VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

KYBERNETICKÁ KRIMINALITA V OBLASTI MAJETKOVÉ TRESTNÉ ČINNOSTI

Autor práce: Lukáš Byrtus, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: kombinovaná
Vedoucí práce: RNDr. Růžena Ferebauerová
Katedra: Katedra právních oborů a bezpečnostních studií

2022

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 6, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Lukáš Byrtus, DiS.

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Kybernetická kriminalita v oblasti majetkové trestné činnosti

Název bakalářské práce v anglickém jazyce: CyberCrime in property crime

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, titul):
RNDr. Růžena Ferebauerová
Datum zadání bakalářské práce (měsíc, rok): listopad 2021

Cíl bakalářské práce:
Hlavním cílem je empirický výzkum pomocí dotazníkového šetření, který má za úkol teritoriálně analyzovat odborné znalosti a připravenost příslušníků pořádkové Policie České republiky na stále vzrůstající hrozbu, kyberkriminalitu.
Vedlejším cílem bakalářské práce je seznámit s vybranými pojmy, projevy a formami kybernetické kriminality v oblasti majetkových trestných činů. Následně je práce zaměřena na vybrané kybernetické útoky orientující se na majetek, jejich odhalování a vyšetřování.

Student: Lukáš Byrtus, DiS.	19.11.2021 *datum*	*podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	19.11.21 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	6.12.2021 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	8.12.2021 *datum*	*podpis*
Pověřený rektor: doc. Ing. Jiří Dušek, Ph.D.	14.12.2021 *datum*	*podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, P.Z. JUDR. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

BYRTUS, L. *Kybernetická kriminalita v oblasti majetkové trestné činnosti*. České Budějovice: Vysoká škola evropských a regionálních studií, 2022. 69 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: Internet, kybernetická kriminalita, kybernetický prostor, kybernetický prostor, kybernetické útoky, policie České republiky, vzdělávání

Bakalářská práce pojednává o relativně novém aspektu „kybernetické kriminalitě“, dříve také označované jako počítačová kriminalita. Práce je rozdělena na dvě části: teoretickou a praktickou. V teoretické části práce je shrnuta historie internetu ve světě, tak v České republice, jsou vysvětleny důležité pojmy, projevy a formy kybernetické kriminality ve vztahu k majetkové trestné činnosti. Dále se zabývá vybranými majetkovými trestními činy z pohledu kybernetické kriminality, jejich odhalování a vyšetřování. Praktická část je zaměřena na kvantitativní výzkum pomocí dotazníkového šetření, který má za cíl analyzovat, jak jsou příslušníci Policie České republiky připraveni a školeni na stále vzrůstající hrozbu, kyberkriminalitu.

ABSTRACT

BYRTUS, L. *CyberCrime in property crime.* České Budějovice: The College of European and Regional Studies, 2022. 69 p. Supervisor: RNDr. Růžena Ferebauerová

Key words: Internet, Cybercrime, Cyberspace, Cyberattacks, Police of the Czech Republic, education

This bachelor thesis discussing a relatively new topic of "cybercrime" that used to be called computer criminality. This paper is divided into two sections: theoretical and practical. In the theoretical part is discussed the history of the internet in the world as well as in the Czech Republic. Furthermore, there are discussed key terms, continuing into signs and forms of cybercrime, more specifically in relation to a property crime. This is followed up by chosen property crimes considering the cybercrime angle, their detection, and investigation. The practical part is focused on quantitative research using questionnaires that result in an analysis of the level of preparation for increasing cybernetic crimes of police members in the Czech republic.

Obsah

Úvod

Bakalářská práce pojednává o více než aktuálním stále vzrůstajícímu problému, tzv. kybernetické kriminalitě. Hlavní problematika práce, tedy praktická část, analyzuje a vyhodnocuje, jak jsou příslušníci Policie České republiky na úrovni základních organizačních článků pořádkové policie připraveni a školení v oblasti kybernetické kriminality a s ní spojenými procesními úkony. Hlavním důvodem, proč si autor toto téma vybral je, že za svoji praxi u Policie České republiky se doposud nesetkal se vzděláváním příslušníků obvodních odděleních s výše uvedenou problematikou. Na základě této zkušenosti byl prostřednictvím dotazníkového šetření proveden teritoriální průzkum, který vyhodnocuje míru účasti na školeních, připravenost a odbornost příslušníků Policie České republiky v popisované problematice. Cílem práce je potvrdit či vyvrátit předem stanovené hypotézy. Na základě analýzy dotazníkového šetření bylo formulováno doporučení, které by mohlo být využito v praxi k efektivnější vyšetřování kybernetické kriminality.

V teoretické části práce je kladen důraz na historii internetu ve světě a v České republice. Je definován a vymezen pojem kybernetická kriminalita a jsou rozebrány další důležité pojmy, které s ní souvisí. Je popsán legislativní rámec majetkové kybernetické kriminality a jsou definovány projevy kybernetické kriminality v oblasti majetkové sféry, jejich odhalování a vyšetřování. Teoretická část bakalářské práce se opírá o odbornou českou i zahraniční literaturu.

1 Cíl a metodika bakalářské práce

Hlavním cílem je empirický výzkum prováděný dotazníkovým šetřením, který má za úkol teritoriálně analyzovat odborné znalosti a připravenost příslušníků pořádkové Policie České republiky na stále vzrůstající hrozbu kyberkriminality.

Cílovou skupinou pro kvalitativní metodu bakalářské práce jsou příslušníci pořádkové policie zařazení na základních organizačních článcích policie, tedy policisté na obvodních odděleních územních odborů Praha venkov – Východ a Nymburk. Dotazníkové šetření bylo určeno pro 125 policistů zařazených na obvodních odděleních zmíněných územních odborů.

Na základě sběru dat práce analyzuje provedené dotazníkové šetření, které následně zhodnocuje a navrhuje doporučení pro zlepšení situace. V rámci dotazníkového šetření byly pro práci formulovány tři hypotézy takto:

H1: *Policisté České republiky na základních organizačních článcích pořádkové policie nejsou dostatečně školení v oblasti kybernetické kriminality.*

H2: *Policisté České republiky na základních organizačních článcích pořádkové policie nejeví zájem o rozvíjení znalostí v oblasti kybernetické kriminality.*

H3: *Policisté České republiky na základních organizačních článcích pořádkové policie neradi vyšetřují případy spojené s kybernetickou kriminalitou.*

Vedlejším cílem bakalářské práce je definovat vybrané pojmy, projevy a formy kybernetické kriminality v oblasti majetkových trestných činů. Následně je práce zaměřena na vybrané kybernetické útoky cílené na majetek, jejich odhalování a vyšetřování.

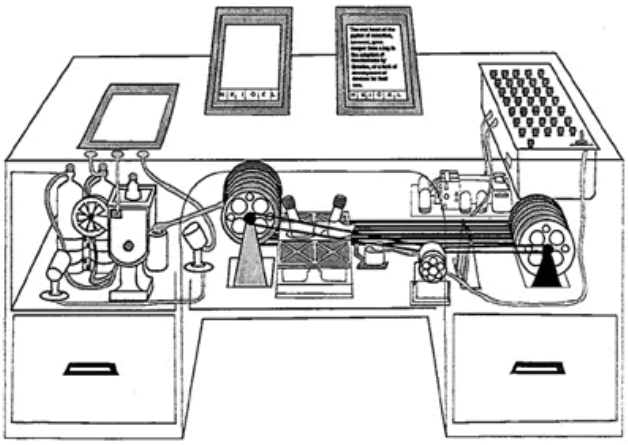
2 Historie internetu

Od vynalezení první počítačové sítě, která je obecně dobře známá a využívaná všemi věkovými skupinami populace po takřka celém světě, uplynulo celkem 53 let. Lze konstatovat, že za tuto dobu počítačová síť prodělala výrazný progres a je odborníky neustále zdokonalována. V jednotlivých podkapitolách jsou popsány počátky internetu ve světě a v České republice.

