlížeče grafických souborů XnView, který je dostupný na všech policejních počítačích (nejméně na území KŘPP) prostřednictvím Centra softwaru, jehož funkce bude také vysvětlena. V rámci uvedených EXIF dat a samotných fotografií budou policisté zkoušet vyhledat konkrétní místo, které se nachází na fotografii, případně kde byla uvedená fotografie vytvořena, jakým zařízením apod.

Samostatnou kapitolou bude vypracování úkolů souvisejících se sociálními sítěmi. Zde účastníci dostanou za úkol provést základní zálohu příspěvků dané sociální sítě, ohledání konkrétního profilu, stejně jako provádění zálohy uživatelských účtů (ať celých, tak jen vybraných částí) sociálních sítí jako jsou Facebook, Instagram či WhatsApp. Dále budou mít za úkol najít konkrétní identifikátory, podle kterých bude možné následně zaslat spolupráci příslušnému provozovateli dané sociální sítě. V rámci provedení uvedených záloh budou mít participant také za úkol vypočítat kontrolní sumy z daných souborů nejméně prostřednictvím 2 algoritmů. K e-mailové komunikaci budou předány znalosti uložení jednotlivých zpráv v datové podobě ve formátu .EML tak, aby mohlo dojít k jejich následnému vyhodnocení. Stejně tak budou muset absolventi těchto úkolů umět zobrazit zdrojový kód e-mailových zpráv, na základě kterého se pokusí odhalit podvržené e-mailové zprávy. V těchto případech budou využity e-mailové schránky portálů Google, Seznam.cz, Centrum a Volný, které budou také implementovány do nejčastěji užívaných e-mailových klientů, jako jsou Microsoft Outlook, Mozilla Thunderbird, Apple Mail.

Důležité informace budou předány také směrem k užívaným internetovým prohlížečům tak, aby účastníci byli schopni nalézt historii prohlížených stránek

případně ověřit informaci o uloženém heslu uživatele konkrétní internetové stránky.

V rámci některých RMS budou účastníci muset zjistit, jaký software je na daném počítači nainstalován, kdy byl nainstalován a případně zda je používán.

Výše uvedené informace budou účastníci zjišťovat jak na počítači či notebooku, tak také ale na mobilních telefonech či tabletech tak, aby byla zvýšena jejich gramotnost i v této oblasti.

Z uvedeného tak vyplývá, že výše představená koncepce vzdělávání bude ucelená a zaměřená na získání co největšího množství informací.

4. Výzkum

Jako vhodný přístup k výzkumu v této práci jsem zvolil exploratorní výzkum s ohledem na jeho charakteristiku, který hledá a popisuje systém a jeho závislosti.¹⁵⁴ Výzkum byl proveden prostřednictvím dotazníkového šetření, který byl v části otázek koncipován s uzavřenými odpověďmi, avšak ve vhodných částech také s odpověďmi polouzavřenými. Cílem uvedených otázek bylo zjistit, zda a v jakém rozsahu obdrželi respondenti znalosti týkající se kybernetické trestné činnosti a počítačové gramotnosti v rámci ZOP, zda měli a využili další jim dostupné nabídky na vzdělávání v těchto oblastech a ke vhodné formě školení v daných oblastech. K naplnění účelu této diplomové práce byly vydefinováno níže uvedené výzkumné otázky:

1. Jak hodnotíte znalosti předávané v rámci základních odborných příprav (dále jen ZOP) týkající se kybernetické trestné činnosti?
2. Jak hodnotíte znalosti předávané v rámci ZOP týkající se počítačové gramotnosti (schopnost používat účelově a účinně počítač a jinou výpočetní techniku)?
3. Kolik školení po ZOP týkajících se kybernetické trestné činnosti či počítačové gramotnosti jste díky PČR absolvovali?
4. Jak hodnotíte znalosti předávané v rámci školení týkajících se kybernetické trestné činnosti?
5. Jaké zaměření uvedená školení týkající se kybernetické trestné činnosti měla?
6. Jak hodnotíte znalosti předávané v rámci specializačních kurzů týkajících se počítačové gramotnosti?
7. Měli jste možnost se v rámci služebního poměru účastnit jakéhokoliv školení týkající se kybernetické trestné činnosti či počítačové gramotnosti?
8. Jakou formu vzdělávání v uvedené oblasti preferujete?
9. Vyhovovalo by Vám školení formou řízených modelových situací v oblasti kybernetické trestné činnosti?

¹⁵⁴ MOLNÁR, Zdeněk, MILDEROVÁ, Stanislava, ŘEZANKOVÁ, Hana, BRIXÍ, Radim a KALINA Jaroslav. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting, 2012. Věda pro praxi (Profess Consulting). ISBN 978-80-7259-064-3, str. 30

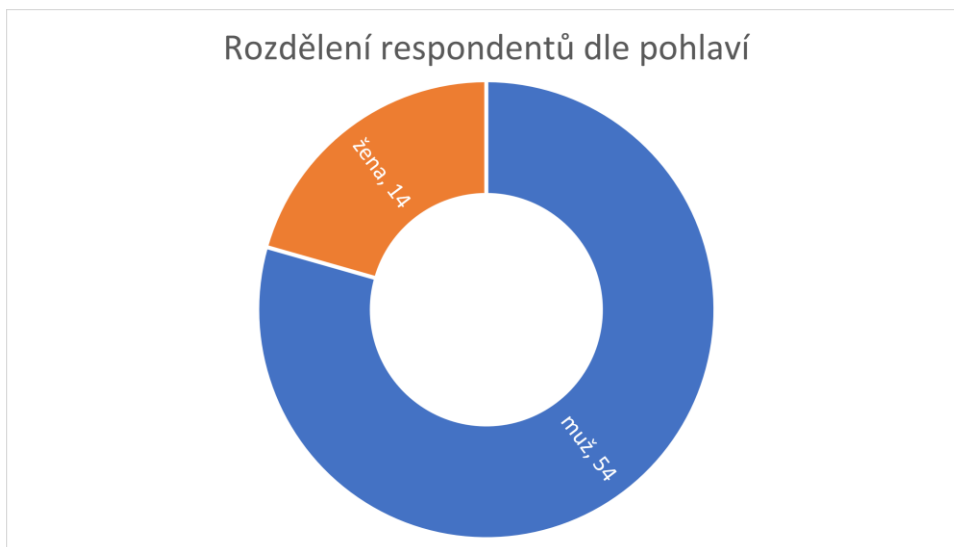
10. Vyhovovalo by Vám školení formou řešení předem připravených úkolů v oblasti počítačové gramotnosti?

Na počátku výzkumné části je nejprve definován vzorek účastníků, na kterých proběhl výzkum, následované jednotlivými podkapitolami formulujícími hypotézy na výše uvedené výzkumné otázky za použití logické metody indukce zkomponované s daty od účastníků.

4.1. Výzkumný vzorek respondentů

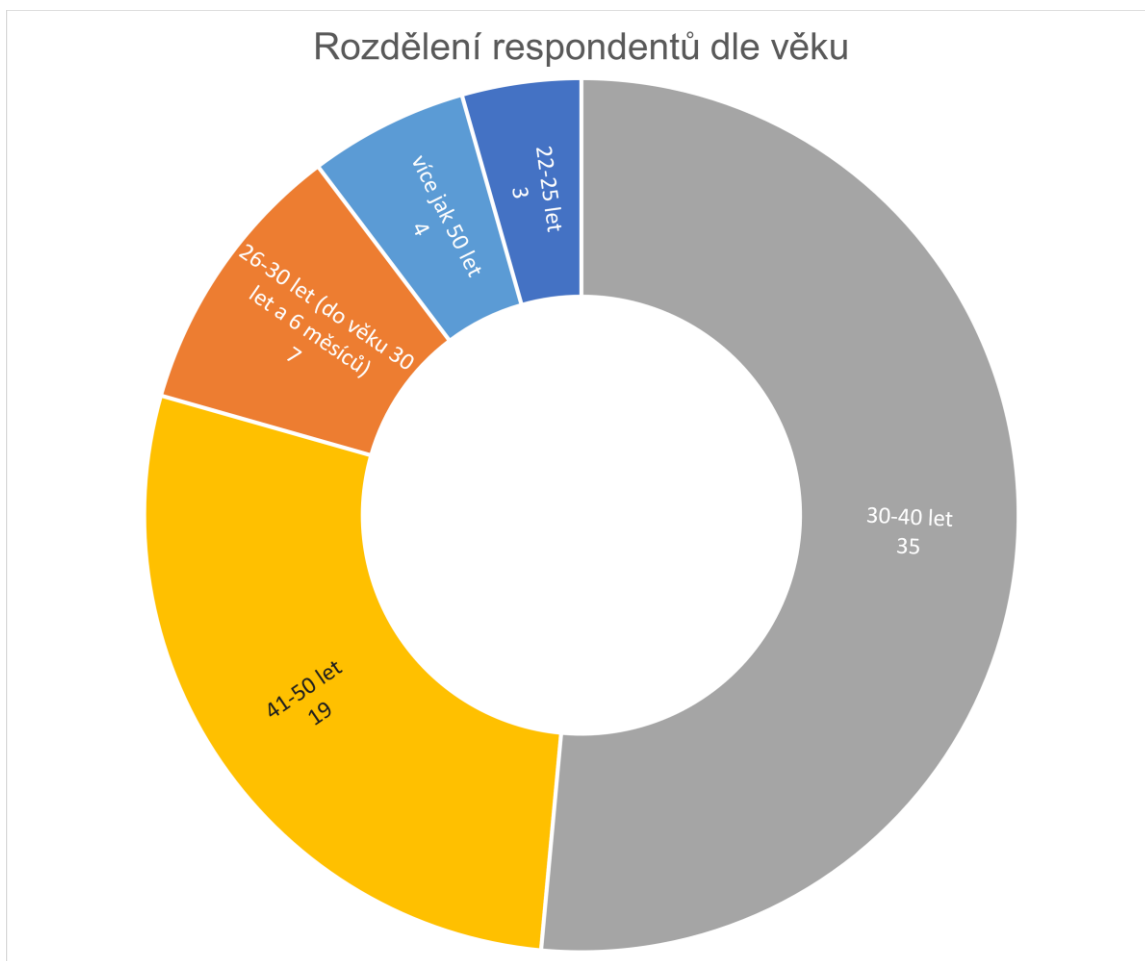
K tomu, abych mohl v co největší míře objektivně posoudit současný stav předávaných znalostí policistů v Plzeňském kraji v oblasti kybernetické trestné činnosti a jejich počítačové gramotnosti, jsem vytvořil dotazník, který jsem se snažil distribuovat pouze mezi policisty aktuálně zařazené na jakémkoliv článku podléhajícím KŘPP, či přímo na tomto článku. Uvedený dotazník jsem rozeslal dne 30. 11. 2023, kdy tento sbíral odpovědi do 11. 02. 2024. Umístěn byl na online platformě Dokumenty Google. Za uvedenou dobu tento dotazník vyplnilo celkem 68 respondentů. Dotazník obsahuje nejprve 6 otázek týkajících se respondenta a následuje 10 výzkumných otázek. Aby bylo dosaženo co nejnižšího času stráveného respondentem nad uvedeným dotazníkem, byly koncipovány odpovědi tak, aby zahrnovaly, pokud možno, nejširší možnosti odpovědi, kdy v části otázek bylo možné respondentem vyplnit vlastní odpověď. Definování jednotlivých odpovědí na dotazníkové otázky bylo uzpůsobeno záměru této práce, kdy však zejména věkové rozhraní bylo u věku 30 let voleno s ohledem na dobu, kdy začalo docházet ke tvoření specialistů na kybernetickou (v dané době informatickou) trestnou činnost.

Graf č.1 – Rozdělení respondentů dle pohlaví



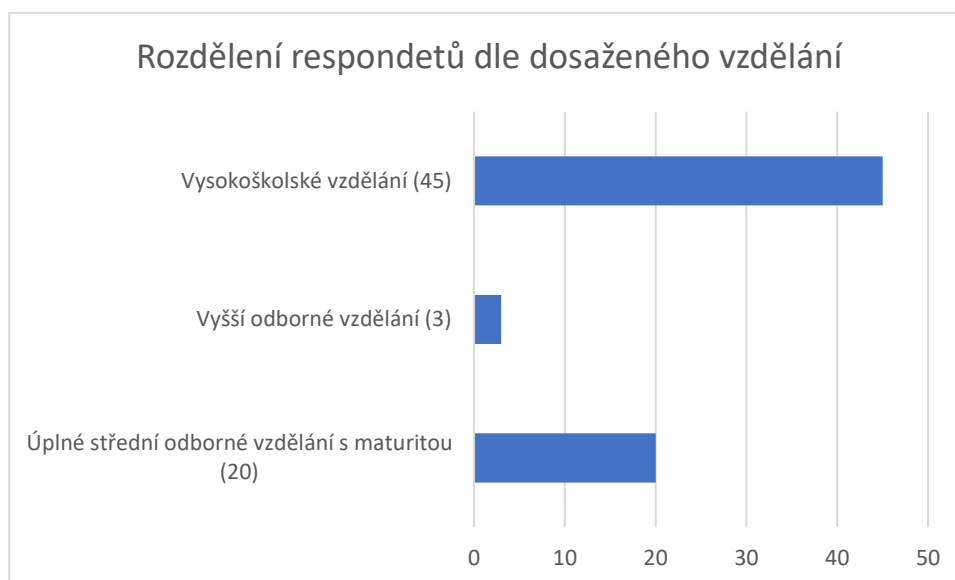
Z celkového počtu 68 účastníků bylo 54 osob mužského pohlaví (79,4 %) a 14 pohlaví ženského (20,6 %). I přes možnost respondentem vyplnění jiného než uvedené pohlaví, žádný z respondentů této možnosti nevyužil.

Graf č. 2 – Rozdělení respondentů dle věku



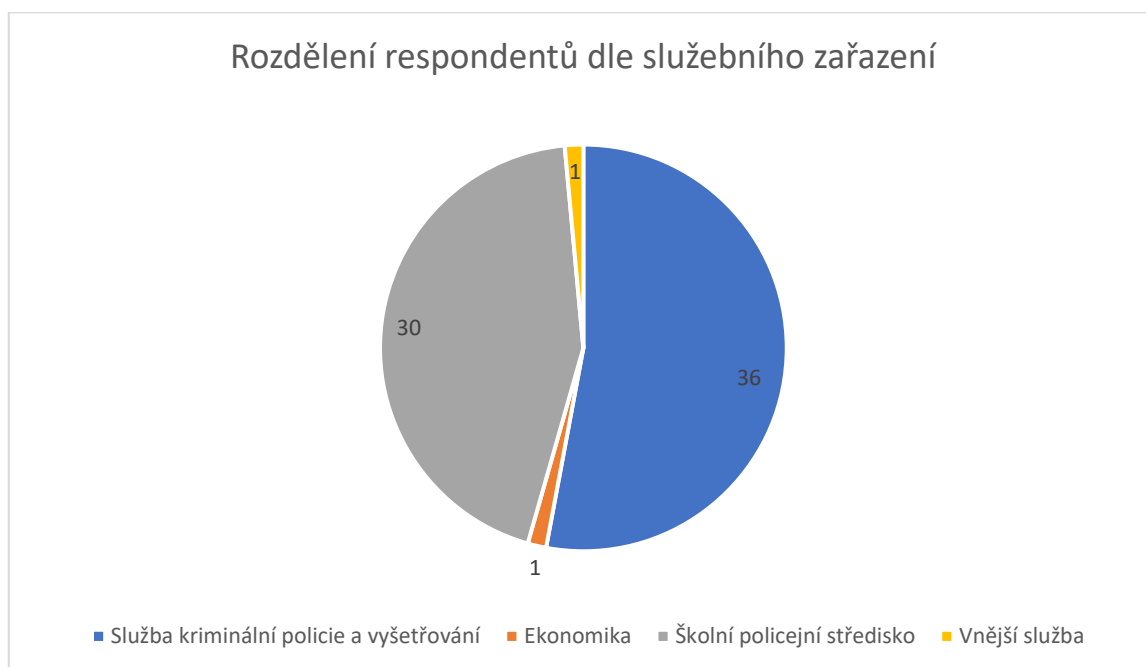
Co se týče věkové struktury, pak byly zastoupeny všechny věkové skupiny vyjma nejmladších možných příslušníků, kdy ve věku 18-21 let nebyl žádný respondent. Ve věku 22-25 let bylo 4,4 % respondentů, ve věku 26-30 let (do věku 30 let a 6 měsíců) bylo celkem 10,3 % respondentů, ve věku 30-40 let 51,5 % respondentů, ve věku 41-50 let 27,9 % a ve věku více jak 50 let 5,9 % respondentů.

Graf č. 3 – Rozdělení respondentů dle dosaženého vzdělání



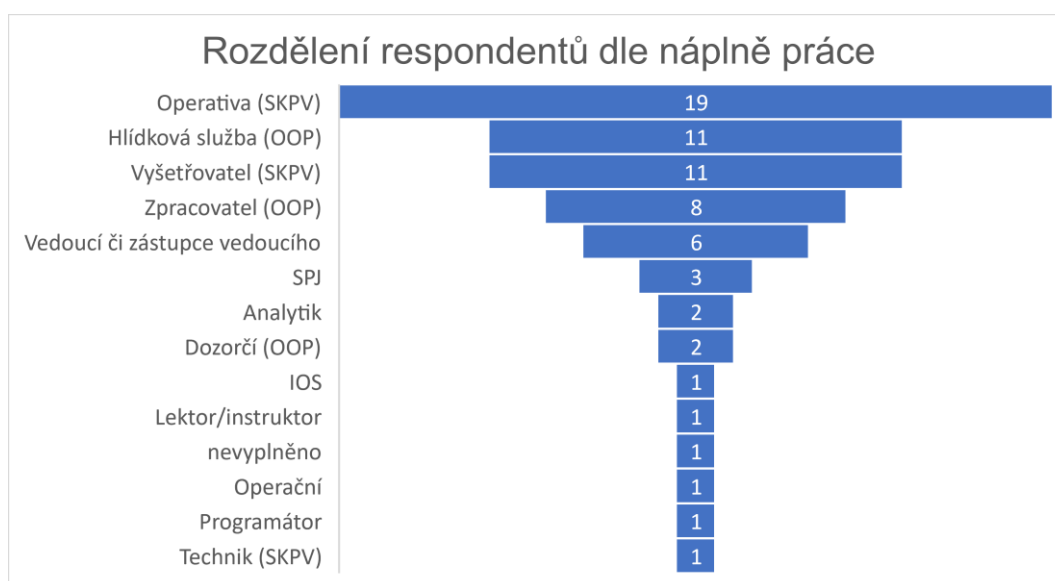
Nejvíce odpovídajících - 66,2 % - uvedlo, že dosáhli vysokoškolského vzdělání, 29,4 % pak úplného středního odborného vzdělání s maturitou a 4,4 % dosáhlo vyššího odborného vzdělání. I přes skutečnost, že jednou z podmínek přijetí k Policii ČR je v současné době pouze střední vzdělání a vyšší, byla v dotazníku možnost vybrání i základního vzdělání. Základní vzdělání, stejně jako střední odborné vzdělání s výučním listem, nevybral žádný z odpovídajících.

Graf č. 4 – Rozdělení respondentů dle služebního zařazení



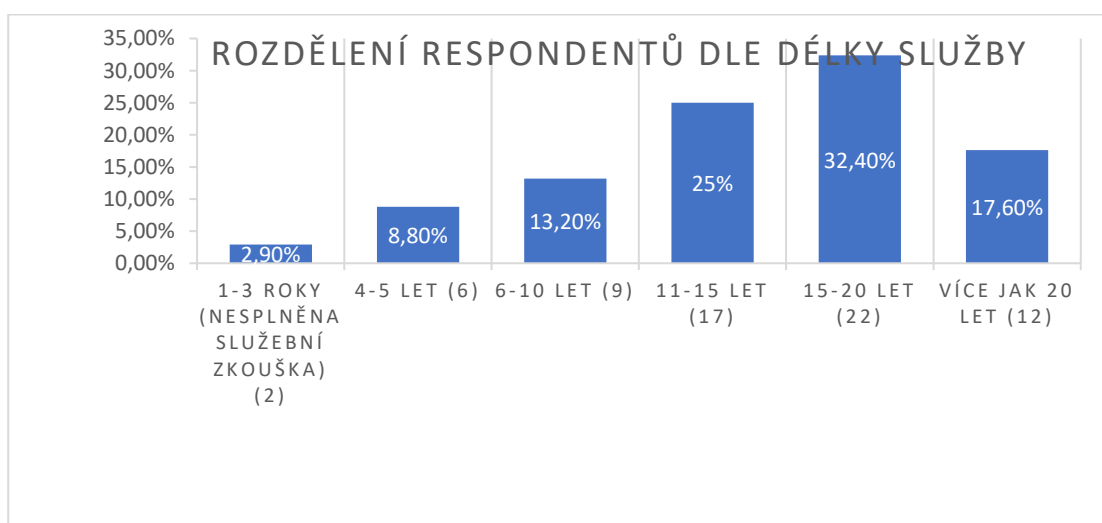
52,9 % účastníků uvedlo, že slouží na článku, který řadíme pod službu kriminální policii a vyšetřování, 1,5 % (1 účastník) uvedl, že slouží na OIKT (patří do ekonomické sekce), 1,5 % (1 účastník) slouží ve Školním policejním středisku vedeným přímo ředitelem krajského ředitelství. Zbýlých 44,2 % pak slouží na některém z článků vnější služby. S ohledem na rozsáhlé možnosti služebního zařazení policistů, byla možnost využít možnost jiné s vypsáním vlastní odpovědi, kdy tuto využili celkem 4 respondenti.

Graf č. 5 – Rozdělení respondentů dle náplně práce



Dle náplně práce je rozdělení policistů také velmi různorodé. Nejvíce respondentů pracuje na úseku odhalování trestné činnosti¹⁵⁵ – 19, následují policisté z hlídkové služby a vyšetřovatelé trestné činnosti – shodně 11, zpracovatelů na obvodních obvodech je součástí šetření 8, velkým překvapením pro mne bylo zapojení 6 vedoucích či zástupců vedoucího, 3 respondenti jsou zařazeni do speciální pořádkové jednotky, 2 z respondentů jsou analytici a 2 jsou dozorčí na obvodním oddělení. Vždy po jednom policistovi jsou pak z integrovaného operačního střediska, z operačního odboru, programátor, technik, jeden uvedl jako náplň práce lektor/instruktor a jeden svoji náplň práce nevyplnil.

Graf č. 6 – Rozdělení respondentů dle délky služby



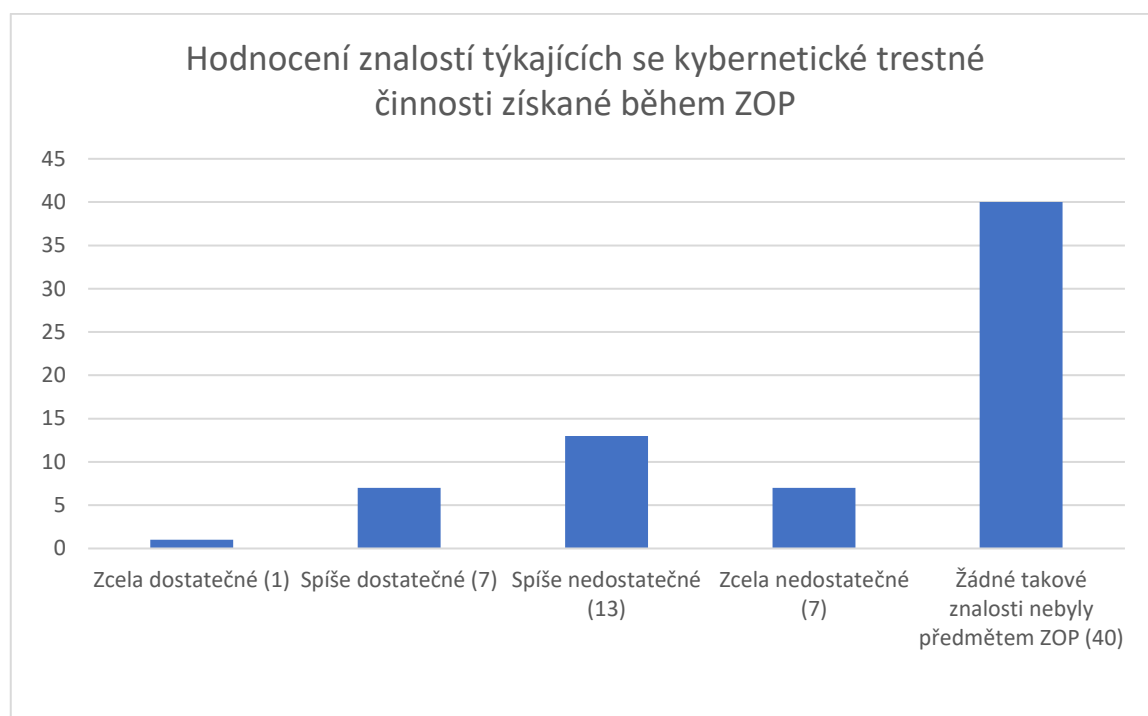
¹⁵⁵ V policejním slangu se označují slovem „operativa“.

Na základě údajů o doby služby vyplývá, že v uvedených zjištěních budou zastoupena všechna časová období, během kterých kybernetická kriminalita, jak vznikla, tak byla na vzestupu či byla stanovena jako priorita ze strany Policejního prezidia ČR. Nejvíce respondentů je s dobou služby mezi 15-22 let, následování účastníky sloužícími mezi 11-15 lety. Na pomyslných dalších příčkách jsou pak služební poměry s délkou služby více jak 20 let, mezi 6-10 lety, dále 4-5 let a také 2 osoby sloužící méně jak 3 roky.

4.2. Odpovědi respondentů k výzkumné otázce č. 1

Znění výzkumné otázky: Jak hodnotíte znalosti předávané v rámci základních odborných příprav (dále jen ZOP) týkající se kybernetické trestné činnosti?

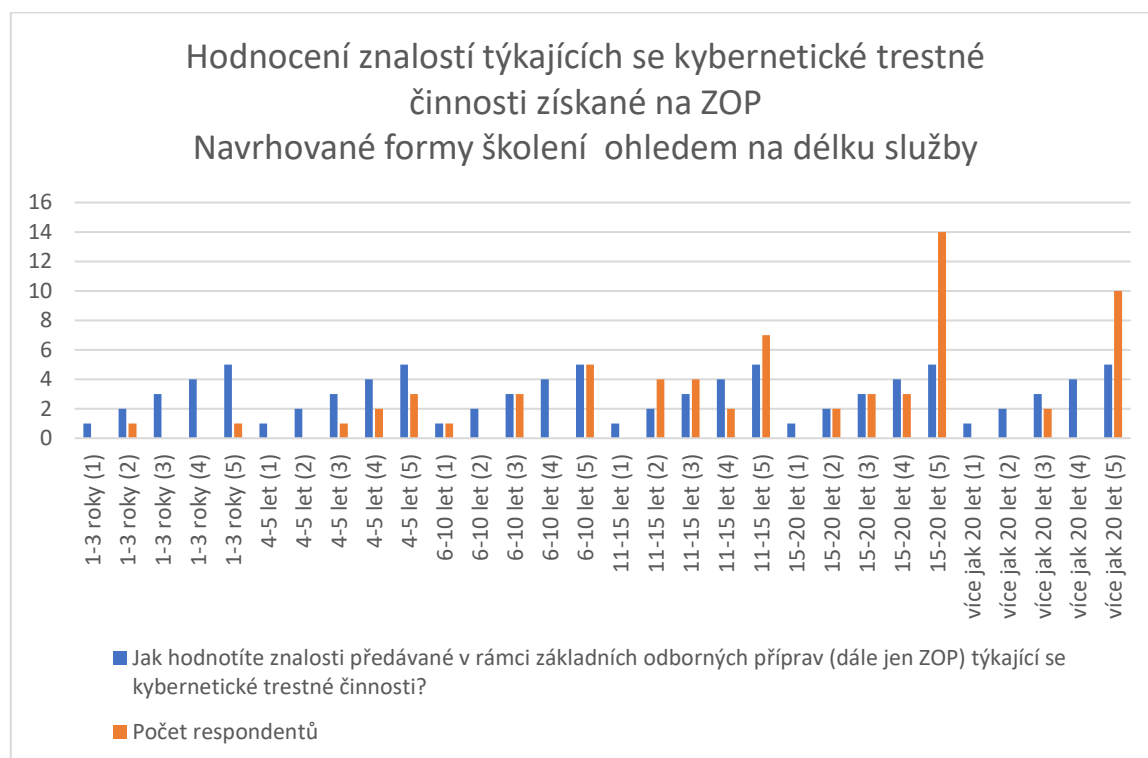
Graf č. 7 – Hodnocení znalostí týkajících se kybernetické trestné činnosti získané během ZOP



Z dotazníkového šetření jednoznačně vyplývá, že 58,8 % (40) respondentů uvádí, že v rámci základních odborných příprav nebyly žádné znalosti týkající se kybernetické trestné činnosti předmětem ZOP, jako zcela nedostatečné tyto znalosti uvádí 10,3 % (7), spíše nedostatečné 19,1 % (13), 10,3 % zúčastněných (7 policistek a policistů – 4 sloužící u Policie ČR mezi 11-15 lety, 2 mezi 15-20 lety a 1 sloužící mezi 1-3 lety) uvedlo, že znalosti byly spíše dostatečné a pouhé 1,5

% (1 účastník sloužící u Policie ČR mezi 6-10 lety) uvedl znalosti jako zcela dostatečné. Během vytváření této výzkumné otázky jsem předpokládal, že u policistů sloužících déle než 10 let bude většina odpovědí na tuto otázku znít – znalosti týkající se kybernetické trestné činnosti nebyly v rámci ZOP předány žádné, případně zcela nedostatečné. Bohužel při vyhodnocování této odpovědi se ukázalo, že policisté většinově napříč celým spektrem uvádí, že žádné takové znalosti nebyly

Graf č. 8 – Hodnocení znalostí týkajících se kybernetické trestné získané během ZOP s ohledem na délku služby



Výše uvedený graf znázorňuje hodnocení respondentů s ohledem na jejich délku služby, kdy pro účely vypracování tohoto grafu bylo potřeba převést údaje týkající se hodnocení do bodové podoby, tak aby uvedený graf byl čitelný. Převodní tabulku uvádím:

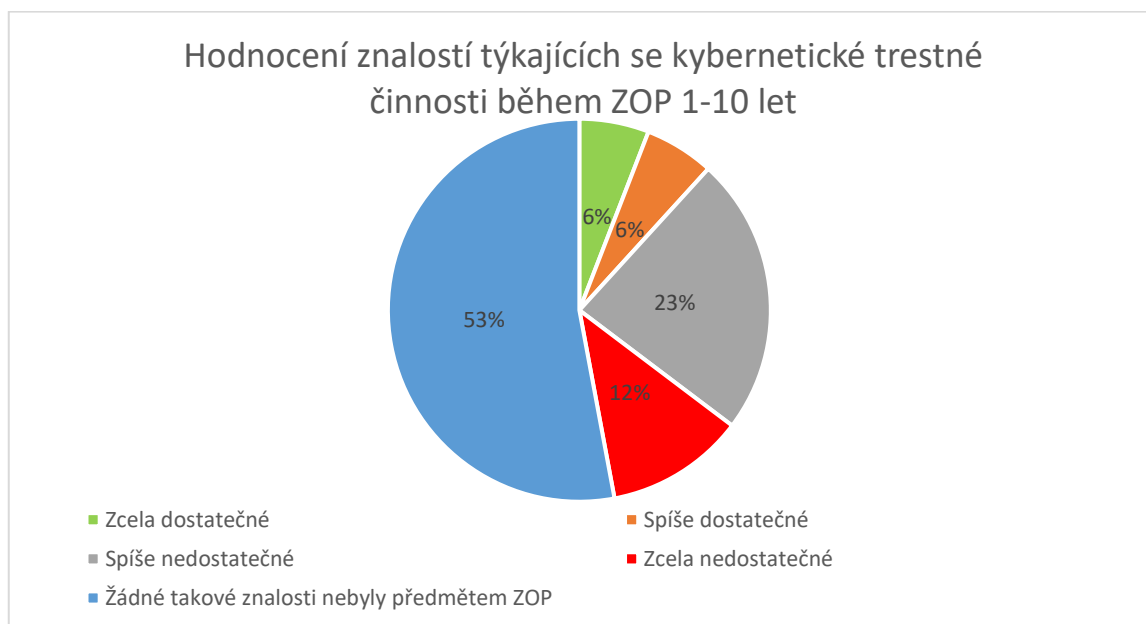
Původní hodnocení	Číselné vyjádření
Zcela dostatečné	1
Spíše dostatečné	2
Spíše nedostatečné	3
Zcela nedostatečné	4
Žádné takové znalosti nebyly předmětem ZOP	5

Zajímavostí tohoto srovnání je odpověď dvou účastníků šetření sloužících méně jak 3 roky, jeden účastník uvedl, že žádné znalosti týkající se kybernetické trestné činnosti součástí ZOP nebyly, kdežto druhý účastník uvedl, že tyto znalosti hodnotí spíše dostatečně. Oba tito respondenti byly v době vyplňování dotazníku shodně služebně zařazeni na Obvodním oddělení Policie.

Z uvedených 58,8 % respondentů, kteří uvedli, že nebyly v ZOP předávány žádné znalosti v oblasti kybernetické trestné činnosti je 10 sloužících více jak 20 let (z celkového počtu 12 takto dlouze sloužících policistů), dále 14 sloužících mezi 15-20 lety (z celkových 22). U těchto respondentů je však tento stav pochopitelný, jelikož musíme brát v potaz, že se jedná o osoby absolvující ZOP v letech 2009 a méně, kdy pojem kybernetická trestná činnost nebyla u Policie ČR téměř vůbec známa. Pokud se podíváme na data u respondentů patřících do kategorie v délce služby 4-5 let, pak vidíme, že 3 z těchto uvedli, že žádné znalosti o kybernetické trestné činnosti nebyly předmětem ZOP. Další 2 uvedli, že znalosti předané byly zcela nedostatečné a jeden z účastníků tyto uvedl jako spíše dostatečné.