2.1 Počátky internetu ve světě

Prvopočátky internetu jsou spojeny se vznikem počítačů, tedy s první polovinou dvacátého století, konkrétně rokem 1945, kdy v červnovém vydání amerického časopisu The Athlantic Monthly zveřejnil vědec Vannevar Bush článek základních kamenů informační vědy. Ve svém článku definoval pojem Memex, což bylo zařízení pro zvýšení lidské paměti. Základní funkcí Memexu mělo být ukládání a zpětné vyhledávání informací. Toto zařízení bylo složeno z několika obrazovek, klávesnice a dalších potřebných součástek pro ovládání. Zařízení Memex zajišťovalo uchovávání importovaných informací pomocí mikrofilmového uložiště. Mělo sloužit zejména k ukládání vlastních poznatků a sdělení, což připomíná funkci dnešního osobního počítače. Zařízení Memex však nikdy nebylo zrealizováno.[1]

Obrázek 1 - Ilustrace schématu zařízení Memex[2]



[1] Internet a jeho služby: *Historie internetu.* [online]. [cit. 2022-01-11]. Dostupné z: http://ijs.8u.cz/index.php/internet/historie-internetu

[2] Dostupné z: https://wikisofia.cz/wiki/Memex

První zásadnější moment, který odstartoval výzkum počítačových a síťových komunikací, datujeme k 50. létům minulého století, k období tzv. Studené války – konfliktu mezi Sovětským svazem a Spojenými státy. Obě velmoci se připravovaly na případnou jadernou válku, ve které by byly oběti počítány ve stovkách miliónů. Na začátku zmíněného desetiletí doporučovali poradci tehdejšího amerického prezidenta Harryho Trumana, aby se Spojené státy pustily do masivního zbrojení, s cílem úspěšně čelit komunistické hrozbě. To mělo zabezpečit rychlejší budování politické, ekonomické a vojenské síly. Toto nelehké období bylo frustrující pro obě strany, jelikož jakékoli špatné rozhodnutí mohlo nést fatální následky. Letectvo Spojených států amerických začalo v polovině 60. let používat k odpalování jaderných střel pevné pohonné hmoty, čímž snížilo dobu jejich spuštění z 8 hodin na několik sekund. V důsledku toho byly atomové rakety k dispozici k neprodlenému použití a jejich zážeh trval mrknutí oka. Již v roce 1950 byl prezident Spojených států, Harry Truman, varován, že je potřeba bránit a udržovat komunikační linky v případě jaderné války. Přesto dalších 10 let neměl nikdo ponětí, jak zabezpečit komunikaci velení a řízení v případě, že na zem začnou padat atomové bomby. Jaderná detonace v ionosféře by ochromila FM rádio komunikaci na celé hodiny a počet jaderných útoků by mohl vyřadit vysoce centralizovanou Národní telefonní síť AT&T.[3]

RAND, prestižní americká výzkumná instituce zabývající se hledáním řešení důležitých společenských problémů, v čele s výzkumníkem jménem Paulem Baranem, dostala za úkol zlepšit komunikační sít po celých Spojených státech amerických, a odvrátit tak válku. Baran se obával, že jedna náhodně vystřelená zbraň ze strany kterékoli velmoci, spustí nezastavitelnou nukleární pohromu. Z tohoto důvodu hledal způsob, jak komunikovat i v takovémto krajním scénáři se svými údernými jadernými jednotkami, které byly takticky rozptýlené po celém území Ameriky. Navrhl radikální změnu národní komunikační sítě, tím, že jí situoval z centra směrem ke kontrolním bodům, kde se dále rozvětvovaly. Toto se dalo přirovnat k paprskovému designu. V roce 1960 však Baran tvrdil, že takto strukturovaná komunikační síť je neudržitelná, a to zejména z důvodu věku balistických raket. Alternativou, kterou proto vyvinul byla odstředivá decentralizovaná distribuovaná síť, která neměla zranitelný centrální bod. Tento model

[3] RYAN, J. *A HISTORY OF THE INTERNET AND THE DIGITAL FUTURE*. 1. papírové vyd. 2013. London. 13 s. ISBN 978-1-78023-112-9

poskytl spolehlivé velení a řízení jaderných sil, a to i v případě, že by nepřátelské útoky poškodily komunikační sítě.[4]

Na základě výzkumu RAND přinesl do této problematiky revoluční řešení, a to i proto, že definoval hlavní pilíře internetu. Paul Baran navrhl kombinaci dvou od sebe izolovaných technologií počítače a komunikace. Když letectvo Spojených států amerických chtělo jeho koncept otestovat, tvrdě narazilo u tehdejšího monopolu AT&T, který užíval ke komunikacím analogovou síť a v digitální přístup popisovaný v Baranově konceptu nevěřilo. Jeho realizaci odložilo, a to i přesto, že předpokládané náklady digitální sítě byly v roce 1964 vyčísleny na 60 milionů dolarů, oproti 2 miliardám dolarů ročně za analogový systém. [5]

Spojené státy americké a Sovětský svaz v době studené války vedli tzv. horkou válku v oblasti technologií a výzkumu. Koncem roku 1957 se Američanům zdálo, že v těchto oblastech Sověti zvítězili, a to zejména tím, že dne 26. srpna 1957 jako první na světě zahájili úspěšný test mezikontinentální balistické střely rakety Vostok R-7. O dva měsíce později, 4. října 1957, vypustili první umělou družici obíhající Zemi, sovětského Sputnika I. Vytoužený úspěch Sovětského svazu měl diametrálně odlišný dopad na Spojené státy, které najednou zaostávaly ve vývoji kosmických technologií, jež měly využití především ve vojenství. Spojené státy si tuto hrozbu začaly uvědomovat a okamžitě jednaly. 07. února 1958 založilo Ministerstvo obrany Spojených států agenturu s názvem Advanced Research Projects Agency (dále jen „ARPA“), která primárně podporovala výzkumné projekty vyvíjející nové technologie. Dalším úkolem agentury bylo zajistit, aby armádní síť počítačů zůstala v provozu i v případě, že by její nedílná část byla vyřazena z provozu. Výsledkem těchto snah bylo vytvoření počítačové sítě bez centrálního uzlu. V době, kdy ARPA začala pracovat na networkingu, měl úřad informačních technologií pouze dva zaměstnance spravující rozpočet 16 milionů dolarů za rok.[6]

Průkopník informačních technologií, americký sociolog a filozof Theodor Holm Nelson, definoval v roce 1963 pojem hypertext. Usiloval o vytvoření počítače, který bude

[4] RYAN, J. *A HISTORY OF THE INTERNET AND THE DIGITAL FUTURE*. 1. papírové vyd. 2013. London. 14–16 s. ISBN 978-1-78023-112-9.
[5] RYAN, J. *A HISTORY OF THE INTERNET AND THE DIGITAL FUTURE*. 1. papírové vyd. 2013. London. 17 s. ISBN 978-1-78023-112-9.
[6] RYAN, J. *A HISTORY OF THE INTERNET AND THE DIGITAL FUTURE*. 1. papírové vyd. 2013. London. 23-24 s. ISBN 978-1-78023-112-9.

snadno dostupný běžným lidem. Nelson zastával heslo, že uživatelské prostředí by mělo být tak jednoduše srozumitelné a intuitivní, že jeho nový uživatel mu porozumí během deseti sekund.[7]

Důležitým datem je 29. října 1969. Právě tento den začal fungovat internet financovaný agenturou ARPA, spadající pod Ministerstvo obrany Spojených států. Tehdy byla spuštěna experimentální síť ARPANET, která však sloužila striktně k vládním a vojenským účelům a propojovala také čtyři americké univerzity. Jednalo se o Kalifornskou univerzitu v Los Angeles, Stanfordovu univerzitu, Kalifornskou univerzitu v Santa Barbaře a univerzitu v Utahu. Historicky první zpráva odeslána prostřednictvím sítě ARPANET byla zaslána ve 22:30 hodin z Kalifornské univerzity v Los Angeles na Stanfordovu univerzitu. Tato zpráva obsahovala jedno klíčové slovo LOGIN, ale software se po odeslání dvou znaků zhroutil a na Stanfordovu univerzitu byla doručena jen část zprávy ve tvaru LO. Na další pokus byla však chyba opravena a komunikace proběhla úspěšně. I po této pozitivní zkušenosti se správnou funkčností však síť ARPANET nelákala firmy ke komerčnímu využití. Nikdo v té době nedokázal odhalit skrytý potenciál sítě k podnikání. Ke dni 5. prosince 1969 byly připojeny k síti ARPANET všechny výše zmíněné univerzity. Hlavním myšlenkou bylo umožnit vzdáleným uživatelům přístup k superpočítačům a využít jejich výkon. Realita byla taková, že si vědci spolupracující na nejrůznějších projektech napříč univerzitami, zasílali soubory a zprávy převážně mezi sebou, síť ARPANET jim umožňovala výrazné zrychlení komunikace. V roce 1971 americký programátor Ray Tomlinson vytvořil a následně implementoval do sítě ARPANET e-mailový program, který je hojně využíván dodnes. Od roku 1971 až do roku 1973 došlo k přejmenování agentury ARPA na agenturu Defense Advanced Research Projects Agency (dále jen DARPA). Síť ARPANET se neustále rozšiřovala a v roce 1973 pronikla podmořskou linkou do Evropy, kde se k ní jako první připojilo z univerzity University College of London Spojené království.[8]

[7] Internet a jeho služby: *Historie Internetu.* [online]. Cit. 2022-01-25]. Dostupné z: https://ijs2.8u.cz/index.php?option=com_content&view=article&id=32&Itemid=134