Velmi protichůdné informace jsou také u skupiny účastníků sloužících mezi 6-10 lety, kdy 5 uvedlo, že žádné znalosti týkající se kybernetické trestné činnosti předány nebyly, 3 uvedli, že byly předány spíše nedostatečně a 1 uvedl znalosti za zcela dostatečné. U účastníků sloužících mezi 11-15 lety je situace taková, že celkem 7 z nich uvádí, že žádné takové znalosti předány nebyly, 4 tyto informace považuje za spíše dostačující, další 4 za spíše nedostačující a 2 za zcela nedostatečné.

Graf č. 8 - Hodnocení znalostí týkajících se kybernetické trestné činnosti získané během ZOP s dobou služby 1-10 let



Výše uvedená tabulka ilustruje odpovědi s vynecháním respondentů sloužících více jak 10 let, kdy ke stanovení hypotézy se kloním spíše k touto údaj, a to s ohledem na skutečnost, kdy Policie ČR začala sledovat počet trestných činů spáchaných v kyberprostoru od roku 2011

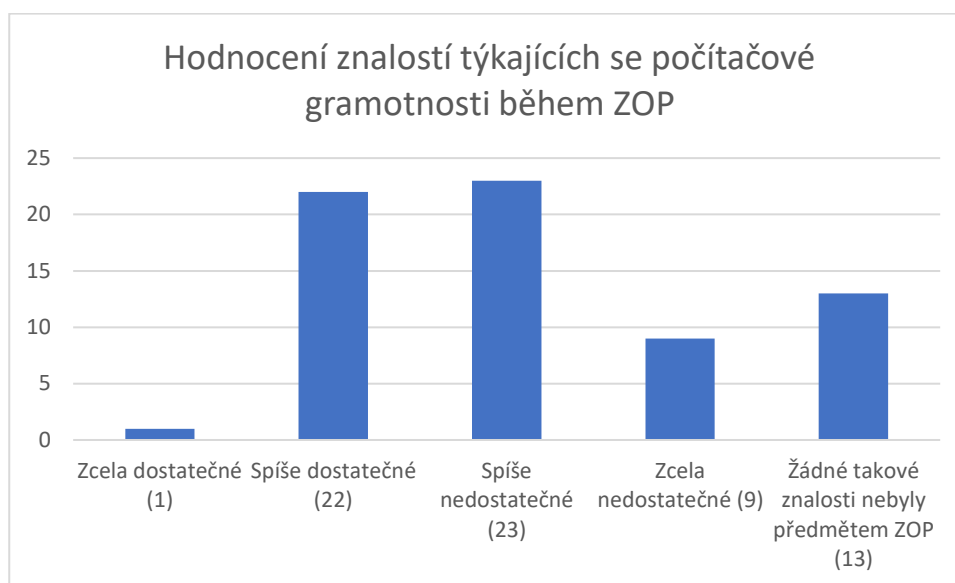
Hypotéza k výzkumné otázce č. 1 konstruovaná na základě odpovědi respondentů:

Nadpoloviční většina policistů absolvujících ZOP od roku 2013 dále (53 %) uvádí, že v rámci ZOP nebyly předávány žádné znalosti týkající se kybernetické trestné činnosti, 23 % respondentů uvádí takové znalosti jako spíše nedostatečné, dalších 12 % uvádí, že tyto znalosti jsou zcela nedostatečné a shodně 6 % uvádí, že předané znalosti jsou zcela dostatečné či spíše dostatečné.

4.3. Odpovědi respondentů k výzkumné otázce č. 2

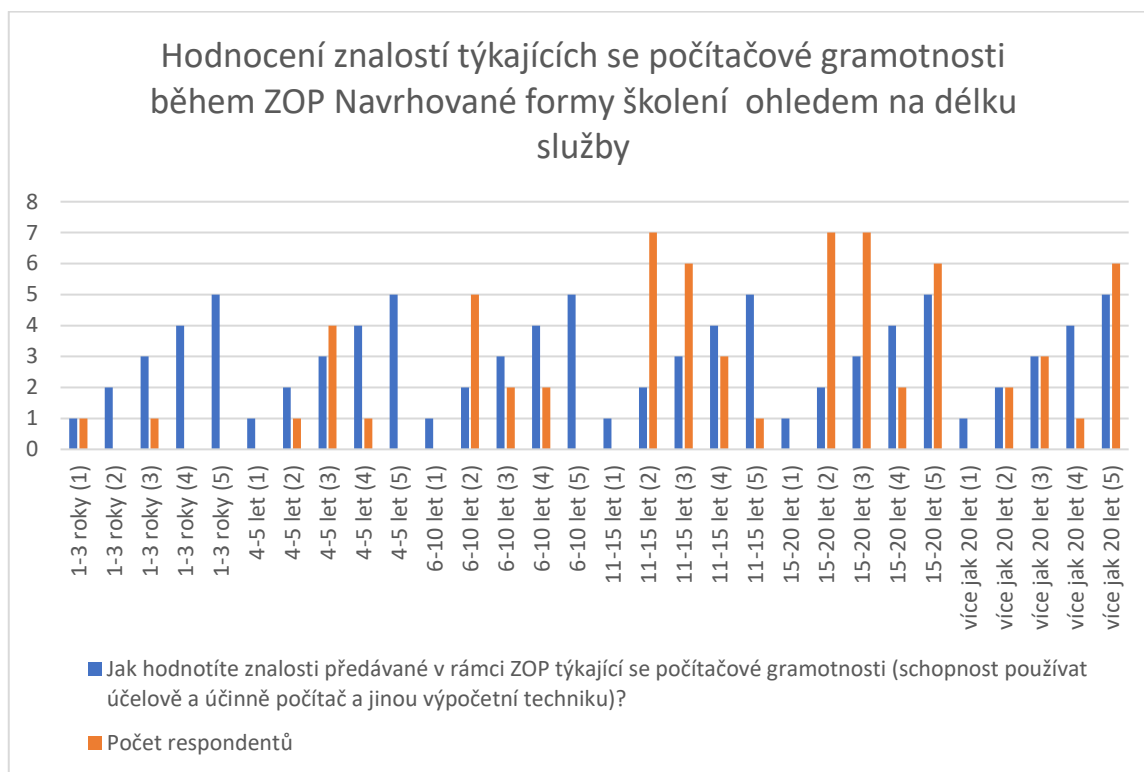
Znění výzkumné otázky: Jak hodnotíte znalosti předávané v rámci ZOP týkající se počítačové gramotnosti (schopnost používat účelově a účinně počítač a jinou výpočetní techniku)?

Graf č. 9 – Hodnocení znalostí týkajících se počítačové gramotnosti získané během ZOP



Situace je v případě znalostí v oblasti počítačové gramotnosti předávaných v rámci ZOP o poznání lepší. Zde 33,8 % zúčastněných uvedlo, že tyto byly spíše nedostatečné, 32,4 % jako spíše dostatečné, 19,1 % uvedlo, že žádné takové znalosti obsahem ZOP nebyly, 13,2 % uvedlo tyto znalosti jako zcela nedostatečné a 1,5 % jako zcela dostatečné. Zajímavým údajem sledávám skutečnost, kdy pouze 6 z 22 respondentů, jenž odpověděli, že tyto znalosti byly spíše dostatečné, slouží u Policie ČR déle jak 10 let. Velmi obdobný poměr je u osob reagujících jako spíše nedostatečně, kdy z celkových 23 osob pouze 7 osob slouží méně jak 10 let u Policie ČR.

Graf č. 10 – Hodnocení znalostí týkajících se počítačové gramotnosti získané během ZOP s ohledem na délku služby

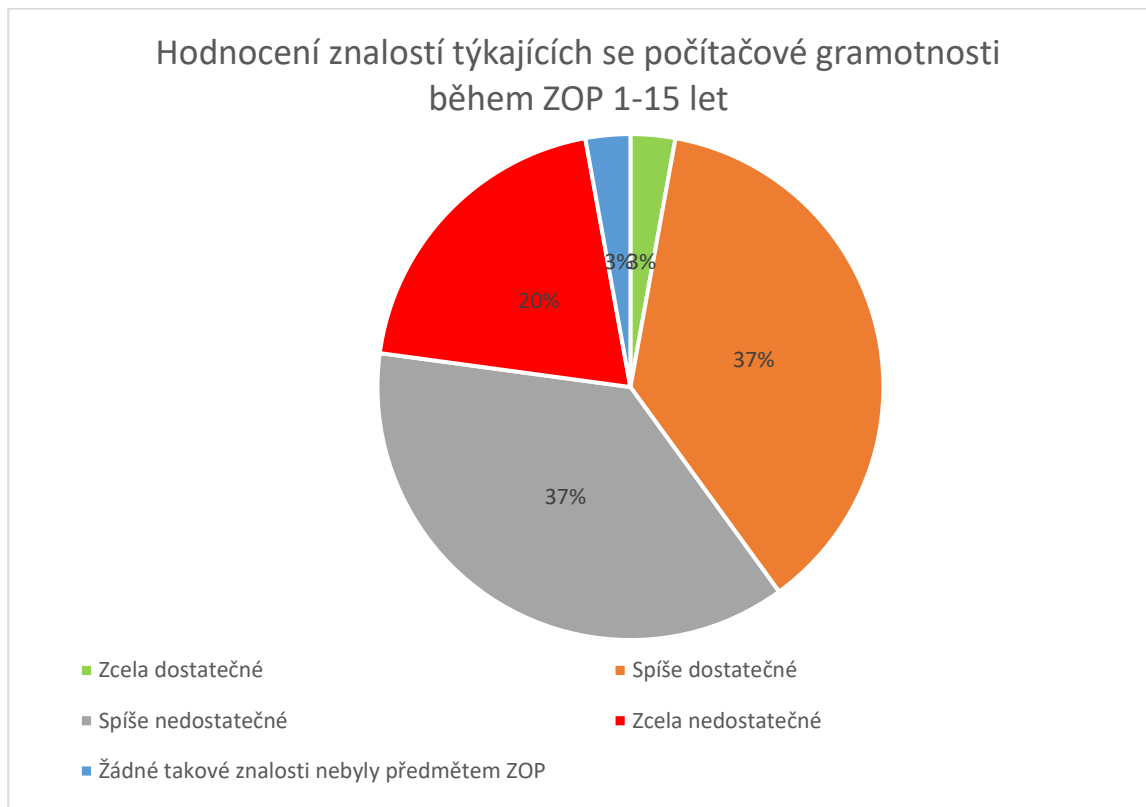


Výše uvedený graf znázorňuje hodnocení respondentů, kdy pro účely vypracování tohoto grafu bylo opět užito převodní tabulky dle kapitoly 4.2. I z tohoto grafu je patrné, že nejvíce respondentů uvádějících, že předmětem jejich ZOP nebyly žádné znalosti v oblasti počítačové gramotnosti, jsou osoby sloužící 15 a více let. Zde si je třeba opět uvědomit vzájemné souvislosti, kdy systém ETR¹⁵⁶ byl celoplošně zaveden u Policie ČR od 01. 01. 2008 a ani po této době nebylo výjimkou využívání psacích strojů k dokumentaci trestné činnosti.

Pokud bychom se tedy bavili pouze o policistech, kteří absolvovali ZOP zcela jistě již v době, kdy byl výše uvedený systém zaveden, pak bychom zjistili, že 37 % z nich shodně uvádí, že tyto znalosti byly předány spíše dostatečně i spíše nedostatečně. Dalších 20 % uvádí znalosti jako zcela nedostatečné a shodně 3 % uvádí, že žádné takové znalosti předmětem ZOP nebyly či byly zcela dostatečné. Uvedená zjištění ilustruje graf níže.

¹⁵⁶ Evidence trestního řízení

Graf č. 11 - Hodnocení znalostí týkajících se počítačové gramotnosti získané během ZOP s dobou služby 1-15 let



V rámci stanovení hypotézy se domnívám, že z důvodu objektivnosti je opět třeba zúžit okruh respondentů zahrnutých do této hypotézy, kdy však tentokrát se jedná o účastníky sloužící 15 a méně let.

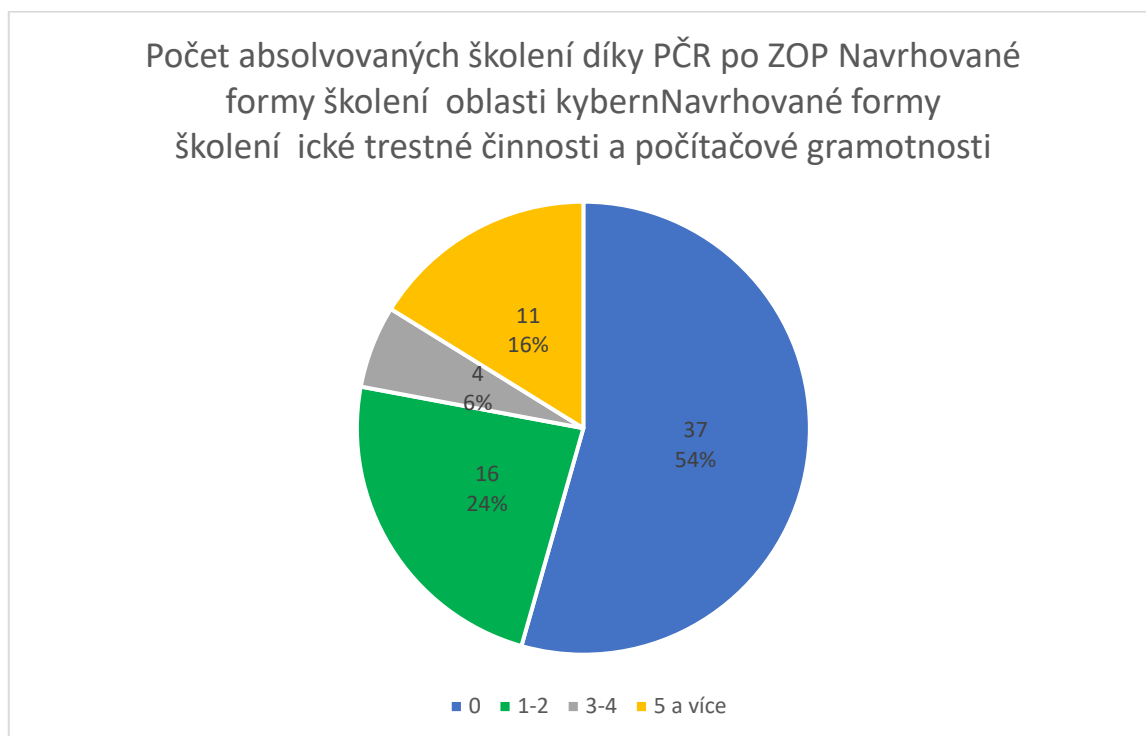
Hypotéza k výzkumné otázce č. 2 konstruovaná na základě odpovědí respondentů:

37 % respondentů sloužících 15 a méně let shodně uvádí, že v rámci jimi absolvované ZOP byly znalosti týkající se počítačové gramotnosti spíše dostatečné či spíše nedostatečné, 20 % uvádí znalosti jako zcela nedostatečné a 3 % tyto znalosti považuje za zcela dostačující, stejně jako 3 % uvádí, že žádné takové znalosti nebyly předmětem ZOP.

4.4. Odpovědi respondentů k výzkumné otázce č. 3

Znění výzkumné otázky: Kolik školení po ZOP týkajících se kybernetické trestné činnosti či počítačové gramotnosti jste díky PČR absolvovali?

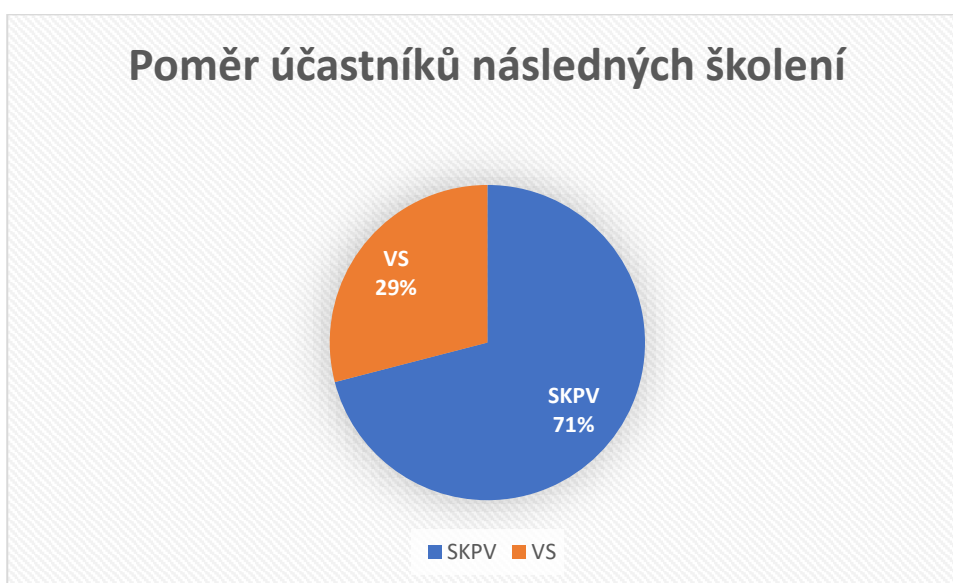
Graf č. 12 – Počet absolvovaných školení díky Policii ČR po ZOP v oblasti kybernetické trestné činnosti a počítačové gramotnosti



Pokud se podíváme na výsledky grafu č. 12, pak můžeme konstatovat, že nadpoloviční většina odpovídajících (54 %) neabsolvovala žádné školení týkající se kybernetické trestné činnosti či počítačové gramotnosti díky Policii ČR po absolvování ZOP. 24 % odpovídajících absolvovalo 1-2 školení, 6 % 3-4 školení a 16 % 5 a více školení. S ohledem na další zkoumání byly z hypotéz na otázky č. 4-6 vyloučeny odpovědi odpovídajících, kteří uvedli, že se neúčastnili žádného takového školení.