[8] Internet a jeho služby: *Historie Internetu.* [online]. Cit. 2022-01-25]. Dostupné z: https://ijs2.8u.cz/index.php?option=com_content&view=article&id=32&Itemid=134

Obrázek 2 - Schéma prvních čtyř propojených univerzitních sítí v USA[9]

Dalším důležitým milníkem internetu se stal rok 1983, ve kterém Ministerstvo obrany Spojených států rozdělilo síť ARPANET na dvě části. Vznikla tak armádní síť MILNET a síť ARPANET byla k dispozici pro civilní účely. Důležité je zmínit, že v tomto roce, konktrétně v lednu, se přestal používat protokol NCP (network control protocol), který běžel v tuto dobu v síti ARPANET. Nahradila jej nová sada protokolů TCP/IP (Transmission Control Protocol/Internet – primární přenosný protokol/protokol síťové vrstvy). Tyto protokoly umožnily geograficky propojit vzdálené a technologicky různorodé sítě. Protokol TCP/IP vznikl v době, kdy byly připojeny desítky až stovky počítačů a funguje dodnes, přičemž v současnosti jsou na něj napojeny miliardy zařízení. Vytvořil jej americký informatik Vinton Gray Cerf společně s americkým elektroinženýrem Bobem Kahnem. Tito muži jsou považováni za otce internetu.[10]

Síť ARPANET, financovaná resortem Ministerstva obrany Spojených států amerických, nebyla jedinou počítačovou sítí v USA ani na světě. Počítačové sítě si budovaly i jiné organizace, a právě díky dostupnosti protokolů TCP/IP mohli jejich provozovatelé propojit svou vytvořenou síť se sítí ARPANET. Síť ARPANET se tak stala jakousi zárodečnou sítí, na kterou se postupně napojovaly další a další, až vznikla celá flotila takto vzájemně propojených sítí. Postupem času se síť ARPANET dostala do role tzv. páteřní sítě, přes kterou procházel veškerý síťový provoz. Vzhledem k výše uvedenému je zapotřebí zmínit nejvýznamnější síť, která se v roce 1986 s ARPANETEM propojila. Jednalo se o síť NSFNET (National Science Foundation), která se ve Spojených státech zabývala podporou vědy a výzkumu obecně. Síť NSFNET díky svým

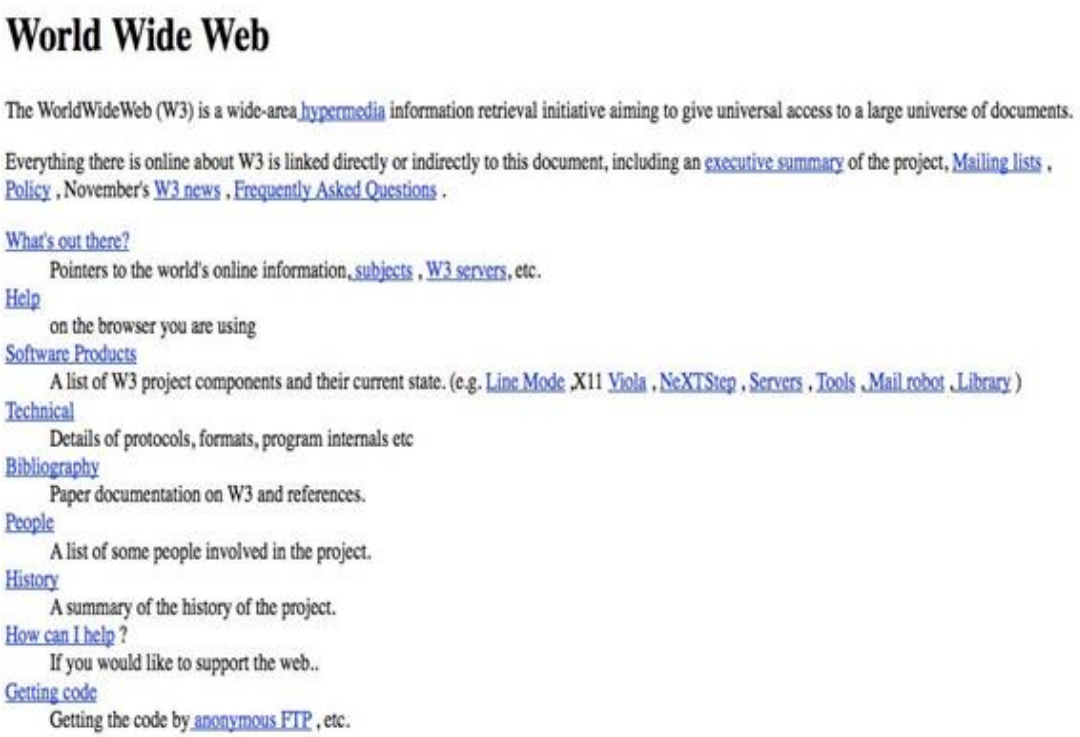
[9] Dostupné z: https://hrej.cz/article/internet-vznikl-kdyz-clovek-dobyval-mesic

[10] Internet a jeho služby: *Historie Internetu*. [online]. [cit. 2022-01-25]. Dostupné z: https://ijs2.8u.cz/index.php?option=com_content&view=article&id=32&Itemid=134

schopnostem postupně přejala roli páteřní sítě, tedy původní roli ARPANETU, což vedlo k tomu, že v březnu 1990 byla síť ARPANET v tichosti odstavena a následně zrušena.[11]

Krátce před zánikem ARPANETU se v roce 1989 začali Tim Bernes-Lee a Robert Cailliau zabývat hypertextovými dokumenty. Hypertextové dokumenty měly původně obsahovat odkazy vážící se na jiné dokumenty kdekoli na síti. Tato dovednost měla být využita pouze pro vnitřní potřebu švýcarské organizace CERN (Evropská organizace pro jaderný výzkum), ale časem se zpřístupnila širšímu spektru uživatelů a dnes je stále používaná v podobě „www“ (WorldWideWeb). Dne 6. srpna 1991 byly na adrese hhttp://info.cern.ch spuštěny první webové stránky, které jsou taktéž domovskou stránkou organizace CERN. V průběhu roku 1992 se k dokumentům dostupným na www začaly přidávat i obrázky. Tento rok je považován za start komerčního internetu, který se pomalu a jistě začal rozšiřovat, a to i vlivem rostoucí dostupnosti počítačů ve firmách a domácnostech.[12]

Obrázek 3 - První World Wide Web na světě[13]



[11] PETERKA, J., *EaRCHIV.CZ, Na počátku byl ARPANET ….* . [online]. [cit. 2022-01-28]. Dostupné z: http://www.earchiv.cz/a95/a504c502.php3

[12] Internet a jeho služby: *Historie Internetu.* [online]. [cit. 2022-01-25]. Dostupné z: https://ijs2.8u.cz/index.php?option=com_content&view=article&id=32&Itemid=134

[13] Dostupné z: http://info.cern.ch/hypertext/WWW/TheProject.html

Následující léta byla ve znamení bleskového rozvoje internetu, zejména v souvislosti se zlepšováním grafického náhledu a ohromným nárůstem připojených uživatelů. Síť se rozšiřovala závratným tempem. Pro představu lze uvést, že v roce 1987 bylo statisticky zaznamenáno téměř 27 tisíc propojených uživatelů internetu na světě, v roce 1996 jejich počet vzrostl na 55 milionů. V roce 2000 vzrůstající trend pokračoval, bylo evidováno zhruba 250 milionů uživatelů, a z toho v České republice přibližně 500 tisíc. V roce 2010 už počet uživatelů po celém světě přesáhl 2 miliardy. V roce 2021 bylo evidováno přes 5,1 miliardy uživatelů internetu.[14]

Ačkoli byl internet vybudován na základech sítí ARPANET a NSFNET, v současné době internet vlastníka nemá a neexistuje ani centrální autorita či instituce, která by jej řídila.[15]

2.2 Počátky internetu v České republice

Počátky českého internetu lze datovat do doby tehdejšího Československa. První počítač byl oficiálně připojen 13. února 1992, a to prostřednictvím sítě univerzity ČVUT v Praze. Za vším stála zhruba desetičlenná skupina odborníků z řad akademiků, která se velmi zajímala o internet a technologie obecně. Díky svým kontaktům s kolegy z rakouské univerzity v Linci, kde byla v provozu počítačová síť EARN (European Academic and Research Network), se odhodlali k experimentu spočívajícím na kontinuálním vytáčení přístupu do Lince. Šlo však o mezinárodní hovor, který nebyl nikterak kvalitní, a navíc byl relativně drahý. Postupem času nabídla americká nadace George Mellon Foundation českým vědcům prostředky na nákup modemů umožňujících navýšení rychlosti spojení. Díky tomu se v rámci jednoho uzlu dokázalo připojit výše zmiňované pracoviště výpočetního centra ČVUT. Významná osoba, Steven Goldstein, zástupce americké grantové agentury National Science Foundation (NSF), rozhodoval o tom, kdo se může k síti připojit. Zásadní podmínku vymezil tak, že síť může používat výhradně akademická instituce, tudíž komerčním zájemcům, kteří začali o využívání sítě jevit zájem, měl být svět internetu zapovězen. Prvním připojením internetu v Československu bylo pověřeno Oblastní výpočetní centrum vysokých škol, konkrétně

[14] *World Internet Users and 2021 PopulationStars.* [online]. [cit. 2021-12-23]. Dostupné z: https://www.internetworldstats.com/stats.htm
[15] KOLOUCH, J. *CyberCrime.* 1. vyd. Praha: CZ.NIC, z. s. p. o. 91 s. ISBN 978-80-88168-15-7.

Oddělení informačních soustav. V jeho čele stál Ing. Jan Gruntorád, CSc., emeritní ředitel sdružení CESNET. V den prvního připojení internetu do Československa byla přenosná rychlost dat 19,2 kb/s. Pro srovnání, v dnešní době nejvýkonnější infrastruktura, kterou disponuje akademická síť CESNET2, je s mezinárodním internetem spojena linkami o kapacitě až 100 Gb/s, což je milionkrát efektivnější vzhledem k rychlosti, než tomu bylo při prvním připojení. Další zajímavostí je informace o prvním počítači, který byl v tehdejším Československu připojen. Jednalo se o sálový počítač firmy IBM, vážící několik tun. V dnešní době lze připojit k internetu mobilní telefon vážící několik stovek gramů.[16]

Začátky internetu v České republice po prvním oficiálním připojení k síti byly obtížné, jelikož zde neexistovala žádná infrastruktura, která by umožňovala rozšíření ve více místech. Hlavní roli při šíření internetu sehrála akademická sféra. Rozhodlo se o rozvoji celostátní páteřní sítě spojující akademické instituce, které dále rozváděly internet do metropolitních sítí. V březnu roku 1993 disponovala Česká republika jedenácti uzly propojujícími jedenáct českých měst. Další rozmach internetu v České republice zajistila dohoda rektorů, kteří podpořili návrh na vzájemné propojení vysokých škol. Vlivem tohoto rozhodnutí byly z rozpočtu vysokých škol vyčleněny finanční prostředky, které umožnily vznik sdružení CESNET (Sdružení vysokých škol a Akademie věd České republiky) pro budování páteřní sítě, která nesla stejný název jako sdružení. CESNET byl založen v roce 1996 a od té doby je největším lídrem technologického pokroku v zemi, kterou navíc reprezentuje v nejpokrokovějších internetových projektech, například v budování panevropské gigabitové sítě GÉANT spojující vědce a výzkumníky z celého evropského kontinentu. V polovině 90. let minulého století se internet začal otevírat komerčním, podnikatelským a soukromým uživatelům. Postupně se dostal mimo akademickou sféru a začala jej používat většina světové populace.[17]

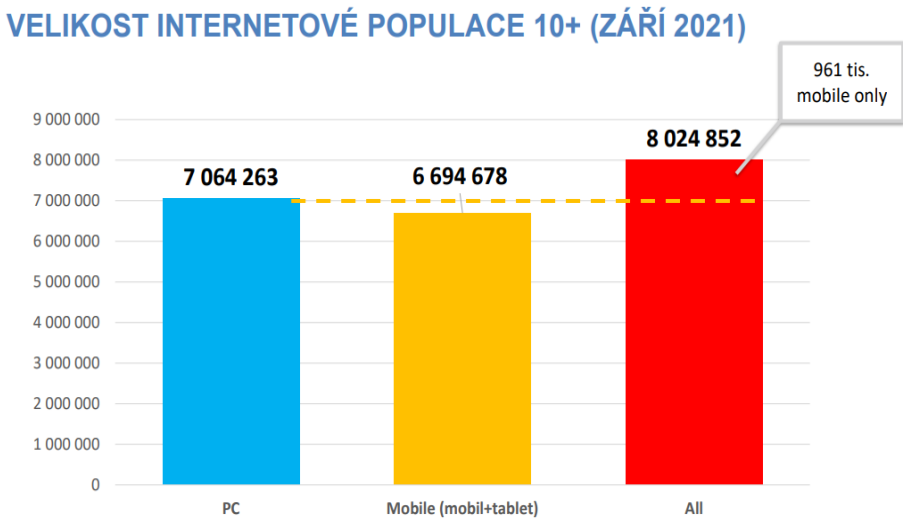
Internet ve světě i v České republice je neustále na vzestupu a téměř každý moderní člověk se bez něj neobejde či jej minimálně občas využívá. Lze konstatovat, že připojit k internetu se dá díky místům s veřejně přístupnou sítí téměř všude. Na světě je dle odhadu téměř 7,9 miliard lidí, a z toho internet využívá dle nejnovějších údajů ITU

[16] KASÍK, P., iDNES.cz: *Český internet slaví 20. Narozeniny, vzpomíná skromné začátky*. [online]. [cit. 2012-02-13]. Dostupné z: https://www.idnes.cz/technet/internet/cesky-internet-slavi-20-narozeniny-vzpomina-na-skromne-zacatky.A120213_000221_sw_internet_pka

[17] KASÍK, P., iDNES.cz: *Český internet slaví 20. Narozeniny, vzpomíná skromné začátky.* [online]. [cit. 2012-02-13]. Dostupné z: https://www.idnes.cz/technet/internet/cesky-internet-slavi-20-narozeniny-vzpomina-na-skromne-zacatky.A120213_000221_sw_internet_pka

(Mezinárodní telekomunikační unie) větší polovina světové populace, tedy přes 5,2 miliardy uživatelů, což je 65,6 % uživatelů celosvětově. Bez přístupu k internetu jsou dnes ještě stále méně vyspělé země, což tvoří 34,4 % světové populace. Dle Českého statistického úřadu měla Česká republika k 23.12.2021 10 682 029 obyvatel, z toho 83 %, tedy 8 866 084 obyvatel, má v domácnosti připojení k internetu.[18]

Obrázek 4 - Velikost internetové populace v ČR k září 2021[19]



[18] *Český statistický úřad.* [online]. [cit. 2021-12-23]. Dostupné z: https://vdb.czso.cz/vdbvo2/faces/cs/index.jsf?page=vystup-objekt&z=T&f=TABULKA&skupId=2705&katalog=31031&pvo=ICT03B&pvo=ICT03B

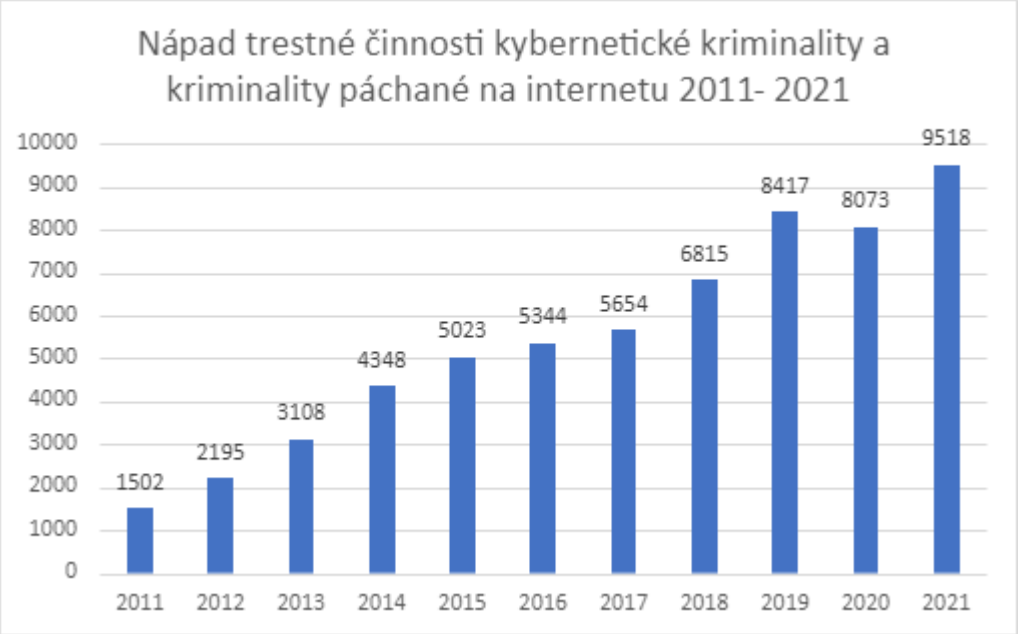
[19] Dostupné z: https://www.spir.cz/sites/default/files/prilohy/SPIR_2021_10_3Q_kvartalni_prezentace_zkracena.pdf

3 Kybernetická kriminalita

Dynamický rozvoj informačních technologií s sebou přináší nové společensky škodlivé jednání, proto je kybernetické kriminalitě věnována stále větší pozornost. Pojem kybernetická kriminalita je odvozován od pojmu kybernetický prostor, případně zkráceně kyberprostor.