Zajímavé se jeví porovnání absolventů těchto školení, kdy z celkových 31 odpovídajících bylo 22 zařazených na člancích SKPV oproti 9 zařazeným na člancích vnější služby.

Graf č. 13 – Poměr účastníků následných školení



Hypotéza k výzkumné otázce č. 3 konstruovaná na základě odpovědí respondentů:

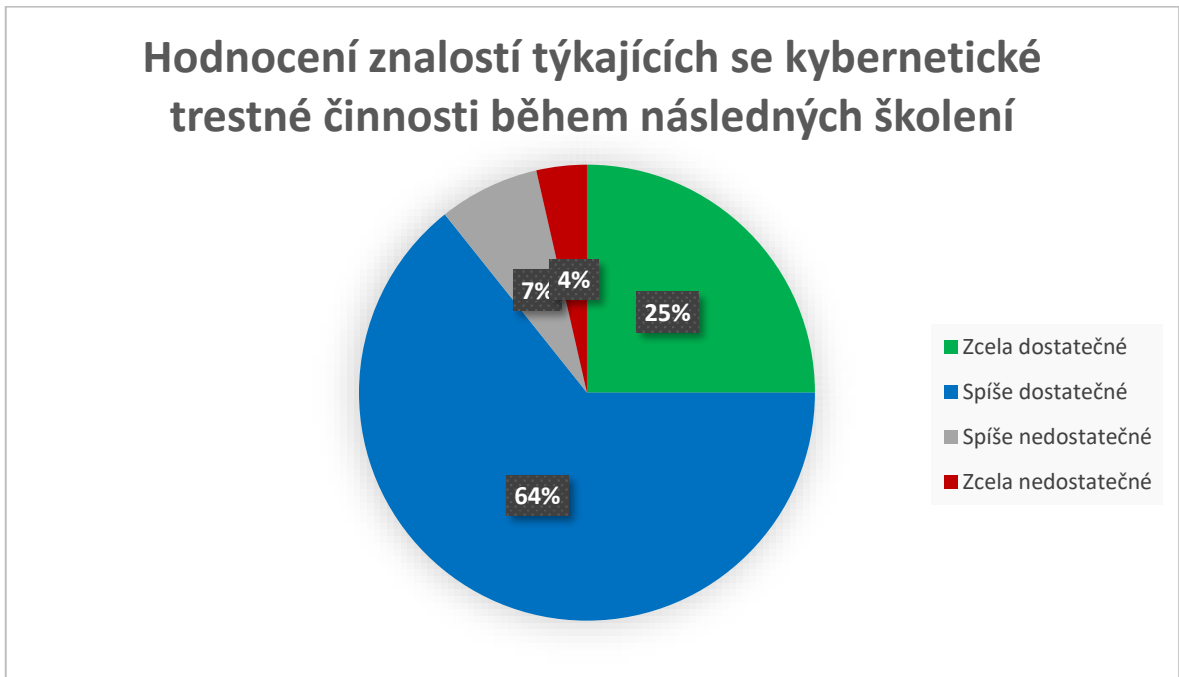
Nadpoloviční většina odpovídajících (54 %) neabsolvovala žádné školení týkající se kybernetické trestné činnosti či počítačové gramotnosti díky Policii ČR po absolvování ZOP. 24 % odpovídajících absolvovalo 1-2 školení, 6 % 3-4 školení a 16 % 5 a více školení.

4.5. Odpovědi respondentů k výzkumné otázce č. 4, č. 5 a č. 6

Znění výzkumných otázek: Jak hodnotíte znalosti předávané v rámci školení týkajících se kybernetické trestné činnosti? Jaké zaměření uvedená školení týkající se kybernetické trestné činnosti měla? Jak hodnotíte znalosti předávané v rámci školení týkající se počítačové gramotnosti?

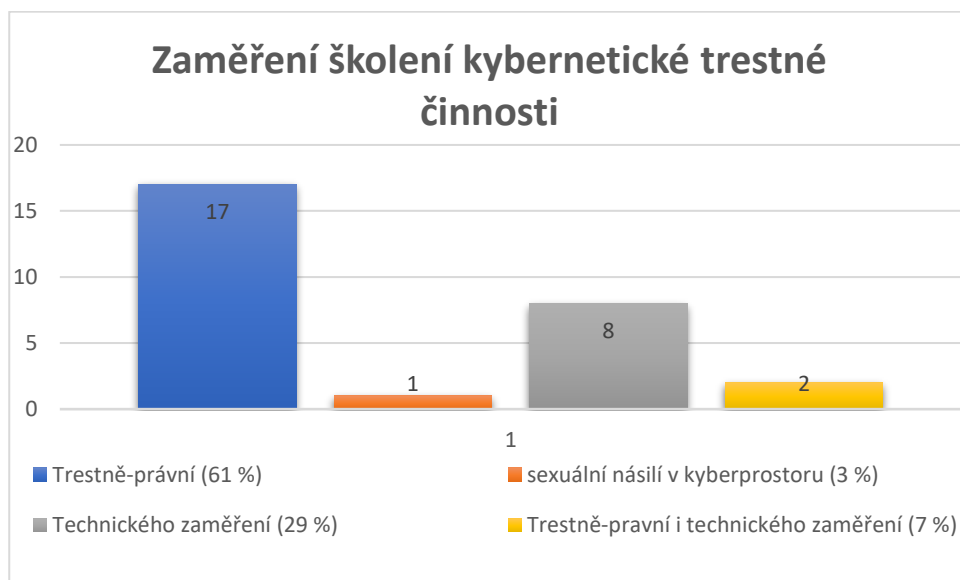
S ohledem na souvislost výzkumných otázek č. 4–6 bude vytvořena hypotéza souhrnně pro tyto otázky. Z uvedených 31 dotazovaných osob, které absolvovali jakékoliv následné školení, jich 28 absolvovalo školení z oblasti kybernetické trestné činnosti, 23 dotazovaných absolvovalo školení z oblasti počítačové gramotnosti a celkem 22 z dotazovaných absolvovalo školení v obou odvětvích. 71 % všech dotazovaných jakéhokoliv z výše uvedených následných školení absolvovalo školení z obou zjišťovaných oblastí.

Graf č. 14 – Hodnocení znalostí týkajících se kybernetické trestné činnosti získaných během následných školení



Velmi příjemné zjištění bylo, že 64 % dotazovaných uvádí získané znalosti jako spíše dostatečné a dalších 25 % jako zcela dostatečné. Což nám tedy v celkovém součtu činí 89 % „spokojených“ dotazovaných. 7 % uvádí, že znalosti jsou spíše nedostatečné, další 4 % je hodnotí jako zcela nedostatečné.

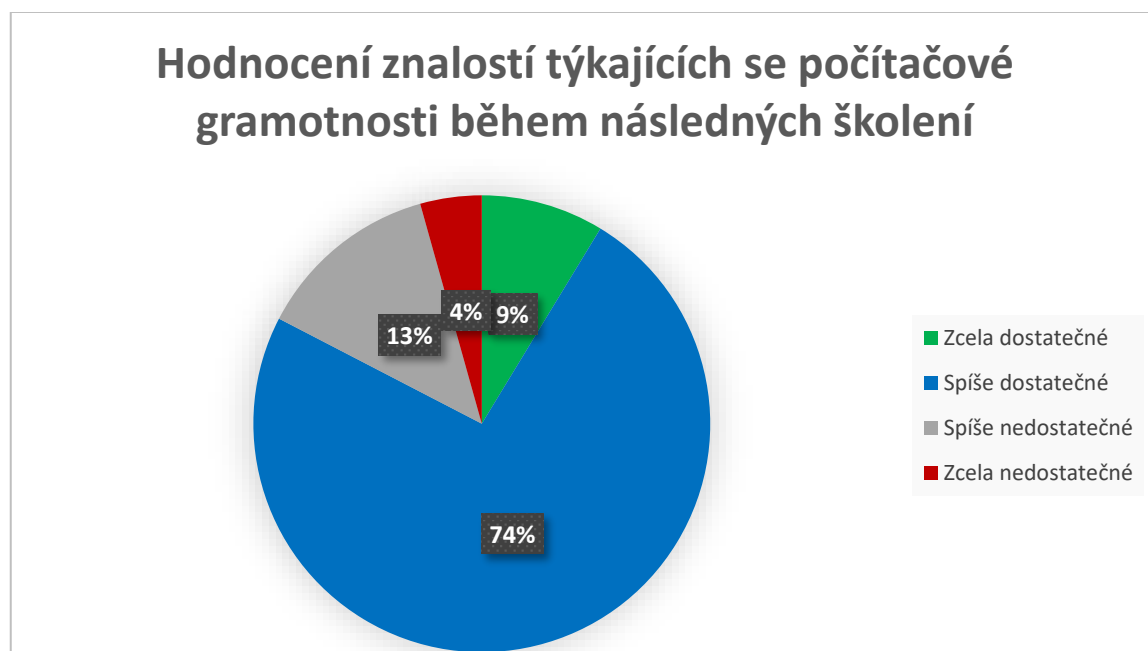
Graf č. 15 – Zaměření školení kybernetické trestné činnosti



Nejčastější zaměření následných školení kybernetické trestné činnosti bylo trestně-právní, a to v 61 % případů, 29 % školení bylo technického zaměření, 7 %

bylo částečně zaměřeno trestně-právně a částečně technicky a 3 % pak bylo zaměřeno na sexuální násilí v kyberprostoru. Bohužel nelze s jistotou určit, o jaké školení v případě daného sexuálního násilí v kyberprostoru šlo, jelikož pisatel diplomové práce si dokáže představit zaměření jak trestně-právní, tak technické a samozřejmě i smíšené.

Graf č. 16 – Hodnocení znalostí týkajících se počítačové gramotnosti získané během následných školení



74 % dotazovaných, kteří se zúčastnili některého z následných školení týkajících se počítačové gramotnosti uvádí, že předávané znalosti byly spíše dostatečné, dalších 9 % uvádí, že tyto znalosti byly zcela dostatečné. V tomto případě se tedy jedná o celkem 83 % „spokojených“ dotazovaných. 13 % uvádí znalosti jako spíše nedostatečné a 4 % jako zcela nedostatečné.

Hypotéza k výzkumným otázkám č. 4, č. 5 a č. 6 konstruovaná na základě odpovědí respondentů:

61 % dotazovaných osob absolvovalo trestně-právně zaměřené školení kybernetické trestné činnosti, 29 % technicky zaměřené školení kybernetické trestné činnosti, 7 % smíšený kurz obsahující obě uvedené oblasti a 3 % dotazovaných absolvovalo školení týkajícího se sexuálního násilí v kyberprostoru. Dotazovaní hodnotí tato školení kybernetické trestné činnosti kladně, kdy 64 % uvádí znalosti jako spíše dostatečné, 25 % jako zcela dostatečné, 7 % jako spíše

nedostatečné a pouhé 4 % jako zcela nedostatečné. V rámci školení počítačové gramotnosti je situace obdobná, kdy 74 % dotazovaných hodnotí znalosti jako spíše dostatečné, 13 % jako spíše nedostatečné, 9 % jako zcela dostatečné a opět pouze 4 % jako zcela nedostatečné.

4.6. Odpovědi respondentů k výzkumné otázce č. 7

Znění výzkumné otázky: Měli jste možnost se v rámci služebního poměru účastnit jakéhokoliv školení týkající se kybernetické trestné činnosti či počítačové gramotnosti?

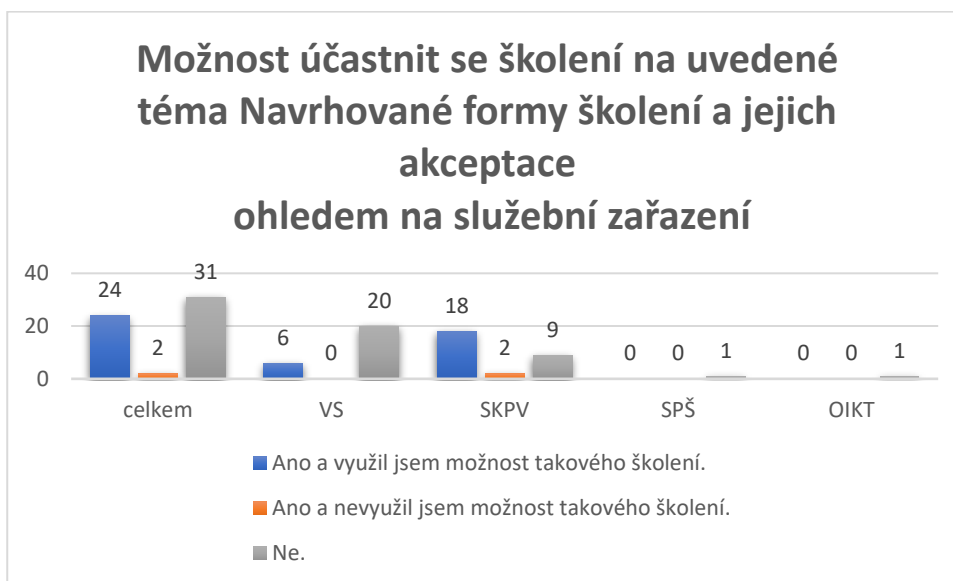
Při podrobném analyzování odpovědí subjektů výzkumu jsem zjistil, že celkem v 11 případech je odpověď na tuto otázku v přímém rozporu s odpovědí daného subjektu na výzkumnou otázkou č. 3, proto tyto odpovědi byly vyhodnoceny jako chybné a nejsou tedy obsahem dalšího vyhodnocení ve výzkumné otázce č. 7. Zpracovatele zajímají blíže subjekty, které nebyly účastni žádného z uvedených školení a důvody jejich neúčasti.

Graf č. 17 – Možnost účastnit se školení na téma kybernetická trestná činnost či počítačová gramotnost



Z uvedeného grafu vyplývá, že pouze 4 % zájmových subjektů uvedlo, že měli možnost se daného školení účastnit, ale této nevyužili, naopak 42 % uvedlo, že možnost školení využili, avšak 54 % uvedlo, že neměli možnost žádné takové školení absolvovat.

Graf č. 18 – Možnost účastnit se školení na uvedené téma s ohledem na služební zařazení



V rámci této výzkumné otázky jsem také vypracoval přehledový graf znázorňující porovnání účasti a samotné možnosti účasti policistů na základě jejich služebního zařazení. Z tohoto srovnání jednoznačně vyplývá, že příslušníci SKPV mají větší možnost ke zvyšování svých znalostí prostřednictvím školení. 62 % účastníků z SKPV uvedlo využití možnosti školení, 31 % možnost školení nemělo a 7 % přiznalo, že možnost účastnit se školení měli, ale nevyužili ji. Oproti tomu z vnější služby žádný respondent nevedl, že by měl možnost účastnit se školení, kterou odmítl, 77 % možnost účastnit se školení nikdy neměli a 23 % tuto možnost měli a využili ji. Policisté sloužící na Odboru informačních a komunikačních technologií a ve Školním policejním středisku shodně uvedli, že neměli možnost jakéhokoliv z uvedených školení. Vzhledem k nízkému počtu respondentů z Odboru informačních a komunikačních technologií a Školního policejního střediska nebudou tito (s ohledem na objektivnost) zahrnuti v konstruované hypotéze.

Hypotéza k výzkumné otázce č. 7 konstruovaná na základě odpovědí respondentů:

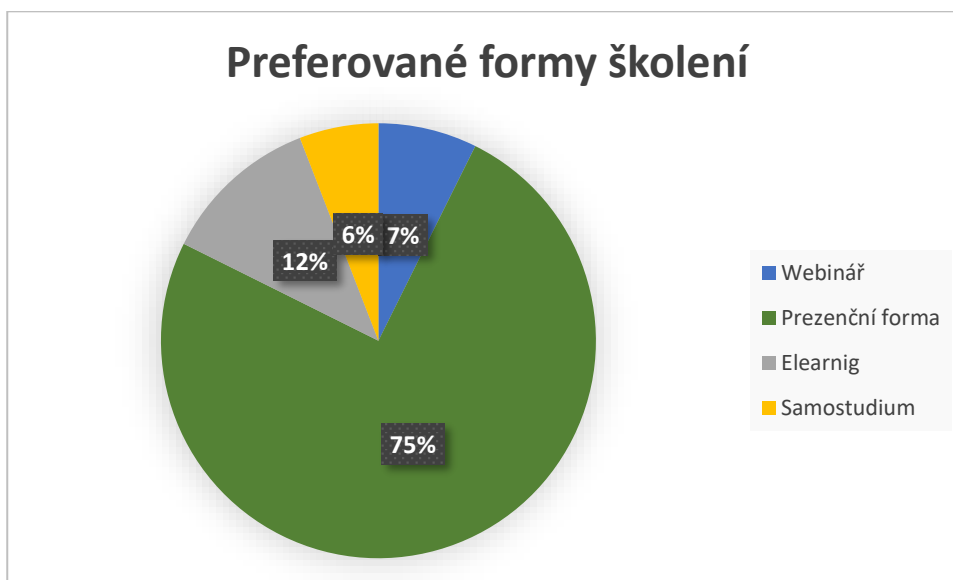
69 % subjektů výzkumu sloužících na článku SKPV mělo možnost se v rámci jejich služebního poměru účastnit školení z oblasti kybernetické trestné činnosti či počítačové gramotnosti, přičemž z těchto uvedenou možnost využilo 90 % a 10 % tuto možnost nevyužilo, 31 % subjektů z článků SKPV možnost takových školení nemělo. 77 % subjektů sloužících na článku vnější služby nemělo možnost v rámci

jejich služebního poměru účastnit se výše uvedených školení, 23 % tuto možnost mělo, přičemž ji využili ve 100 %.

4.7. Odpovědi respondentů k výzkumné otázce č. 8

Znění výzkumné otázky: Jakou formu vzdělávání v uvedené oblasti preferujete?

Graf č. 19 – Preferované formy školení



V uvedené otázce se tazatel zajímal o preferované možnosti forem školení účastníků dotazníkového šetření, kdy jako možnosti byly zvoleny běžné aktuální formy školení doplněné o samostudium. Možnosti subjektům dotazování byly předloženy elearning, webinář, prezenční forma, samostudium.

Hypotéza k výzkumné otázce č. 8 konstruovaná na základě odpovědí respondentů:

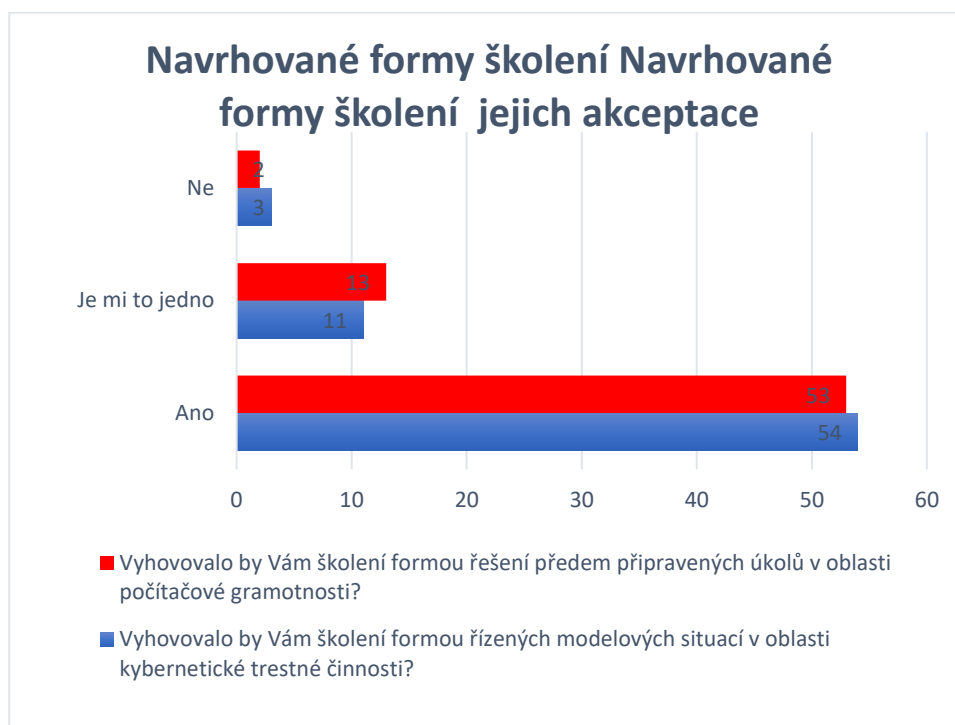
Ve ¾ případů subjekty dotazování preferují školení v oblasti kybernetické trestné činnosti a počítačové gramotnosti prezenční formou, zatímco 12 % preferuje školení formou elearnigu, 7 % formou webináře a 6 % subjektů dokazování preferují školení formou samostudia.

4.8. Odpovědi respondentů k výzkumné otázce č. 9 a č. 10

Znění výzkumné otázky: Vyhovovalo by Vám školení formou řízených modelových situací v oblasti kybernetické trestné činnosti? Vyhovovalo by Vám školení formou řešení předem připravených úkolů v oblasti počítačové gramotnosti?

S ohledem na obdobně položené otázky jsem tyto sloučil a budu vytvářet společnou hypotézu, jelikož odpovědi a zadání otázek jsou velmi podobné. Při samotném vyhodnocení odpovědí na uvedené otázky v souvislostech jsem zjistil, že pouze 9 z 68 respondentů odpovědělo na uvedené otázky rozdílně, zbytek respondentů odpovědělo vždy stejně – tedy v případě, kdy respondent uvedl, že by mu vyhovovalo školení v oblasti kybernetické trestné činnosti formou řízených modelových situací, pak uvedl, že by mu vyhovovalo školení týkající se počítačové gramotnosti formou předem připravených úkolů. Avšak i přes tuto skutečnost jsou odpovědi v celkovém počtu velmi podobné.

Graf č. 20 – Navrhované formy školení a jejich akceptace



79 % dotazovaných se domnívá, že by jim vyhovovalo školení ohledně kybernetické trestné činnosti formou řízených modelových situací, 16 % dotazovaných je to jedno a 5 % by takové školení nevyhovovalo. V oblasti počítačové gramotnosti dotazovaní v 78 % uvádí školení formou řešení předem připravených úkolů jako vyhovující, 19 % dotazovaných uvádí, že je jim to jedno a pouhé 3 % dotazovaných uvádí takové školení jako nevyhovující.

Hypotéza k výzkumným otázkám č. 9 a 10 konstruovaná na základě odpovědí respondentů:

Více jak $\frac{3}{4}$ respondentů se domnívá, že mezi školení v rámci kybernetické trestné činnosti by měla být zahrnuta školení formou řízených modelových situací a v oblasti počítačové gramotnosti školení formou řešení předem připravených úkolů, 5 % potažmo 3 % takové školení nevyhovuje a 16 % potažmo 19 % uvádí, že je jim to jedno.

Závěr

Kybernetická trestná činnost během posledních let výrazně narůstá, zvyšují se pachatelé způsobené škody, avšak podíl objasněných trestných činů se stále snižuje. Nejedná se o situaci, která by reflektovala stav pouze na území Plzeňského kraje či České republiky, jedná se o situaci napříč světem. Stejně problémy, které jsou řešeny v rámci prověřování těchto trestných činů na území České republiky, řeší také nejméně ostatní země Evropy. V rámci vzdělávacích programů vytvářených agenturou CEPOL tak stále častěji vídáme nabídky na účast v programech zabývajících se právě výpočetní technikou či některým z druhů kybernetické trestné činnosti. Mohlo by se proto zdát, že uvedená koncepce nebude mít mnoho praktického využití, opak je však pravdou, jelikož vzdělávání prostřednictvím agentury CEPOL probíhá v anglickém jazyce, kdy signifikantní počet policistů má v tomto ohledu jazykovou bariéru.

Stejně tak je třeba mít na paměti, že prověřování a vyšetřování kybernetické trestné činnosti, a s tím související zvýšená počítačová gramotnost, činí většinu policistů závažný problém. I přes skutečnost, že v posledních letech se do vzdělávacích programů v rámci Policie ČR dostaly části základních informací týkajících se prověřování kybernetické trestné činnosti, je většina policistů v této oblasti velmi nezkušená. Tato situace není však problémem pouze v rámci policistů sloužících v územní působnosti Krajského ředitelství policie Plzeňského kraje, ale tato situace je celorepubliková.

Tato diplomová práce si dala za cíl vytvořit koncepci policejního vzdělávání v oblasti kybernetické trestné činnosti a zvýšení počítačové gramotnosti policistů v Plzeňském kraji a domnívám se, že tohoto cíle bylo dosaženo. Je třeba upozornit na skutečnost, že cílem práce nebylo do detailu propracovat jednotlivá školení, řízené modelové situace nebo předem připravené úkoly k řešení v oblasti počítačové gramotnosti¹⁵⁷. Práce je multidisciplinárního charakteru a jejím největším přínosem je prezentace reálně splnitelné koncepce příslušného vzdělávání policistů v Plzeňském kraji, která v sobě komponuje předpokládané znalosti trestně právní povahy policistů společně s technickými definicemi

¹⁵⁷ Dále jen předem připravené úkoly.

základních pojmů a praktickými ukázkami či příklady, kdy předpokládám využití této koncepce i v samotné praxi, na základě mého služebního zařazení a postavení. Největší odlišností, a podle mého názoru také největší přidanou hodnotou představeného konceptu vzdělávání, oproti dřívějším či aktuálně probíhajícím výukovým programům, je představení plánovaných řízených modelových situací a předem připravených úkolů. Vypracování samotných modelových situací a předem připravených úkolů k řešení bude časově velmi náročné, jelikož tvůrce se musí pokusit identifikovat, vzájemně skloubit a vypracovat veškeré možné scénáře dotazů a návazných odpovědí, které by účastníky mohli napadnout. Stejně tak následné samotné provedení těchto modelových situací a předem připravených úkolů bude časově velmi náročné. Proto v tomto ohledu bude pracovní skupina KYBER sloužit jako testovací skupina uchazečů. Tito budou prvními účastníky této koncepce, jež budou poskytovat důležitou prvotní zpětnou vazbu k uvedeným školením, modelovým situacím a předem připraveným úkolům. Na jejich základě, vyhodnocením jednotlivých připomínek a jejich doplnění ze strany testovací skupiny, budou dotvořeny jednotlivá skripta zmiňovaná v kapitole č. 3. Následně předpokládám vytvoření instruktorů modelových situací a předem připravených úkolů z členů pracovní skupiny, kteří budou zodpovědní za jejich předávání v rámci jejich služební působnosti. Tento způsob jsem vyhodnotil jako nejefektivnější s ohledem na personální a časové možnosti KŘPP. Samozřejmě předpokládám také určité posílení instruktorů ze strany OAKK KŘPP zejména vůči Městskému ředitelství policie Plzeň, jež má největší počet sloužících policistů a jejich proškolení by tak bylo časově velmi náročné.

V rámci provedeného výzkumu ze strany příslušníků Policie ČR zcela jasně vyplynulo, že znalosti předávané v rámci základních odborných příprav v oblasti kybernetické trestné činnosti byly většinou nulové nebo jakkoliv nedostatečné, o něco lepší situace je v oblasti počítačové gramotnosti. Další zajímavé zjištění bylo, že větší polovina respondentů neměla možnost účastnit se jakéhokoliv školení týkajícího se počítačové gramotnosti nebo kybernetické trestné činnosti (vyjma ZOP), kdy i v tomto ohledu spatřuji jednoznačný přínos této diplomové práce, kdy by takovou možnost při zavedení předpokládaných školení měli

policisté dostat. V první řadě bude třeba diskutovat pravidla výše popsané koncepce s vedením KŘPP, kdy dle předběžných zjištění je nejméně vedení SKPV těmto nakloněno. V další řadě by díky tomuto v následujících měsících a letech měli mít policisté v působnosti KŘPP mnohem více možností účastnit se dalších vzdělávacích aktivit směrem ke kybernetické trestné činnosti a počítačové gramotnosti, čímž by si zvyšovali vlastní povědomí v uvedené oblasti. Zamýšleným následkem by mělo dojít k efektivnějšímu a rychlejšímu zpracování spisových materiálů. Stejně tak tyto policisté budou moci nabyté informace o jednotlivých způsobech kontaktování poškozených pachatelů předávat dále ve svých rodinách a u svých známých tak, aby se i tímto způsobem mohla samovolně šířit prevence proti kybernetické trestné činnosti.

Závěrem je však třeba zmínit, že ani ty nejlépe vymyšlené výukové metody samy o sobě nejsou klíčem k úspěchu v rámci odhalování a vyšetřování kybernetické trestné činnosti. Klíčem k úspěchu bude vždy zejména píle a osobní odhodlání každého z policistů, jejich nasazení a schopnost zajistit všechny dostupné důkazy vytvořené pachatelů, jejich vyhodnocení vzájemně i samostatně a následně kvalifikované a odůvodněné rozhodnutí v konkrétní věci.

Seznam použité literatury

Monografie

1. JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti = Cyber security glossary*. Praha: Česká pobočka AFCEA, Centrum kybernetické bezpečnosti, z.ú., 2022, 10. 10. 2022. ISBN 978-80-908388-4-0.
2. KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. ISBN 978-80-88168-15-7.
3. MOLNÁR, Zdeněk, MILDEROVÁ, Stanislava, ŘEZANKOVÁ, Hana, BRXÍ, Radim a KALINA Jaroslav. *Pokročilé metody vědecké práce*. Zeleneč: Profess Consulting, 2012. Věda pro praxi (Profess Consulting). ISBN 978-80-7259-064-3.
4. MUSIL, Jan, KONRÁD, Zdeněk a SUCHÁNEK, Jaroslav. *Kriminalistika*. 2. přepracované a doplněné vyd., Praha, C.H.Beck, 2004. ISBN 80-7179-878-9.

Zákonná úprava a IAŘ (interní akty řízení)

1. *103 POKYN policejního prezidenta ze dne 28. května 2013, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení*. 28. 05. 2013. Str. 3. Dostupné z: <http://esiar.pcr.cz/kniha/siar>. [cit. 2023-09-10].
2. *108 ROZKAZ ředitele Krajského ředitelství policie Plzeňského kraje ze dne 12. října 2023, kterým se zřizuje pracovní skupina KYBER*. 12. 10. 2023. Dostupné z: <http://esiar.pcr.cz/kniha/siar>. [cit. 2024-02-10]
3. *Zákon č. 40/2009 Sb., trestní zákoník, ve znění účinném ke dni 04. 02. 2024*
4. *Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění účinném ke dni 04. 02. 2024*
5. *Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů*. Online. Dostupné z: <https://www.zakonyprolidi.cz/cs/2008-300#p2>. [cit. 2024-02-02].

6. Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti). Online. Dostupné z: <https://www.zakonyprolidi.cz/cs/2004-480>. [cit. 2024-02-02].

Webové stránky a elektronické zdroje

1. BHASKER, Das. *Darknet vs. Dark Web vs. Deep Web vs. Surface Web — The Difference*. Online. In: TechLog360, 16. 03. 2022. Dostupné z: <https://techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/>. [cit. 2023-10-05].
2. COPELAND, B.J. *artificial intelligence*. Online. In: Encyklopedia Britannica, 18. 11. 2023. Dostupné z: <https://www.britannica.com/technology/artificial-intelligence>. [cit. 2024-02-02].
3. Council of Europe. *Úmluva o počítačové kriminalitě*. Online. In: Council of Europe, 04. 01. 2013. Dostupné z: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804931c0>. [cit. 2023-09-10].
4. ČÁP, Jan plk. v. v. Mgr. *100 Bezpečnostní teorie a praxe 1/2022 informace – Zajišťování, zpřístupňování a vyhodnocování digitálních stop*. Online. PDF. In: Policejní akademie ČR, 06. 04. 2022. Dostupné z: <https://veda.polac.cz/wp-content/uploads/2022/04/Zajistovani-zpristupnovani-a-vyhodnocovani-digitalnich-stop.pdf>. [cit. 2023-11-23].
5. Česká bankovní asociace. *Češi a kyberbezpečnost*. Online. In: Česká bankovní asociace, 30. 01. 2024. Dostupné z: <https://cbaonline.cz/cesi-a-kyberbezpecnost-2024>. [cit. 2024-02-05].
6. Česká spořitelna. *Co je kryptoměna*. Online. In: Česká spořitelna. Dostupné z: <https://www.csas.cz/cs/financni-slovník/kryptomeny>. [cit. 2024-02-23].
7. Český statistický úřad. *20. INFORMAČNÍ A KOMUNIKAČNÍ TECHNOLOGIE*. Online. In: Český statistický úřad, 18. 02. 2011. Dostupné z: <https://www.czso.cz/documents/10180/25385875/19874229+000110c20.p>

- df/08cfdb7a-a8c6-4fc4-83a8-4ee94258aab2?version=1.0. [cit. 2023-09-11].
8. ECDL PROFILE. *O konceptu ECDL/ICDL*. Online. In: ECDL PROFILE. Dostupné z: https://www.ecdl.cz/o_projektu.php. [cit. 2023-09-11].
 9. ENISA. *What is "Social Engineering"?*. Online. In: ENISA. Dostupné z: <https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering>. [cit. 2024-02-04].
 10. FOLGER, Jean. *What Is Spoofing? How Scam Works and How To Protect Yourself*. Online. In: Investopedia, 2022, 07. 09. 2022. Dostupné z: <https://www.investopedia.com/terms/s/spoofing.asp>. [cit. 2024-02-03].
 11. GILLIS, Alexander S. *internet of things (IoT)*. Online. In: TechTarget, srpen 2023. Dostupné z: <https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT>. [cit. 2024-02-03].
 12. ICDL Europe. *About us*. Online. In: ICDL Europe. Dostupné z: <https://icdleurope.org/about-us/>. [cit. 2023-09-11].
 13. Infoz.cz Slovník cizích slov. *Slovník výpočetní techniky*. Online. In: Infoz.cz slovník cizích slov. Dostupné z: <https://www.infoz.cz/slovník-vypocetni-techniky/>. [cit. 2023-11-17].
 14. INTERNETEM BEZPEČNĚ. *Kybergrooming*. Online. In: INTERNETEM BEZPEČNĚ. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/>. [cit. 2024-02-04].
 15. INTERNETEM BEZPEČNĚ. *Kyberstalking*. Online. In: INTERNETEM BEZPEČNĚ. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/>. [cit. 2024-02-04].
 16. IT Slovník. *Co je to Grafická karta?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/graficka-karta>. [cit. 2024-02-23].
 17. IT Slovník. *Co je to chipset?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/chipset>. [cit. 2024-02-23].
 18. IT Slovník. *Co je to Pevný disk?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/pevny-disk>. [cit. 2024-02-23].
 19. IT Slovník. *Co je to procesor?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/procesor>. [cit. 2024-02-23].