Policie ČR od roku 2011 sleduje počet trestných činů spáchaných v kyberprostoru. V tomto období je zaznamenán stále vzrůstající trend evidovaných případů kybernetické kriminality (vzrůst z 1502 trestných činů v roce 2011 až po 9518 trestných činů v roce 2021).[20]

Obrázek 5- Statistika vývoje kybernetické kriminality 2011-2021 vedená Policií ČR[21]



V roce 2020 lze z grafického znázornění shledat snížení trestných činů páchaných v kyberprostoru oproti roku 2019. Tato skutečnost je dle Národní centrály proti organizovanému zločinu České republiky zapříčiněna zejména změnou legislativy, tedy zákona č. 40/2009 Sb., trestního zákoníku, kdy od 1. října 2020 došlo ke změně ustanovení § 138 odst. 1 trestního zákoníku, které se týkalo hranice výše škody. Dřívější

[20] POLICIE ČESKÉ REPUBLIKY, *Vývoj registrované kriminality v roce 2021*. [online]. [cit. 2022-01-29]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx
[21] Zdroj: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx

hranice trestného činu, škoda nikoli nepatrná činila 5 000,- Kč. Po novele trestního zákona se zvýšila na minimální částku 10 000,- Kč.[22]

3.1 Historie kybernetické kriminality a současnost

Kriminalita je s lidskou společností spojena už odjakživa. Pachatelé trestných činů neustále zdokonalují jejich provádění, využívají k tomu nové technologie a vytvářejí nové metody, které jim pomáhají utajit svou identitu. Kybernetická kriminalita vznikla již prvním propojením počítače se sítí, protože již od této doby mohlo docházet k jejím prvním náznakům. V počátcích vývoje internetu však nikdo nepředpokládal tak dynamický vzestup informačních technologií v nastávajících desetiletích, tudíž nebyl kladen velký důraz na jejich bezpečnost. Počátky kyberkriminality v té době spočívaly v kopírování technických a uživatelských vlastností počítačů, jelikož byly pro většinu populace neznámým pojmem a byly velice obtížně dostupné. Počítače zprvu vlastnila jen hrstka podniků a vědecké instituce. Později se postupně dostávají ke každému z nás. Pravděpodobně první počítačový zločin, který se u nás odehrál v sedmdesátých letech minulého století, byl založen na tom, že nespokojený zaměstnanec Úřadu důchodového zabezpečení magnetem poškozoval záznamy na magnetických páskách. Oficiální informace o tomto případu sice neexistují, ale měl být kvalifikován jako sabotáž tehdejšího zákona.[23]

Za dob éry socialistického režimu si uživatelé, kteří neměli přístup k počítačům nacházejícím se především ve velkých klimatizovaných sálech pod dohledem specialistů, uvědomovali další možnosti páchání trestné činnosti spojené s využitím počítačů. Jednalo se o dokladové delikty, které byly založeny na tom, že pachatelé začali pozměňovat podklady připravené ke zpracování do počítače. Tento počítačový zločin byl nejčastěji odhalitelný. Jeho podstatou byla převážně manipulace s doklady ve mzdových účtárnách, v zásobování a na jiných pracovištích, kde měl zaměstnanec možnost pracovat s penězi. V 80. letech bylo odhaleno 14 případů trestního stíhání tohoto typu. Pachatelé si

[22] NÁRODNÍ CENTRÁLA PROTI ORGANIZOVANÉMU ZLOČINU SLUŽBY KRIMINÁLNÍ POLICIE A VYŠETŘOVÁNÍ. *VÝROČNÍ ZPRÁVA.* [online]. [cit. 2022-01-29]. Dostupné z: www.policie.cz ›soubor ›vyrocni-zprava-ncoz-2020

[23] SMEJKAL, V. *Kybernetická kriminalita*, 2. vyd. Plzeň: Aleš Čeněk, 2018. 102 s. ISBN 978-80-7380-720-7.

uvědomovali, že jednodušší je měnit údaje přímo v počítači, ale tento krok byl velmi problematický, protože dostat se k němu bylo složité. Další časté páchání trestné činnosti v souvislosti s počítači spočívalo v provádění úkonů na počítačích zaměstnavatelů. Jednalo se především o tisk různých obrázků na řádkové tiskárně, výpočty diplomových prací, až po nelegální podnikání za účelem vlastního zisku.[24]

Další zdokonalování v oblasti počítačových systémů a jejich následné využívání společností má za následek zvyšující se trestnou činnost spojenou s počítači. Nových technologií začali využívat ve většině případů podvodníci, kteří zneužívali počítače pro klasickou známou trestnou činnost již dříve. Nyní však byla snáze proveditelná a pro orgány činné v trestním řízení hůře zjistitelná. Jedná se především o podvody, které zahrnují další podvody (pharming, phishing apod.). Vznikají útoky na funkčnost počítačových systémů, zejména DoS a DDoS útoky, nasazování malware a spyware atd. Dochází k organizovaným útokům teroristickými a státními orgány ve snaze dostat se k informacím zpracovaným v počítačích. Významnou kategorií trestných činností spojených s počítači je porušování autorských práv.[25]

Tato práce se bude detailněji zabývat podvodnými praktikami pachatelů.

Z rozvojového hlediska internetu dělí Završnik ve své publikaci s názvem „Kyberkriminalita“ kyberkriminalitu do tří generací:

1. První generace, ve které se informační technologie používají zejména ke shromažďování informací nebo ke komunikaci.

2. Druhá generace (tzv. hybridní kriminalita), kdy se informační technologie používají k šíření zločineckých dovedností, které existovaly již před vznikem informačních technologií a internetu.

3. Třetí generace (tzv. automatizovaná kriminalita), která vznikla s rozvojem širokopásmového propojení informačních technologií.[26]

[24] SMEJKAL, V. *Kybernetická kriminalita*, 2. vyd. Plzeň: Aleš Čeněk, 2018. 103 s. ISBN 978-80-7380-720-7.
[25] KOLOUCH, J. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z. s. p. o. 181 s. ISBN 978-80-88168-15-7.
[26] ZAVRŠNIK, A. *Kyberkriminalita*. Praha: Wolters Kluwer ČR, 2017. 17 s. ISBN 978-80-7552-759-2.

3.2 Vymezení a definice pojmů kybernetické kriminality

Z latinského slova „*crimen*“[27] je odvozeno české slovo kriminalita, které je spojováno s lidskou společností odjakživa. Kriminalita ve spojení se slovem počítač, tedy „počítačová kriminalita“, dále naznačuje nové možnosti páchání kriminality, zejména za užití počítačů. Lze tedy konstatovat, že spojení těchto dvou slov můžeme označovat za relativně nový druh kriminality a lze jej zařadit mezi již ustálené používané pojmy kriminalistiky jako jsou násilná kriminalita, kriminalita mladistvých, ekonomická kriminalita a další. Těmito pojmy jsou označovány skupiny trestných činů mající společný faktor způsobu provedení. V různých publikacích a právních normách zabývajících se trestnými činy v oblasti výpočetní techniky, informačních systémů a informačních technologií, užívají různí autoři odlišných pojmů pro označení těchto deliktů. Zmíněný pojem počítačová kriminalita někteří nahrazují výrazy jako kybernetická kriminalita, kybernalita a další.[28]

Neexistuje jediná univerzální, obecně přijímaná definice kybernetické kriminality, která by plnohodnotně vymezila rozsah a hloubku této definice.

Výkladový slovník kybernetické bezpečnosti uvádí definici počítačová či kybernetická kriminalita takto: *„ Trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti (Více také Počítačová kriminalita). “*[29]

Policie České republiky definuje kybernetickou kriminalitu takto: „*Kybernetická kriminalita je označována jako trestná činnost, která je páchána v prostředí informačních a komunikačních technologií, včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za*

[27] *crimen* – zločin, obvinění
[28] SMEJKAL, V. *Kybernetická kriminalita*, 2. vyd. Plzeň: Aleš Čeněk, 2018. 23 s. ISBN 978-80-7380-720-7.
[29] JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualizované. Vydání. Praha: AFCEA, 2015. 69 s. ISBN 978-80-7251-397-0. Dostupné z: https://cybersecurity.cz/data/slovnik_v310.pdf

výrazného využití informačních a komunikačních technologií, jakožto významného prostředku k jejímu páchání.“[30]

Ze všech výše zmíněných definic je patrné, že s kybernetickou kriminalitou je spojen počítač nebo jemu obdobný prostředek jako například mobilní telefon, tablet, notebook a další. Pochopitelně útok může směřovat i na komponenty počítače jako hardware, software a případně data, která jsou v počítači zpracována nebo uložena. To samé platí o datových nosičích, v nichž jsou data uložena, například externí paměťový flashdisk nebo jiné nosiče dat jako jsou CD nebo DVD. Útok může též směřovat na data během samotného přenosu, tedy na data reprezentovaná posloupností bitů a bytů v digitálním prostředí, buď pomocí hmotného média nebo bezdrátovým přenosem.[31]

Při náhledu do trestního zákoníku nenajdeme přesnou definici kybernetické kriminality, ale lze v něm dohledat konkrétní skutkové podstaty trestných činů týkajících se této problematiky.