20. IT Slovník. *Co je to RAM?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/ram>. [cit. 2024-02-23].
21. IT Slovník. *Co je to Základní deska?*. Online. In: IT Slovník. Dostupné z: <https://it-slovník.cz/pojem/zakladni-deska>. [cit. 2024-02-23].
22. IT SLOVNÍK.cz. *Co znamená zkratka EXIF?* Online. In: IT SLOVNÍK.cz. Dostupné z: <https://it-slovník.cz/pojem/exif>. [cit. 2024-02-03].
23. KOPECKÝ, Kamil. *Policejní virus znovu útočí - tentokráte s prezidentem Zemanem v záhlaví*. Online. In: Projekt E-Bezpečí. 24. 03. 2014. Dostupné z: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/sociotechnikax/843-policejni-virus-znovu-utoci-tentokrate-s-prezidentem-zemanem-v-zahlavi>. [cit. 2024-03-11].
24. MCCANCE, Shaun, CAMPBELL, Jim, HILL, Michael a GERASIMOVA, Ekaterina. *Co je to MAC adresa*. Online. In: GNOME HELP. Dostupné z: <https://help.gnome.org/users/gnome-help/stable/net-macaddress.html.cs>. [cit. 2024-02-11].
25. MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2022*. Online. In: Policie České republiky, 13. 01. 2013. Dostupné z: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx>. [cit. 2024-02-04].
26. MORAVČÍK, Ondřej. *Vývoj registrované kriminality v roce 2023*. Online. In: Policie České republiky, 12. 01. 2024. Dostupné z: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2023.aspx>. [cit. 2024-02-04].
27. NAJJAR, Shebab. *WEBINT in Action | Real-World Applications and Use Cases*. Online. In: Medium, 04. 05. 2023. Dostupné z: <https://osintteam.blog/webint-in-action-real-world-applications-and-use-cases-1c052530698b>. [cit. 2024-02-11].
28. PETERKA, Jiří. *Terminologie datových sítí*. Online. In: eARCHIV, březen 2000. Dostupné z: <http://www.earchiv.cz/b00/b0003002.php3>. [cit. 2024-01-29].
29. Policie České republiky – KŘP Plzeňského kraje. *Statistické ukazatele za rok 2023*. Online. In: Policie České republiky. Dostupné z:

- <https://www.policie.cz/clanek/statisticke-ukazatele-za-rok-2023.aspx>. [cit. 2024-02-10].
30. Policie České republiky. *Kyberkriminalita*. Online. In: Policie České republiky. Dostupné z: <https://www.policie.cz/clanek/kyberkriminalita.aspx>. [cit. 2024-02-20].
31. Policie České republiky. *Útvar policejního vzdělávání a služební přípravy*. Online. In: Policie České republiky. Dostupné z: <https://www.policie.cz/clanek/utvar-policejního-vzdelavani-a-sluzebni-pripravy.aspx>. [cit. 2024-02-11].
32. *Ransomware Explained. What It Is and How It Works*. Online. In: Heimdal Security [online]. 27. 07. 2023 [cit. 2024-03-11]. Dostupné z: <https://heimdalsecurity.com/blog/ransomware/>
33. RAY, Michael. *social network computing*. Online. In: Encyklopedie Britannica, 09. 01. 2024. Dostupné z: <https://www.britannica.com/technology/social-network>. [cit. 2024-02-02].
34. SPRÁVA SÍŤE slovník pojmů. *Co je IMAP*. Online. In: SPRÁVA SÍŤE slovník pojmů. Dostupné z: <https://www.sprava-site.eu/pop3/>. [cit. 2024-03-06].
35. SPRÁVA SÍŤE slovník pojmů. *Co je to POP3*. Online. In: SPRÁVA SÍŤE slovník pojmů. Dostupné z: <https://www.sprava-site.eu/pop3/>. [cit. 2024-02-02].
36. SPRÁVA SÍŤE slovník pojmů. *Co je to protokol*. Online. In: SPRÁVA SÍŤE slovník pojmů. Dostupné z: <https://www.sprava-site.eu/protokol/>. [cit. 2024-02-02].
37. VINČÁLEK, Jakub. *Jak se vyvíjí objasněnost trestných činů v kyberprostoru?*. Online. In: Statistika & My Magazín Českého statistického úřadu. 16. 05. 2023. Dostupné z: <https://www.statistikaamy.cz/2023/05/16/jak-se-vyviji-objasnenost-trestnych-cinu-v-kyberprostoru>. [cit. 2024-02-10].
38. *VZDĚLÁVACÍ PROGRAM Dítě v trestním řízení, kódové označení P3/0073, č.j. UPVSP-3250-6/ČJ-2019-910010*. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].

39. VZDĚLÁVACÍ PROGRAM *Kriminální zpravodajská analýza, kódové označení P2/0188, č.j. UPVSP-675-10/ČJ-2018-9100KR*. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].
40. VZDĚLÁVACÍ PROGRAM *kvalifikačního kurzu Hospodářská kriminalita, kódové označení, č.j. PA-1968-1/-2016-820060*. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].
41. VZDĚLÁVACÍ PROGRAM *Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat – prolongace, kódové označení P2/0298, č.j. UPVSP-/ČJ-4124-3/ČJ-2022-910010*. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].
42. VZDĚLÁVACÍ PROGRAM *Provádění kriminalistickotechnických úkonů při zajišťování výpočetní techniky a digitálních dat, kódové označení P2/0279, č.j. UPVSP-/ČJ-4124-2/ČJ-2022-910010*. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].
43. VZDĚLÁVACÍ PROGRAM *SKPV – profesní specializace odhalování, kódové označení P2/0311b, č.j. UPVSP-3953-3/ČJ-2021-910010*. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].
44. VZDĚLÁVACÍ PROGRAM *SKPV – profesní specializace vyšetřování, kódové označení P2/0312, č.j. UPVSP-3953-2/ČJ-2021-910010*. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].
45. VZDĚLÁVACÍ PROGRAM *Specializační kurz MS EXCEL – pro pokročilé, kódové označení P2/0157, č.j. VO-504/2006*. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].
46. VZDĚLÁVACÍ PROGRAM *Specializační kurz MS EXCEL – základní kurz, kódové označení P2/0159, č.j. VO-503/2006*. PDF. Dostupné z: 10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].
47. WATSON, Robert. *Tor Path Diagram*. Online. PDF. In: Tor Project. 21. 07. 2008. Dostupné z: <https://svn-archive.torproject.org/svn/projects/presentations/security-part2-anon/tor-safe-selection.pdf>. [cit. 2024-03-11].
48. *Základní odborná příprava příslušníků Policie ČR – společné minimum bez specializace (univerzální ZOP) blended learning, Kódové označení:*

P1/0038, Č. j. UPVSP-3208-1/ČJ-2020-910010 PDF. Dostupné z:
10.208.51.99/vzdelavaci_aktivity/. [cit. 2023-10-30].

Seznam grafů

Graf č.1 – Rozdělení respondentů dle pohlaví	74
Graf č. 2 – Rozdělení respondentů dle věku	74
Graf č. 3 – Rozdělení respondentů dle dosaženého vzdělání	75
Graf č. 4 – Rozdělení respondentů dle služebního zařazení.....	76
Graf č. 5 – Rozdělení respondentů dle náplně práce	77
Graf č. 6 – Rozdělení respondentů dle délky služby	77
Graf č. 7 – Hodnocení znalostí týkajících se kybernetické trestné činnosti získané během ZOP	78
Graf č. 8 – Hodnocení znalostí týkajících se kybernetické trestné získané během ZOP s ohledem na délku služby.....	79
Graf č. 8 - Hodnocení znalostí týkajících se kybernetické trestné činnosti získané během ZOP s dobou služby 1-10 let.....	81
Graf č. 9 – Hodnocení znalostí týkajících se počítačové gramotnosti získané během ZOP	82
Graf č. 10 – Hodnocení znalostí týkajících se počítačové gramotnosti získané během ZOP s ohledem na délku služby.....	83
Graf č. 11 - Hodnocení znalostí týkajících se počítačové gramotnosti získané během ZOP s dobou služby 1-15 let.....	84
Graf č. 12 – Počet absolvovaných školení díky Policii ČR po ZOP v oblasti kybernetické trestné činnosti a počítačové gramotnosti	85
Graf č. 13 – Poměr účastníků následných školení	86
Graf č. 14 – Hodnocení znalostí týkajících se kybernetické trestné činnosti získaných během následných školení	87
Graf č. 15 – Zaměření školení kybernetické trestné činnosti.....	87
Graf č. 16 – Hodnocení znalostí týkajících se počítačové gramotnosti získané během následných školení.....	88

Graf č. 17 – Možnost účastnit se školení na téma kybernetická trestná činnost či počítačová gramotnost.....	89
Graf č. 18 – Možnost účastnit se školení na uvedené téma s ohledem na služební zařazení	90
Graf č. 19 – Preferované formy školení.....	91
Graf č. 20 – Navrhované formy školení a jejich akceptace	92

Seznam obrázků

Obrázek č. 1 – Policejní virus.....	107
Obrázek č. 2 – Ransomware vyskakovací okno.....	108
Obrázek č. 3 – Diagram sítě Tor	109
Obrázek č. 4 – Náhled EXIF dat Zoner Photo Studio X	110
Obrázek č. 5 – Náhled EXIF dat Zoner Photo Studio X	111
Obrázek č. 6 – Vlastnosti obrázku dostupné standardně v Microsoft Windows	112
Obrázek č. 7 – Vlastnosti obrázku dostupné standardně v Microsoft Windows	113

Obrázek č. 1 – Policejní virus

Policie. VAROVÁNÍ! Váš prohlížeč je uzamčen z bezpečnostních důvodů z následujících důvodů. Všechny činnosti tohoto počítače byly zaznamenány...

alert.security1-10000243.com.co/424250125D6922105F8C339DFD52A851

Služba Kriminální Policie a Vyšetřování
Útvar pro Boj proti Kyberkriminalitě

SLUŽBA KRIMINÁLNÍ POLICIE A VYŠETŘOVÁNÍ

Země: Czech Republic
ID: 86H65F825104R

VAROVÁNÍ!
Váš prohlížeč je uzamčen z bezpečnostních důvodů z následujících důvodů.
Všechny operace prováděné na tomto počítači jsou zaznamenány.
Všechny Vaše soubory jsou zašifrovány.

Jste obviněn z prohlížení/skladování a/nebo distribuce pornografických materiálů zakázáno obsahu (dětská pornografie/Zvířecost atd.). Že jste porušil Všeobecnou deklaraci o boji proti šíření dětské pornografie a obviněn z trestného činu podle článku 161 trestního zákoníku České republiky.

Článek 161 trestního zákoníku České republiky stanoví jako trest odnětí svobody v trvání 5-11 roků.

Také jste osoba podezřelá z porušení "zákon o autorském právu a právech souvisejících s právem" (stahování pirátské hudby, videa, bez licence software) a použití a/nebo šíření obsahu chráněného autorskými právy. Tím jste osoba podezřelá z porušení článku 148 trestního zákoníku České republiky.

Článek 148 trestního zákoníku České republiky, musí být trest pokuta 150 až 550 základních jednotek nebo odnětím svobody na dobu 3-7 roků.

S vešeho počítače byl proveden neoprávněný přístup k omezenému přístupu veřejnosti k informacím a informacím národního významu na internetu.

Neautorizovaný přístup si můžete sjednat záměrně z sobeckých motivů nebo neoprávněným přístupem může dojít bez Vašeho vědomí nebo souhlasu, jak váš osobní počítač může být napaden škodlivým softwarem. Proto, jste podezřelí, že zkoumat, neúmyslné porušení článku 215 trestního zákoníku České republiky (dále jen "zákon

Zbývající čas: 23:59:17

paysafecard Ukash

PIN Kód Hodnota
Zadejte kód 2000

1 2 3 4 5 6 7 8 9 0 Clear

Zaplatit PaySafeCard Zaplatit Ukash

Kde mohu získat peněžní poukázku PaySafeCard?

PaySafeCard můžete naprosto bezpečně zakoupit ve své blízkosti, v České republice např. v řadě novinových stánek a trafik v uvedených časech. PaySafeCard je k dostání v mnoha supermarketech, na čerpacích stanicích. Přehled prodejců: Tipsport, RoBIN OIL, Zabka, PAPOIL, JPServis, Euro Oil, Shell, Agip, OMV, WestPay.
Internetový obchod: www.WertKartenVerkauf.com

wertkartenverkauf.com

Kde mohu získat peněžní poukázku Ukash?

158

¹⁵⁸ KOPECKÝ, Kamil. *Policejní virus znovu útočí - tentokrát s prezidentem Zemanem v záhlaví*. Online. In: Projekt E-Bezpečí. 24. 03. 2014. Dostupné z: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/sociotechnikax/843-policejni-virus-znovu-utoci-tentokrat-s-prezidentem-zemanem-v-zahlavi>. [cit. 2024-03-11].

107

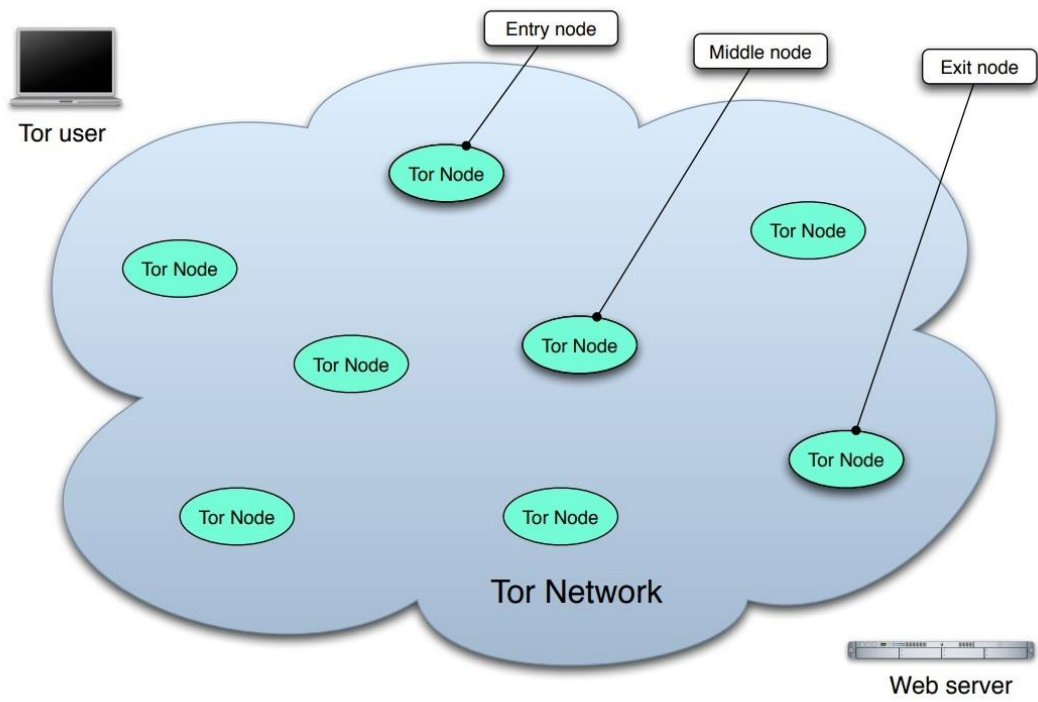
Obrázek č. 2 – Ransomware vyskakovací okno



159

¹⁵⁹ *Ransomware Explained. What It Is and How It Works.* In: Heimdal Security [online]. 27. 07. 2023 [cit. 2024-03-11]. Dostupné z: <https://heimdalsecurity.com/blog/ransomware/>

Obrázek č. 3 – Diagram síť Tor



160

¹⁶⁰ WATSON, Robert. *Tor Path Diagram*. Online. PDF. In: Tor Project. 21. 07. 2008. Dostupné z: <https://svn-archive.torproject.org/svn/projects/presentations/security-part2-anon/tor-safe-selection.pdf>. [cit. 2024-03-11].

Obrázek č. 4 – Náhled EXIF dat Zoner Photo Studio X

Informace o souboru
✕



Jméno souboru: IMG_0225

Velikost souboru: 37.5 MB (39 288 078 bajtů)

Rozměry: 5760 x 3840

Bitová hloubka: 24

Datum pořízení: neděle 15. října 2023 9:03:10

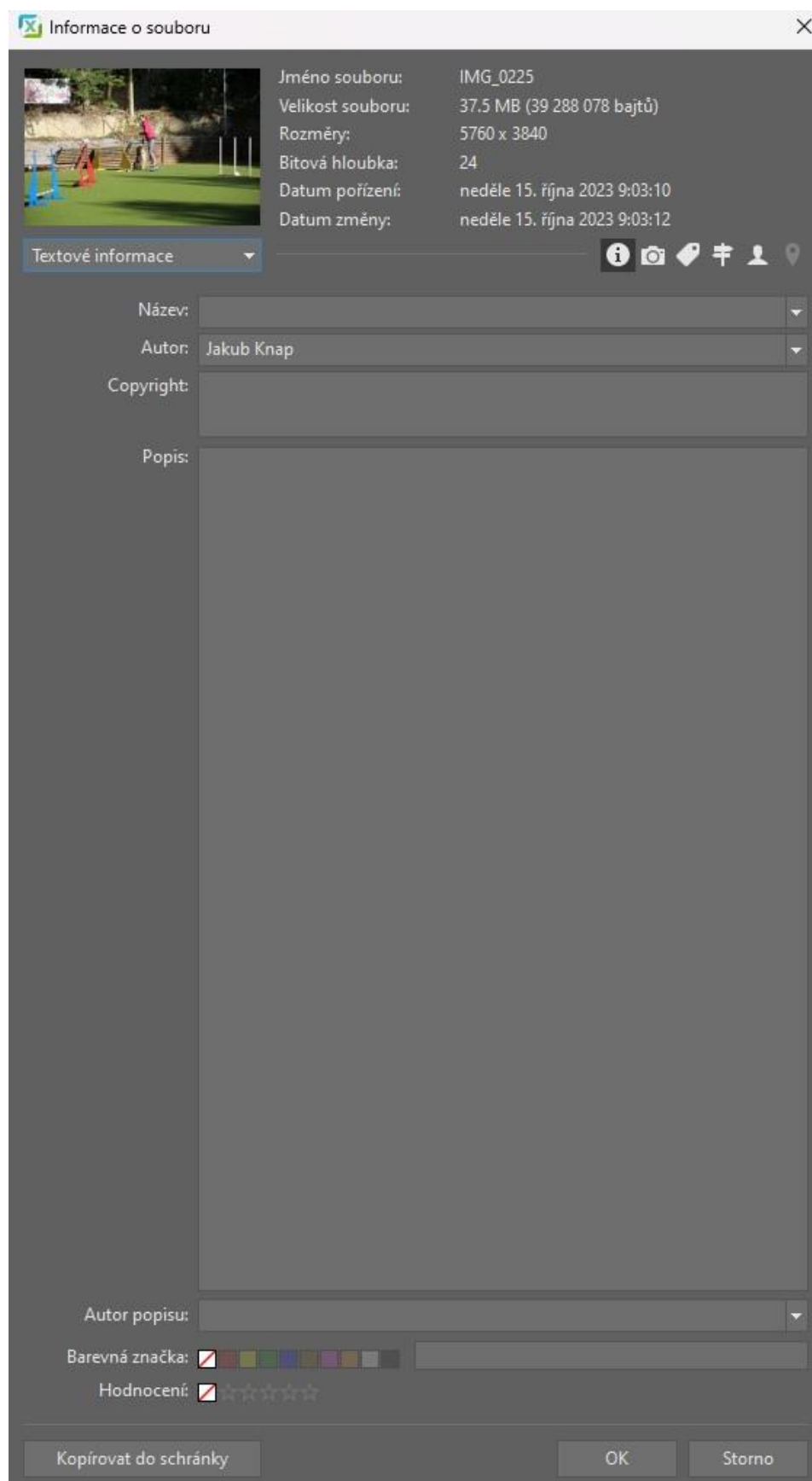
Datum změny: neděle 15. října 2023 9:03:12

Fotografické informace ▾

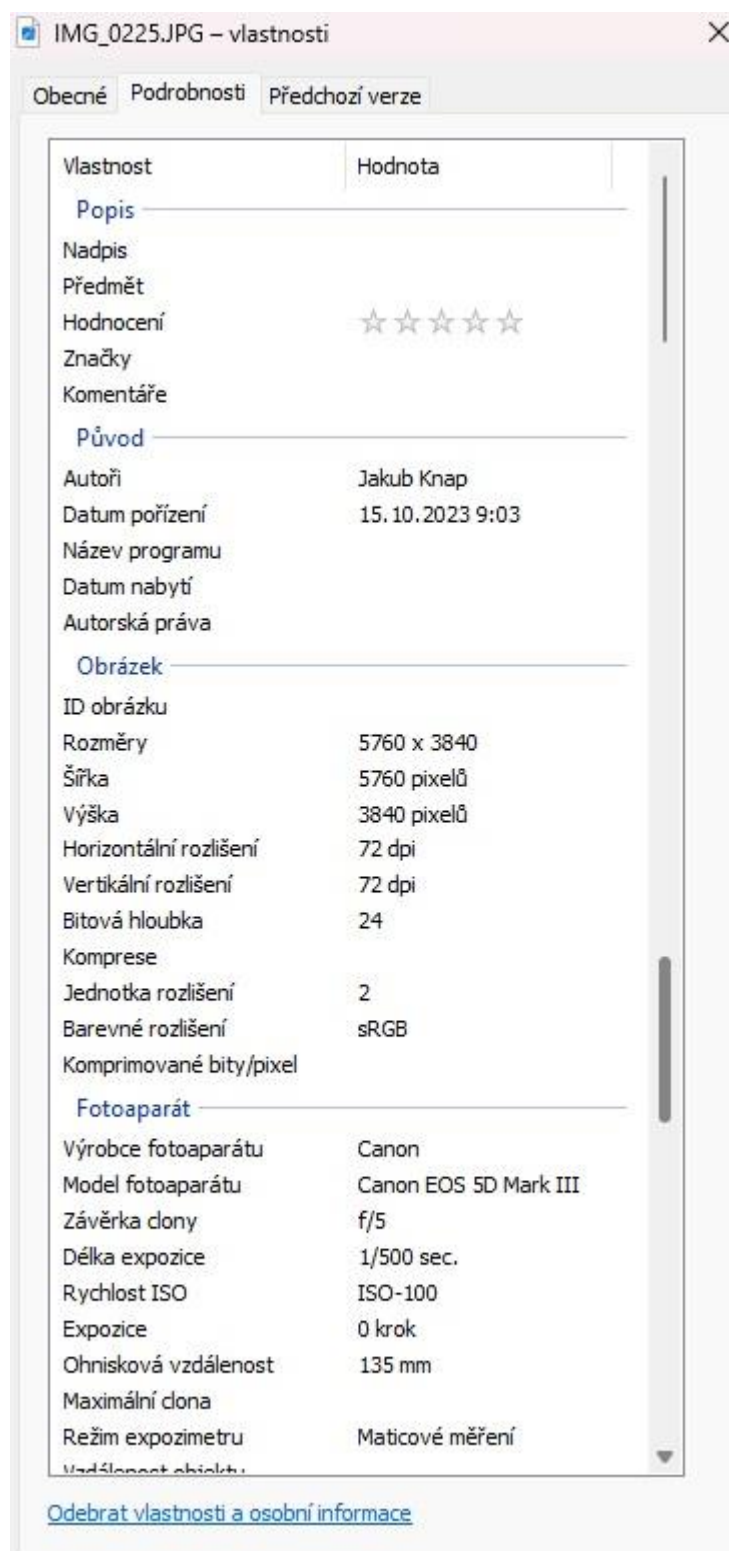
 ⓘ 📷 🗑️ 🏠 👤 📍

Název značky	Data	
Informace o čase		
Vytvořeno	neděle 15. října 2023 9:03:10	✎
Digitalizováno	neděle 15. října 2023 9:03:10	✎
Změněno	neděle 15. října 2023 9:03:10	
Základní EXIF		
Citlivost	100	✎
Doba expozice	1/500 s	✎
Clona	5.0	✎
Ohnisková vzdálenost	135 mm	✎
Ohnisková vzdálenost (EQ35mm)	135 mm	✎
Objektiv	EF70-300mm f/4-5.6 IS USM	
Kompensace expozice	0	
Blesk	Ne	
Detailní EXIF		
Výrobce fotoaparátu	Canon	✎
Model fotoaparátu	Canon EOS 5D Mark III	✎
Firmware fotoaparátu	Firmware Version 1.2.1	
Sériové číslo fotoaparátu	083024014712	
Sériové číslo objektivu	0000149291	
Program expozice	S preferencí času	
Režim expozice	Automatická expozice	
Režim měření expozice	Vzorek	
Typ snímané scény	Běžná	
Vyrovnání bílé	Automatické	
Blesk podrobně	Ne, Vypnutý blesk	
Transformace	Normální	
Kontrast	Normální	
Sytost	Normální	
Režim vzdálenosti	Vzdálené	
Ostatní informace		
Barevný prostor	sRGB	
Uživatelské zpracování	Normální	
Barevný model	YCbCR	
Kompresce	JPEG	
Rozlišení	72	
Horizontální rozlišení senzoru	3942.51	
Vertikální rozlišení senzoru	3950.62	
Jednotka rozlišení senzoru	in	
Digitální podpis	Ne	

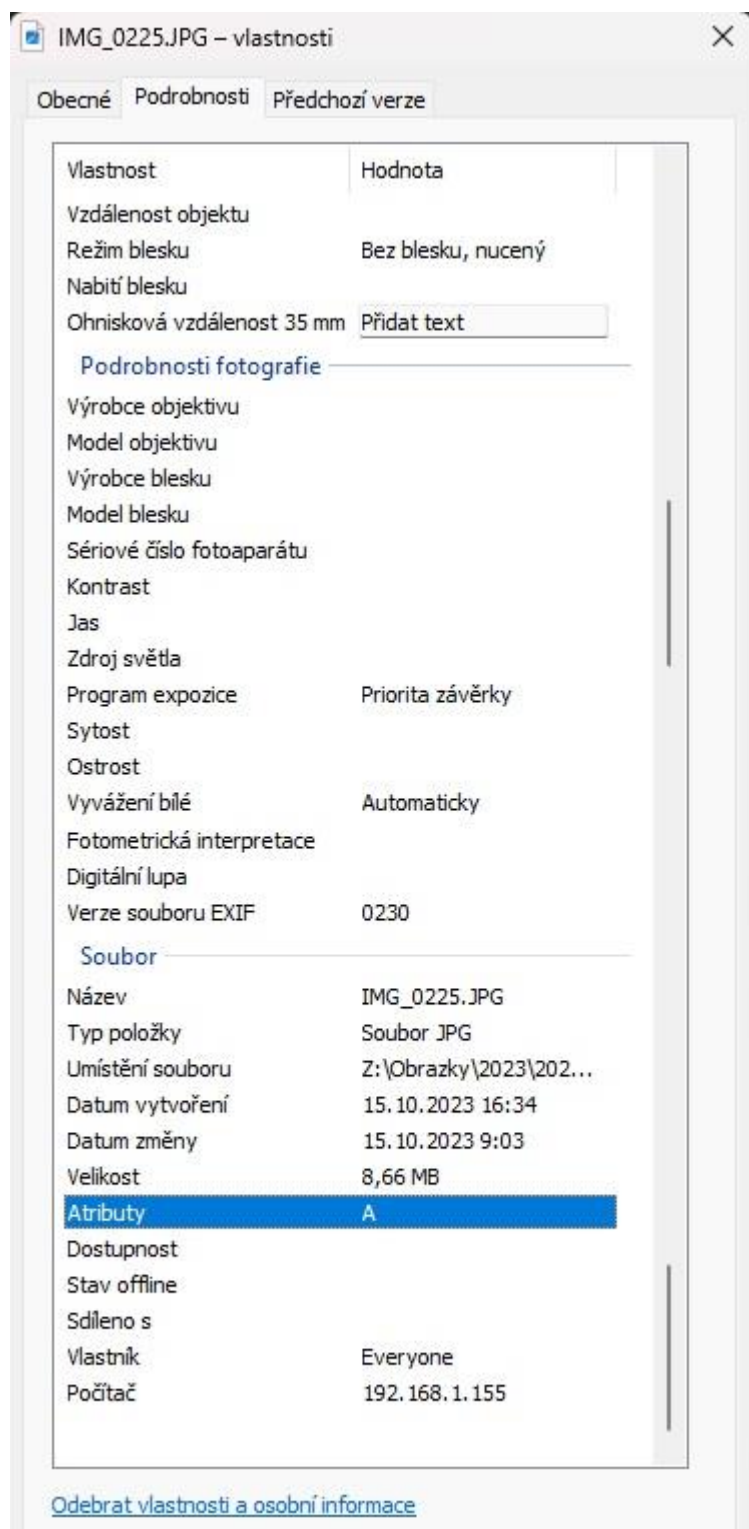
Obrázek č. 5 – Náhled EXIF dat Zoner Photo Studio X



Obrázek 6 – Vlastnosti obrázku dostupné standardně v Microsoft Windows



Obrázek 7 – Vlastnosti obrázku dostupné standardně v Microsoft Windows



Seznam příloh

Příloha č. 1 – Vishing	115
Příloha č. 2 – IP adresy privátních sítí.....	116
Příloha č. 3 – IP adresy pro speciální účely	116
Příloha č. 4 – Logovací soubor z NAS Asustor	118
Příloha č. 5 – Texty vytvořené ChatGPT 3.5.....	120
Příloha č. 6 – Vzor dotazníkového šetření	123
Příloha č. 7 - Systematika školení	samostatně v kapse
Příloha č. 8 - Systematika skript.....	samostatně v kapse

Typy podvodných telefonátů?

Zaměstnanec banky

Podvodník se vydává nejčastěji za bankovního úředníka, který vám volá z pověření bankovní instituce a předstírá, že je součástí technické podpory pro kontrolu platebních operací. Důvodem hovoru může být naléhavá informace, že vaše karta byla zneužita. Následně vám nabízí okamžité řešení domnělého problému – pomůže vám se zablokováním karty. Vyžaduje po vás číslo karty, datum platnosti a CVC/CVV kód, s nimiž za vás provede na pozadí bankovní operaci a po vás vyžaduje potvrzovací kód pro uskutečnění převodu. To vše pod pláštěm nutnosti ověření vaší bankovní identity. Útočník zůstává na lince a působí velmi důvěryhodně, dokud nedosáhne svého cíle – získání vašich finančních prostředků.

Investiční makléř

Druhým častým případem podvodného scénáře je investiční makléř, který vám nabízí výhodnou investici do akcií významné firmy. Útočník se vydává za zaměstnance této firmy nebo za makléře renomované investiční společnosti či banky. Pro uskutečnění investice po vás vyžaduje přihlášení do internetového bankovníctví a převod peněz na jeho účet. Ochotně vám nabízí pomoc s využitím nástrojů pro vzdálenou správu (např. TeamViewer, AnyDesk aj.). Pokud se nachytáte, získá útočník nejen kontrolu nad vaším bankovním účtem, ale i nad vaším počítačem, kam může nainstalovat třeba malware.

Příloha č. 2 – IP adresy privátních sítí

Třída	Rozsah adres	Počet sítí
Třída A	10.0.0.0 ~ 10.255.255.255	1 Třída A
Třída B	172.16.0.0 ~ 172.31.255.255	16 Třída C
Třída C	192.168.0.0 ~ 192.168.255.255	256 Třída C

Příloha č. 3 – IP adresy pro speciální účely

Blok adresy	Rozsah adres	Rozsah	Popis
0.0.0.0/8	0.0.0.0–0.255.255.255	Software	Aktuální síť (platí pouze jako zdrojová adresa).
10.0.0.0/8	10.0.0.0–10.255.255.255	Soukromá síť	Používá se pro místní komunikaci v soukromé síti.
100.64.0.0/10	100.64.0.0–100.127.255.255	Soukromá síť	Sdílený adresový prostor pro komunikaci mezi poskytovatelem služeb a jeho předplatiteli při použití NAT na úrovni operátora.
127.0.0.0/8	127.0.0.0–127.255.255.255	Hostitel	Používá se pro adresy zpětného smyčky místnímu hostiteli.
169.254.0.0/16	169.254.0.0–169.254.255.255	Subnet	Používá se pro lokální adresy spojení mezi dvěma hostiteli na jednom spoji, pokud není IP adresa specifikována jinak, jako by to bylo normálně načteno ze serveru DHCP.
172.16.0.0/12	172.16.0.0–172.31.255.255	Soukromá síť	Používá se pro místní komunikaci v soukromé síti.
192.0.0.0/24	192.0.0.0–192.0.0.255	Soukromá síť	Přiřazení protokolu IETF.
192.0.2.0/24	192.0.2.0–192.0.2.255	Dokumentace	Přiřazeno jako TEST-NET-1, dokumentace a příklady.