3.3 Pojmy související s kyberkriminalitou

Při definici kybernetické kriminality se setkáváme s mnoha pojmy, které nám přibližují tuto problematiku.

3.3.1 Kybernetický prostor

Existuje mnoho definic a pojetí kyberprostoru. Výkladový slovník kybernetické bezpečnosti definuje kybernetický prostor jako *„Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.“*[32] Kybernetický prostor lze označit jako imaginární počítačový svět tvořící globální počítačovou síť, která je základem online komunikace. Dá se konstatovat, že kyberprostor je rozsáhlá počítačová síť tvořena menšími a po takřka celém světě strategicky rozmístěnými počítačovými sítěmi, které užívají TCP/IP protokol, umožňující komunikaci a výměnu dat. Znaky kyberprostoru jsou

[30] POLICIE ČESKÉ REPUBLIKY, *Kyberkriminalita* [online]. [cit. 2022-01-29]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[31] SMEJKAL, V. *Kybernetická kriminalita*, 2. vyd. Plzeň: Aleš Čeněk, 2018. 23 s. ISBN 978-80-7380-720-7.

[32] JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualizované. Vydání. Praha: AFCEA, 2015. 70 s. ISBN 978-80-7251-397-0. Dostupné z: https://cybersecurity.cz/data/slovnik_v310.pdf

decentralizovanost, globálnost, otevřenost, hojnost dat/informací a to včetně tzv. *„informačního smogu“*[33] , interaktivnost a možnost ovlivňovat uživatele. Společnost se v běžném životě za pomocí internetu (kyberprostoru) a nových technologií neustále vystavuje hrozbám a rizikům kybernetických útoků.[34]

Kybernetický prostor lez rozdělit do tří částí:

1. **Surface Web** (někdy také jako Visible Web, Clearnet, Indexed Web aj.) je součástí kybernetického prostoru, který je dostupný většině populace a lze v něm surfovat za užití standardních webových prohlížečů. Tato část kyberprostoru obsahuje běžně používané služby jako např. Google, Facebook, YouTube, Seznam a mnoho dalších webů. Surface Web tvoří zhruba 4 % celkové kapacity internetu.

2. **Deep Web** – jedná se o World Wide Web, jehož obsah není přístupný pomocí klasických vyhledávačů jako například Internet Explorer, Google Chrome a dalších. Tyto prohlížeče nejsou schopny nebo nechtějí zahrnout některé webové stránky do svého indexu. Tvoří 96 % celého internetu.

3. **Dark Web** – jedná se o podmnožinu deep webu, protože dostat se k jeho obsahu lze jen za užití specifického softwaru a možné autorizace, opět jako u deep webu, není dohledatelný běžným vyhledávačem. Jedná se spíše o ilegální web.[35]

Obrázek 6 - Schéma kyberprostoru[36]

[33] Tento pojem označuje informaci, která je založena na nepravdě, jedná se o absolutní nesmysl, polopravdu nebo lež.
[34] KOLOUCH, J. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z. s. p. o. 42 s. ISBN 978-80-88168-15-7.
[35] KOLOUCH, J. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z. s. p. o. 47 s. ISBN 978-80-88168-15-7.
[36] Dostupné z: https://itigic.com/cs/deep-web-best-sites-markets-domains-links/

Zmiňovaný Deep Web a Dark Web jsou zcela legálními sítěmi. Je relativně složité se do nich dostat. Myšlenkou těchto webů je umožnit uživatelům přístup k internetu a ke svobodným informacím s vyšším stupněm anonymity a bezpečnosti. Tyto weby nepodléhají cenzuře ani zákonům. Ovšem díky vysoké anonymitě se na nich nachází stránky s ilegálním obsahem, například prodejem drog, zbraní, dětskou pornografií, falešnými identitami, čísly bankovních účtů atd. Není divu, že tyto weby jsou monitorovány speciálními skupinami bezpečnostních služeb po celém světě.[37]

3.3.2 Kybernetický útok

Výkladový slovník kybernetické bezpečnosti definuje kybernetický útok jako *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků“*.[38] Tato definice však neoznačuje všechny negativní aktivity uživatelů kyberprostoru, například nepostihuje ekonomicky motivované útoky, které v současné době dramaticky rostou. Na základě toho lze obecně konstatovat, že kybernetický útok je jakékoli protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby. Protiprávní jednání v kyberprostoru je zmíněno, jelikož toto jednání nemusí mít vždy znaky trestného činu, ale podstatné je, že jím útočník narušuje běžný způsob života poškozeného. To znamená, že kybernetický trestný čin sice musí být zároveň kybernetickým útokem, ale nemusí být vždy trestným činem z důvodu, že takovéto jednání není zahrnuto v trestně právní normě, ale je možné ho zahrnout pod jednání, které má povahu správně právního deliktu, či občanskoprávního deliktu nebo se může jednat o jednání, které není vyjádřitelné žádnou právní normou.[39]

[37] HACKERS LEAGUE BOOKS. *WhatisSurface Web, Deep Web and Dark Web?* [online]. [cit. 2022-01-29]. Dostupné z: https://medium.com/@hackersleaguebooks/what-is-surface-web-deep-web-anddark-web-cdbaf71b30d5

[38] JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualizované. Vydání. Praha: AFCEA, 2015. 71 s. ISBN 978-80-7251-397-0. Dostupné z: https://cybersecurity.cz/data/slovnik_v310.pdf

[39] KOLOUCH, J. *CyberCrime.* 1. vyd. Praha: CZ.NIC, z. s. p. o. 55 s. ISBN 978-80-88168-15-7.

3.4 Legislativní rámec majetkové kybernetické kriminality

Legislativní pojetí majetkové kybernetické kriminality vychází regulativně především z mezinárodních smluv, především Úmluvy o kyberkriminalitě a z Dodatkového protokolu. Dále jsou pro legislativní rámec klíčové evropské směrnice, které definují požadavky na dobu hmotně i procesněprávní, národní úpravy, které jsou poté definovány v české národní úpravě, tedy především v trestním zákoníku a trestním řádu.[40]

V důsledku zvýšené kybernetické kriminality, která je páchána i za hranicemi České republiky, je zapotřebí spolupracovat s ostatními státy, které však mají mnohdy odlišné právní úpravy. Spolupráce probíhá na bázi mezinárodních úmluv, které zabezpečují sjednocený přístup v boji s kyberkriminalitou. K tomuto účelu vznikla Úmluva o počítačové kriminalitě, která byla schválená 31. listopadu 2001 v Budapešti. Česká republika podepsala Úmluvu 9. února 2005. Ratifikovaná byla 22. srpna 2013. Úmluva o počítačové kriminalitě je hlavním nástrojem v oblasti kybernetické kriminality. Ve čtyřech kapitolách pojednává o problematice hmotného a procesního práva a zaměřuje se i na mezinárodní spolupráci. První kapitola vymezuje základní pojmy užívané Úmluvou. Druhá kapitola zahrnuje trestní právo hmotné a trestní právo procesní. Kapitola třetí se zaměřuje na mezinárodní spolupráci a spolupráci justičních orgánů. Kapitola čtvrtá se zabývá procedurálními záležitostmi. Řeší spory, výhrady, územní působnost apod. K Úmluvě je zahrnut i Dodatkový protokol o kriminalizaci činů rasistické a xenofobní povahy páchaných za pomocí počítačového systému.[41]

Evropská unie usiluje o výrazné snížení kybernetické kriminality, a to za pomoci silných a účinných právních předpisů a také se snaží o efektivnější koordinaci mezi orgány činných v trestním řízení v Evropské unii. Na základě toho byla vypracována strategie kybernetické bezpečnosti Evropské unie, ze které vychází Směrnice Evropské unie. Nejstarší směrnicí je „*Návrh Evropského parlamentu a Rady o potírání podvodu v oblasti bezhotovostních prostředků pro placení a jejich padělání a o nahrazení*

[40] POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018, 544 s. ISBN: 978-80-7598-045-8 (váz.)
[41] POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018, 545 s. ISBN: 978-80-7598-045-8 (váz.)

rámcového rozhodnutí Rady č. 2001/413/SVV"[42], která je neustále Evropskou unií novelizována, naposledy ze dne 17. dubna 2019.[43]

V České republice je právní úprava kyberkriminality zahrnuta v trestněprávních předpisech, a to zejména ve zvláštní části trestního zákoníku, kde jsou uvedeny jednotlivé skutkové podstaty trestných činů. V trestním zákoníků lze shledat skutkové podstaty trestných činů, k jejichž naplnění dochází při využití informačních a komunikačních technologií. Skutkové podstaty kyberkriminality můžeme rozdělit do třech rovin a to:

1. Trestné činy proti důvěrnosti, dostupnosti a integritě počítačových systémů nebo dat,

2. Trestné činy, k jejichž uskutečnění je nutné využití informačních a komunikačních technologií,

3. Trestné činy spojené s využitím informačních a komunikačních technologií jako znak kvalifikované skutkové podstaty.[44]

Majetková kybernetická kriminalita je v legislativním pojetí součástí majetkové kriminality, kterou se zabývá zákon č. 40/2009 Sb., trestní zákoník. Jedná se především o následující paragrafová znění:

§ 182 Trestního zákoníku (dále jen „TZ") – Porušení tajemství dopravovaných zpráv

§ 183 TZ – Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

§ 209 TZ – Podvod

§ 230 TZ – Neoprávněný přístup k počítačovému systému a nosiči informací

§ 231 TZ – Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

[42] Směrnice Evropského parlamentu a Rady (EU) 2019/713 ze dne 17. dubna 2019. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32019L0713&qid=1643569660363
[43] POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018, 546 s. ISBN: 978-80-7598-045-8 (váz.)
[44] POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018, 553 s. ISBN: 978-80-7598-045-8 (váz.)

§ 232 TZ – Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

§ 234 TZ – Neoprávněné opatření, padělání a pozměnění platebního prostředku

§ 236 TZ – Výroba a držení padělatelského náčiní

§ 268 TZ – Porušení práv k ochranné známce a jiným označením[45]

4 Kybernetické útoky zaměřené na majetek v kyberprostoru

Mezi kybernetické útoky majetkové internetové kriminality můžeme zařadit sociální inženýrství, hacking, cracking, internetové pirátství, phishing, pharming, spearphising, vishing, smishing, podvodné weby atd.

4.1 Sociální inženýrství

Sociální inženýrství není přímým kybernetickým útokem. Jedná se o chování útočníků, kteří svým počínáním ovlivňují uživatele, manipulují s nimi a dovedou je přimět k provedení akce, díky které získají jejich citlivá data a další informace.

Sociální inženýři chtějí, aby se uživatelé na internetu domnívali, že vše je ve skutečnosti v pořádku. Pachatel nechce prolamovat složitě hesla, ale snaží se je vymámit ze samotných uživatelů. Oběť zmanipuluje natolik, že mu sama prozradí heslo nebo jiné přístupové údaje. Sociální inženýři se snaží získat tímto způsobem co nejvíce dat a informací a využívají k tomu neopatrnost a důvěřivost uživatelů. S rozvojem informačních a komunikačních technologií vylepšují své techniky. Mezi nejčastější útoky sociálního inženýrství patří podvodné e-maily. Pachatelé posílají e-maily, které mají vypadat jako důležitá zpráva od důvěryhodné instituce, např. banky. V e-mailu uvádějí odkaz, pod kterým se má uživatel dostat do bankovnictví, ale odkaz jej následně přesměruje na podvodný web. Dalšími častými metodami útoků jsou podvodné weby,

[45] POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018, 545 s. ISBN: 978-80-7598-045-8 (váz.)

telefonické hovory, prohledávání veřejných informací, webů a sociálních sítí, doručování reklamních a dalších materiálů na paměťových nosičích, podvodné nabídky k vyzkoušení internetové služby zdarma nebo vydávání se za falešné servisní techniky.

Sociální inženýři vedou zpravidla útoky třemi způsoby, které se mezi sebou vzájemně kombinují.

1. Jedná se především o sběr dostupných informací o oběti nacházející se v kyberprostoru.

2. Samotný útok, kdy sociální inženýr provádí útok zejména podvodným jednáním, kdy se vydává za někoho, kým doopravdy není s cílem zmanipulovat oběť, aby mu sdělila potřebné informace, které sociální inženýr žádá.

3. Samotný psychologický útok.

Sociální inženýři nejčastěji používají podvodné e-maily či weby, telefonní hovory, útoky „face to face“, prohledávání „trashe“ v kyberprostoru, vyhledávání citlivých informací na webech a sociálních sítích, doručování webových reklam nebo jiných datových nosičů, ponechávání paměťového média na zájmových místech, různé nabídky zdarma na webech, dodávky nebo nalezení ICT zařízení, falešná identita a další nové metody, které sociální inženýři stále vyvíjejí.

Obrana proti sociálnímu inženýrství je zcela na zodpovědnosti každého jednotlivce. Z toho vyplývá, že je důležité prohlubovat povědomí o této problematice v rámci celé společnosti, hovořit o jednotlivých technikách a praktikách sociálních inženýrů. Jedna známá pranostika hovoří „Důvěřuj, ale prověřuj!“. Už Albert Einstein vyslovil citát *„Pouze dvě věci jsou nekonečné: vesmír a lidská hloupost. Ačkoli tím prvním si nejsem jist.“*[46]

4.2 Hacking a Cracking

Hacking je činnost cílená k získání nelegálního přístupu k cizímu počítačovému systému nebo počítačové síti. Je nejstarším způsobem páchání kybernetické kriminality,

[46] KOLOUCH, J. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z. s. p. o. 186-192 s. ISBN 978-80-88168-15-7.

která je neetická a velmi často na hraně zákona. Cracking je nelegální prolamování přístupových údajů ve snaze způsobit oběti škodu. Je velmi často spojován s porušováním autorských práv, s obcházením ochranných prvků apod. S Crackingem je spojován termín password cracking, který umožňuje vstup do zabezpečeného zařízení či hardwaru, a to díky prolomení uživatelského hesla.[47]

Hackera je náročné definovat, ale dle Jirovského publikace jej lze charakterizovat jako člověka, který se zabývá programováním, je rychlý a může být expertem v konkrétním programu nebo odborníkem ve vědeckém oboru. Hacker bývá okolím vnímán jako jedinec, který se dopouští ilegálních aktivit. Hacker je ale i osoba, která prolamuje údaje např. pro Policii ČR a neobohacuje se na získaných informacích a datech.[48]

4.3 Internetové pirátství

Internetové pirátství je zneužíváním autorství, kdy jsou porušována intelektuální vlastnická práva. Internetové pirátství je jedním z nejčastěji se vyskytujících druhů kybernetické kriminality vůbec. Při porušování práv duševního vlastnictví bývají porušována práva autorská a průmyslová. V případě autorských práv nemusí jít pouze o práva na literární díla, ale také na hudbu, vysílání, programy a reklamu. Průmyslová práva naopak chrání různé ochranné známky a patenty.[49]

4.4 Phishing

Phishing, tzv. rybaření, je nelegální činností kyberzločinců, která má za cíl od uživatelů podvodným způsobem získat citlivé informace jako přihlašovací údaje, hesla, údaje k platebním kartám atd. Tyto informace kyberzločinci získávají navozením důvěryhodného prostředí pomocí elektronické komunikace prostřednictvím e-mailu nebo podvodných webových stránek. Uživatel v mnoha případech zjistí, že byl podveden, až

[47] KLIMEK, L. ZÁHORA, J., HOLCR, K. *POČÍTAČOVÁ KRIMINALITA v európskych súvislostiach*. 2016. Bratislava. Wolters Kluwer s.r.o. 29 s. ISBN: 978-80-8168-5358-5.
[48] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha. 52 s. ISBN: 978-80-247-1766-1.
[49] KOLOUCH, J. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z. s. p. o. 277 s. ISBN 978-80-88168-15-7.

v době, kdy byly jeho přístupové údaje neoprávněně zneužity. Phishing využívá praktiky sociálního inženýrství. V praxi se lze setkat se Spear Phishingem, který je jednou z forem phishingového útoku, s tím rozdílem, že je cílen na konkrétní oběť.[50]

4.5 Pharming

Pharming je typem phishingu. V praxi se nejčastěji setkáváme s odkazem na podvodný web, který vypadá stejně jako internetové bankovnictví. Nepozorný uživatel tam zadá své přístupové údaje, čímž je velmi snadno předá do rukou pachatele.[51]

4.6 Podvodné weby

Podvodné weby jsou internetové stránky, které lákají uživatele na výhru, zboží zdarma nebo na výhodnou koupi. Opět je při těchto podvodech využíváno sociálního inženýrství a přístupové údaje získávají útočníci formou využité nabídky registrace k webu. Uživatel se v dobré víře registruje a věří, že obdrží slíbenou výhru nebo zboží, naopak pachatel získá citlivá data, která může zneužít.[52]