192.88.99.0/24	192.88.99.0– 192.88.99.255	Internet	Rezervováno. Relé IPv6 na IPv4 (zahrnuto IPv6 adresový blok 2002 :: / 16).
192.168.0.0/16	192.168.0.0– 192.168.255.255	Soukromá síť	Používá se pro místní komunikaci v soukromé síti.
198.18.0.0/15	198.18.0.0– 198.19.255.255	Soukromá síť	Používá se pro testování testů mezi sítěmi mezi dvěma samostatnými podsítěmi.
198.51.100.0/24	198.51.100.0– 198.51.100.255	Dokumentace	Přiřazeno jako TEST-NET-2, dokumentace a příklady.
203.0.113.0/24	203.0.113.0– 203.0.113.255	Dokumentace	Přiřazeno jako TEST-NET-3, dokumentace a příklady.
224.0.0.0/4	224.0.0.0– 239.255.255.255	Internet	Používá se pro vícesměrové vysílání IP. (Bývalá síť třídy D).
240.0.0.0/4	240.0.0.0– 255.255.255.254	Internet	Vyhrazeno pro budoucí použití. (Bývalá síť třídy E).
255.255.255.255/32	255.255.255.255	Subnet	Vyhrazeno pro cílovou adresu „omezeného vysílání“.

Příloha č. 4 – Logovací soubor z NAS Asustor

"Type","Time","User","Event"
"INFO","02/03/2024 PM 04:51:43","SYSTEM","[System] \"ADM\" login failure from IP \"192.168.1.149\" detected."
"INFO","02/03/2024 PM 12:30:07","SYSTEM","[Regional Options] Successfully synced from the NTP server."
"INFO","02/03/2024 AM 01:01:00","SYSTEM","[Firmware Update] firmware has already been updated to the latest version."
"INFO","02/03/2024 AM 12:04:58","SYSTEM","[Background Processing -> Schedule] Storage usage calculating is complete."
"INFO","02/03/2024 AM 12:00:00","SYSTEM","[Background Processing -> Schedule] Started to calculate storage usage."
"INFO","02/02/2024 PM 07:35:48","SYSTEM","[System] \"samba\" login failure from IP \"192.168.1.149\" detected."
"INFO","02/02/2024 PM 12:30:07","SYSTEM","[Regional Options] Successfully synced from the NTP server."
"INFO","02/02/2024 AM 11:55:14","SYSTEM","[System] \"samba\" login failure from IP \"192.168.1.149\" detected."
"INFO","02/02/2024 AM 01:01:04","SYSTEM","[Firmware Update] firmware has already been updated to the latest version."
"INFO","02/02/2024 AM 12:04:23","SYSTEM","[Background Processing -> Schedule] Storage usage calculating is complete."
"INFO","02/02/2024 AM 12:00:00","SYSTEM","[Background Processing -> Schedule] Started to calculate storage usage."
"INFO","02/01/2024 PM 12:30:09","SYSTEM","[Regional Options] Successfully synced from the NTP server."
"INFO","02/01/2024 AM 10:01:03","SYSTEM","[System] \"samba\" login failure from IP \"192.168.1.149\" detected."
"INFO","02/01/2024 AM 01:01:03","SYSTEM","[Firmware Update] firmware has already been updated to the latest version."
"INFO","02/01/2024 AM 12:03:55","SYSTEM","[Background Processing -> Schedule] Storage usage calculating is complete."
"INFO","02/01/2024 AM 12:00:00","SYSTEM","[Background Processing -> Schedule] Started to calculate storage usage."
"INFO","01/31/2024 PM 12:30:09","SYSTEM","[Regional Options] Successfully synced from the NTP server."
"INFO","01/31/2024 AM 08:15:52","SYSTEM","[System] \"ADM\" login failure from IP \"213.195.252.143\" detected."
"INFO","01/31/2024 AM 01:01:00","SYSTEM","[Firmware Update] firmware has already been updated to the latest version."
"INFO","01/27/2024 PM 08:04:25","SYSTEM","[System] System starts."
"INFO","01/27/2024 PM 08:04:01","SYSTEM","[Regional Options] Successfully synced from the NTP server."
"INFO","01/27/2024 PM 08:03:47","SYSTEM","[DDNS] NAS WAN IP has changed to 212.79.110.208/. WAN IP information updated to 'AS1102T-E83C'.
"INFO","01/27/2024 PM 08:03:25","SYSTEM","[Regional Options] Successfully synced from the NTP server."
"INFO","01/27/2024 PM 08:03:18","SYSTEM","[Background Processing -> Schedule] Started to calculate storage usage."
"INFO","01/27/2024 PM 08:01:32","SYSTEM","[System] System is restarting."

"INFO","01/27/2024 PM 07:57:56","SYSTEM","[System] "ADM" login failure from IP "192.168.1.149" detected."

"INFO","01/27/2024 PM 12:30:07","SYSTEM","[Regional Options] Successfully synced from the NTP server."

"INFO","01/27/2024 AM 01:01:01","SYSTEM","[Firmware Update] firmware has already been updated to the latest version."

"INFO","01/23/2024 AM 01:01:23","SYSTEM","[Firmware Update] A new version (4.2.6.RPI1) of the firmware image has been downloaded."

"INFO","01/23/2024 AM 12:05:44","SYSTEM","[Background Processing -> Schedule] Storage usage calculating is complete."

"INFO","01/23/2024 AM 12:00:00","SYSTEM","[Background Processing -> Schedule] Started to calculate storage usage."

"INFO","01/21/2024 PM 04:35:02","SYSTEM","[System] "samba" login failure from IP "192.168.1.149" detected."

"INFO","01/21/2024 PM 04:35:02","SYSTEM","[System] "samba" login failure from IP "192.168.1.149" detected."

"INFO","01/21/2024 PM 04:35:02","SYSTEM","[System] "samba" login failure from IP "192.168.1.149" detected."

"INFO","01/21/2024 PM 04:34:53","SYSTEM","[System] "samba" login failure from IP "192.168.1.149" detected."

"INFO","01/21/2024 PM 12:30:13","SYSTEM","[Regional Options] Successfully synced from the NTP server."

"INFO","01/21/2024 AM 01:01:04","SYSTEM","[Firmware Update] firmware has already been updated to the latest version."

"INFO","01/21/2024 AM 12:04:07","SYSTEM","[Background Processing -> Schedule] Storage usage calculating is complete."

"INFO","01/21/2024 AM 12:00:00","SYSTEM","[Background Processing -> Schedule] Started to calculate storage usage."

"WARNING","01/07/2024 PM 05:04:16","SYSTEM","[System] The NAS did not shut down properly last time."

"INFO","01/07/2024 PM 05:04:16","SYSTEM","[System] System starts."

"INFO","01/07/2024 PM 05:04:13","SYSTEM","[Network] LAN1 was plugged in."

"INFO","01/07/2024 PM 05:04:07","SYSTEM","[Network] LAN1 was unplugged."

"INFO","01/07/2024 PM 05:04:06","SYSTEM","[Network] LAN1 was unplugged."

"INFO","01/07/2024 PM 05:03:54","SYSTEM","[Regional Options] Failed to sync from the NTP server."

"INFO","01/07/2024 PM 05:03:49","SYSTEM","[DDNS] Failed to apply 'AS1102T-E83C' IP. (Temporary network error (DNS))"

"INFO","01/07/2024 PM 05:03:30","SYSTEM","[Background Processing -> Schedule] Started to calculate storage usage."

"INFO","01/07/2024 PM 05:03:24","SYSTEM","[Regional Options] Successfully synced from the NTP server."

Příloha č. 5 – Texty vytvořené ChatGPT 3.5

You

Napiš novinový článek o policistovi, jenž zachránil nadnárodní společnosti data před hackerským útokem.

ChatGPT

Hrdinský Policejní Zásah: Policista Zachránil Nadnárodní Společnosti Před Hackerským Útokem

Praha, 6. března 2024

V nejnovějším příkladu statečnosti a odbornosti se jeden z českých policistů stal hrdinou, když úspěšně zmařil pokus hackerské skupiny o napadení nadnárodních společností. Tento mimořádný policejní zásah pomohl chránit citlivá data a informace, které jsou klíčové pro fungování firem na globální úrovni.

Příběh začal ve středu večer, když kybernetičtí zločinci zaútočili na systémy několika nadnárodních společností s cílem získat citlivé informace a data. Ovšem díky rychlé a precizní reakci policisty Jana Nováka, který je členem kybernetického týmu české policie, byl útok úspěšně odvrácen.

Policista Novák, který má za sebou bohaté zkušenosti v oblasti kybernetické bezpečnosti, reagoval na varování systému o neobvyklé aktivitě okamžitě. Během několika minut se dostal na místo činu a začal analyzovat útok. Jeho rychlá reakce a odborné dovednosti byly klíčové pro úspěšné odvrácení hrozby.

Při tiskové konferenci dnes ráno uvedl policejní mluvčí Markéta Novotná: "Jsme nesmírně hrdí na práci policisty Nováka a celého kybernetického týmu. Jejich profesionalita a odhodlání jsou příkladem pro všechny. Díky jejich úsilí byla ochráněna citlivá data a bylo zabráněno potenciálnímu ekonomickému poškození."

Nadnárodní společnosti, které byly terčem útoku, vyjádřily svou vděčnost české policii za rychlou a efektivní pomoc. Ředitel společnosti GlobalTech Solutions uvedl: "Děkujeme policistovi Novákovi a jeho týmu za jejich promptní reakci a ochranu našich firemních dat. Jejich práce má klíčový význam nejen pro nás, ale i pro další společnosti, které jsou vystaveny podobným kybernetickým hrozbám."

Policista Jan Novák zůstává skromný a poděkoval svým kolegům za spolupráci. "Je to týmová práce a věřím, že jsme udělali svou práci dobře. Ale nezapomínejme, že kybernetická bezpečnost je stále výzvou, a je třeba, abychom zůstali ostražití," uvedl Novák na konferenci.

Tento příběh zdůrazňuje důležitost práce kybernetických týmů a policie v ochraně digitálního prostoru. Výjimečný výkon policisty Nováka ukazuje, že i v době stále sofistikovanějších kybernetických hrozeb mohou jednotlivci a týmy s odpovídajícími schopnostmi vytvořit silný štít pro ochranu citlivých dat a informací.



You

Napiš novinový článek o policistovi, jenž zachránil nadnárodní společnosti data před hackerským útokem.

Vstupní data:

policista - kpt. Mgr. Luboš Veselý

poškozená společnost - BlahBla s.r.o.

útočící skupina - HackeR

potencionální způsobená škoda - 1000000Eur

doba útoku - 3 dny

doba prověřování a vyšetřování 8 týdnů

ChatGPT

Hrdinný Policista Zachraňuje Nadnárodní Společnost Před Hackerským Útokem: Kpt. Mgr. Luboš Veselý v Akci

Datum: 6. března 2024

Ve vzrušujícím příběhu o boji proti kybernetickým zločincům vyniká kpt. Mgr. Luboš Veselý, který nedávno zachránil nadnárodní společnost BlahBla s.r.o. před ničivým hackerským útokem.

Skupina známá pod názvem "HackeR" se pokusila napadnout firemní systémy, ale díky statečnému a rychlému jednání policisty byla potenciální škoda v hodnotě 1 milionu eur zamezena.

Útok, který trval tři dlouhé dny, ohrožoval citlivá firemní data společnosti BlahBla s.r.o., jež má nadnárodní působnost. Hackeři chtěli nejen způsobit finanční ztrátu, ale také narušit důvěrnost a integritu firemních informací. Kpt. Mgr. Luboš Veselý však ukázal, že policie je připravena čelit moderním kybernetickým hrozbám.

Po nahlášení útoku rychle reagoval policejní tým pod vedením kapitána Veselého. Během tří denního úsilí se podařilo identifikovat útočníky, sledovat jejich pohyb a získat klíčové informace o jejich plánech. Veselý a jeho tým pracovali v náročných podmínkách, abychom ochránili společnost před katastrofou.

Po odvrácení okamžité hrozby se věnoval kpt. Veselý i následnému prověřování, aby zajistil, že skupina "HacKer" nebude schopna znovu napadnout. Doba prověřování a vyšetřování trvala neuvěřitelných osm týdnů. Během tohoto období byla analyzována každá stopa, každý kód a každý komunikační prvek, který mohl být spojen s hackery.

Výsledkem policejního úsilí bylo nejen identifikování všech členů hackerské skupiny, ale také zabezpečení důkazů, které umožní postavit pachatele před soud. Kpt. Mgr. Luboš Veselý vyzdvihl týmovou spolupráci a podporu ze strany technických expertů, kteří hráli klíčovou roli v úspěchu operace.

Nadnárodní společnost BlahBla s.r.o. vyjádřila vděk kpt. Veselému a jeho týmu za rychlou a efektivní ochranu firemních dat. Tento případ opět zdůraznil nutnost spolupráce mezi soukromým sektorem a veřejnou bezpečností v boji proti kybernetickým hrozbám.

Kpt. Mgr. Luboš Veselý se stal hrdinou, který dokázal, že statečnost a odhodlání mohou překonat moderní výzvy digitálního věku.



Příloha č. 6 – Vzor dotazníkového šetření

Dotazníkové šetření k diplomové práci

Tento formulář je vytvářen za účelem vypracování diplomové práce zpracovatele, jejímž tématem je Koncepce policejního vzdělávání v oblasti kybernetické trestné činnosti a zvýšení počítačové gramotnosti policistů v Plzeňském kraji. Na základě zjištěných odpovědí se pisatel pokusí navrhnout koncepci vzdělávání přímo pro policisty Plzeňského kraje, proto bych Vás požádal o jeho nepřeposílání policistům na jiných krajských ředitelství či celorepublikových útvarech, v rámci Krajského ředitelství policie Plzeňského kraje je možné jej přeposílat. Rád bych vás požádal o nevyplňování formuláře vícekrát z důvodu validity získaných informací.

Tento formulář je zcela anonymní.

K vyplnění formuláře budete potřebovat **méně než 5 minut**.

Předem děkuji všem za jeho úplné a poctivé vyplnění.

Bc. Jakub Knap

Jaké je Vaše pohlaví? *

- Muž
- Žena
- Jiná...

Jaký je Váš věk? *

- 18-21 let
- 22-25 let
- 26-30 let (do věku 30 let a 6 měsíců přesně)
- 30-40 let
- 41-50 let
- více jak 50 let

Jaké je Vaše nejvyšší dosažené vzdělání *

- Základní vzdělání
- Střední odborné vzdělání s výučním listem
- Úplné střední odborné vzdělání s maturitou
- Vyšší odborné vzdělání
- Vysokoškolské vzdělání

Na jakém článku policie sloužíte? *

- Vnější služba
- Služba kriminální policie a vyšetřování
- Jiná...

Jaká je Vaše hlavní náplň práce *

- Hlídková služba (OOP)
- Obchůzková služba (OOP)
- Dozorčí (OOP)
- Zpracovatel (OOP)
- Operativa (SKPV)
- Vyšetřovatel (SKPV)
- Technik (SKPV)
- OKTE (SKPV)
- Vedoucí či zástupce vedoucího
- Jiná...

Jak dlouho jste ve služebním poměru? *

- 1-3 roky (nemám splněnu služební zkoušku)
- 4-5 let
- 6-10 let
- 11-15 let
- 15-20 let
- více jak 20 let

Jak hodnotíte znalosti předávané v rámci základních odborných příprav (dále jen ZOP) týkající se kybernetické trestné činnosti? *

- Zcela dostatečné
- Spíše dostatečné
- Spíše nedostatečné
- Zcela nedostatečné
- Žádné takové znalosti nebyly předmětem ZOP

Jak hodnotíte znalosti předávané v rámci ZOP týkající se počítačové gramotnosti (schopnost používat účelově a účinně počítač a jinou výpočetní techniku)? *

- Zcela dostatečné
- Spíše dostatečné
- Spíše nedostatečné
- Zcela nedostatečné
- Žádné takové znalosti nebyly předmětem ZOP

Kolik školení po ZOP týkajících se kybernetické trestné činnosti či počítačové gramotnosti jste díky PČR absolvovali? *

- 0
- 1-2
- 3-4
- 5 a více

Jak hodnotíte znalosti předávané v rámci školení týkajících se kybernetické trestné činnosti? *

- Zcela dostatečné
- Spíše dostatečné
- Spíše nedostatečné
- Zcela nedostatečné
- Žádné takové znalosti nebyly předmětem specializačního kurzu

Jaké zaměření uvedená školení týkající se kybernetické trestné činnosti měla? *

- Trestně-právní
- Technického zaměření
- Na žádném školení jsem nebyl
- Jiná...

Jak hodnotíte znalosti předávané v rámci školení týkající se počítačové gramotnosti? *

- Zcela dostatečné
- Spíše dostatečné
- Spíše nedostatečné
- Zcela nedostatečné
- Žádné takové znalosti nebyly předmětem specializačního kurzu

Měli jste možnost se v rámci služebního poměru účastnit jakéhokoliv školení týkající se kybernetické trestné činnosti či počítačové gramotnosti? *

- Ano a využil jsem možnost takového školení.
- Ano a nevyužil jsem možnost takového školení.
- Ne.

Jakou formu vzdělávání v uvedené oblasti preferujete? *

- Elearnig
- Webinář
- Prezenční forma
- Samostudium

Vyhovovalo by Vám školení formou řízených modelových situací v oblasti kybernetické trestné činnosti? *

- Ano
- Ne
- Je mi to jedno

Vyhovovalo by Vám školení formou řešení předem připravených úkolů v oblasti počítačové gramotnosti? *

- Ano
- Ne
- Je mi to jedno