4.7 Malware

Malware je škodlivý software, který má za úkol skrytě zaútočit na cizí zařízení, tak aby z něj byly odcizena citlivá data. Oběť, pokud není odborně znalá v oblasti informačních a komunikačních technologií, napadení ani neregistruje. Malware je doručován na koncová zařízení mnoha způsoby, ale pro jeho samotné doručení je potřeba součinnosti oběti. Nejznámější způsob doručení malware do zařízení je tzv. Drive-by

[50] JELÍNEK, J. GŘIVNA, T. POLČÁK, R. *Kybernetická kriminalita.* 1. vyd. Praha 2013. 58 s. ISSN 0323-0619.
[51] KOLOUCH, J. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z. s. p. o. 263 s. ISBN 978-80-88168-15-7.
[52] KOLOUCH, J. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z. s. p. o. 266 s. ISBN 978-80-88168-15-7.

download malware, který se do něj nainstaluje pouhou návštěvou již napadeného webu. Dále trojanizované aplikace, které se mohou nacházet takřka všude v kyberprostoru, tak i mimo něj, např. na různých uložištích nebo přenosných médiích.[53]

5 Odhalování a vyšetřování kybernetické kriminality

Odhalování a vyšetřování kybernetické kriminality spadá pod zvláštní část kriminalistiky, stejně jako vyšetřování jiných druhů trestné činnosti, které jsou charakteristické svými specifickými rysy. Hlavní rys kybernetické kriminality je charakteristický užitím informačních a komunikačních technologií, včetně počítačových sítí. Počítač může být jak předmětem trestného činu, tak nástrojem k páchání trestné činnosti. Proto je zapotřebí, aby orgány činné v trestním řízení disponovaly odbornými znalostmi a adekvátním vybavením, které napomůže k dopadení pachatele a následné správné kvalifikaci skutkové podstaty trestného činu. Při vyšetřování trestných činů je velmi důležitá orientace v procesních nástrojích, díky které je možné získat přístup k důležitým datům a informacím.[54]

K vyšetřování kybernetické kriminality jsou vypracovány obecné rámcové metodiky, nejsou však stejnorodé. Během samotného vyšetřování kybernetického zločinu musí často vyšetřovatel užít více metodik a z nich zvolit konkrétní části. Například u vyšetřování podvodů za pomoci informačních a komunikačních technologií využívá jak metodiku vyšetřování kybernetické kriminality, tak metodiku vyšetřování podvodů apod.[55]

[53] ŠULC, V. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018, 40 s. ISBN 978-80-7380-737-5.
[54] POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018, 567 s. ISBN: 978-80-7598-045-8 (váz.)
[55] KONRÁD, Z.; PORADA, V.; STRAUS, J.; SUCHÁNEK, J. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování.* Plzeň: Aleš Čeněk, 2015. 340 s. ISBN: 978-80-7380-547-0.

5.1 Orgány činné v trestním řízení

Jak vyplývá ze zákona č. 273/2008 Sb., o Policii České republiky, tak *Policie České republiky je jednotný ozbrojený bezpečnostní sbor, který slouží veřejnosti. Jejím úkolem je chránit bezpečnost osob a majetku a veřejný pořádek, předcházet trestné činnosti, plnit úkoly podle trestního řádu a další úkoly na úseku vnitřního pořádku a bezpečnosti svěřené jí zákony, přímo použitelnými předpisy Evropské unie nebo mezinárodními smlouvami, které jsou součástí právního řádu (dále jen „mezinárodní smlouva“)*[56]

Policie České republiky má ve svých řadách na nejvyšší strukturální úrovni odborně školené vyšetřovatele, což je pro ni klíčové s bojem s kybernetickou kriminalitou. Klíčovým subjektem v rámci Policie České republiky na úrovni celostátní působnosti v oblasti kyberkriminality je elitní útvar Národní centrála proti organizovanému zločinu, sekce kybernetické kriminality. Její úkol je především spojen s kybernetickou kriminalitou a její koordinací. Dalším významným útvarem zabývajícím se popisovanou problematikou je Útvar zvláštních činností Policie ČR, který realizuje odposlechy a záznamy telekomunikačního provozu, sleduje osoby, věci, provádí a zaměřuje se na zajišťování elektronických důkazů. Na úrovni jednotlivých krajských ředitelství kriminální policie vznikly a nadále jsou posilovány odbory informační kriminality. Státní zástupci a soudci jsou zaškolováni v oblasti počítačové kriminality. Výše zmínění navíc tvoří odborné seskupení, které vede ke sdílení a rozšiřování know-how. V rámci Policie České republiky je však stále nedostatek odborně vzdělaných vyšetřovatelů, kteří umí pracovat s elektronickými důkazy a vést vyšetřování.[57]

[56] ŠKODA, J.; VAVERA, F.; ŠMERDA, R. *Zákon o policii s komentářem.* 2. vyd. Plzeň: Aleš Čeněk, 2013. 40 s. ISBN 978-80-7380-447-3.
[57] POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018. 567 s. ISBN: 978-80-7598-045-8 (váz.)

5.2 Další významné instituce

CERT (Computer Emergency Response Team) a CSIRT (Computer Security Incident Response Team) jsou státem zřízené instituce, které působí ve svém nadefinovaném poli působnosti a každý z nich je zodpovědný za řešení bezpečnostních a kybernetických hrozeb. Na tyto týmy se mohou obracet orgány činné v trestním řízení se zjištěným bezpečnostním incidentem, žádostí o spolupráci apod. Základní povinností těchto organizací je reagovat na zjištěnou kybernetickou hrozbu a spolupracovat v řešení incidentu. Tyto týmy plní funkci poslední instance, u které je možné žádat o spolupráci, tedy zásah, pomoc či intervenci při řešení rozsáhlejších kybernetických útoků. Rozlišují se CERT/CSIRT týmy národní a vládní. Národní a vládní CERT/CSIRT tým je jakýmsi hlavním kontaktním bodem pro řešení kybernetických incidentů na tuzemské úrovni a také působí jako kontaktní bod pro mezinárodní CSIRT týmy a pracoviště. Působí tedy na nejvyšší úrovni. Národní CERT/CSIRT týmy se zaměřují na kybernetickou bezpečnost klíčových průmyslových sektorů hospodářství státu jako plynárenství, energetika, teplárenství atd. Tyto týmy se zabývají kybernetickou bezpečností na úseku kritické informační infrastruktury státu. Vládní CERT/CSIRT týmy se zaměřují na kybernetické bezpečnostní incidenty v oblasti samosprávy a státní správy České republiky. Obě instituce využívají ke své činnosti internet, který také spravují.[58]

5.3 Postup orgánu činných v trestním řízení

Kybernetickou kriminalitou se zabývá zvláštní část kriminalistiky. *„Kriminalistika je samostatný vědní obor, který se zkoumá a objasňuje zákonitosti vzniku, zániku, vyhledávání, zajišťování, zkoumání a využívání kriminalistických stop, jiných soudních důkazů a kriminalisticky významných informací. Na tomto základě vypracovává metody, postupy, prostředky, operace a doporučení pro kriminalistickou praktickou činnost, bez ohledu na formální podmínky jejich využití v praxi různých policejních sborech.“*[59]

[58] PAČKA, R. *CSIRT: v přední linii boje proti kybernetickým hrozbám.* 1. vydání-Brno 2019. 18 s. ISBN: 978-80-7325-473-5.
[59] KONRÁD, Z.; PORADA, V.; STRAUS, J.; SUCHÁNEK, J. *Kriminalistika, Teorie, metodologie a metody kriminalistické techniky.* Plzeň: Aleš Čeněk, 2014. 12 s. ISBN 978-80-7380-535-7.

Kybernetická kriminalita se vyznačuje především dynamikou a vysokým stupněm latence, jelikož její pachatelé za sebou převážně nezanechávají žádné kriminalisticky relevantní stopy, což vyšetřovateli ztěžuje práci. Dalším problémem s vyšetřováním dané problematiky je složitost orientovat se v informačních a komunikačních technologiích. Na policejní orgán, zejména na jeho vyšetřovatele, je tak kladen velký důraz s ohledem na odborné znalosti z oblasti výpočetní techniky. Vzhledem k vysokému stupni latence je podstatné to, aby se o tomto druhu páchání Policie České republiky vůbec dozvěděla. Škody, které jsou při něm způsobovány, jsou často velmi vysoké, takže v současné době je kladen velký důraz právě na kybernetickou kriminalitu. Odhalování kyberkriminality je dlouhodobě náročné a jeho vyšetřování vyžaduje maximální koncentraci.[60]

Při samotném vyšetřování kybernetické kriminality musí vyšetřovatelé postupovat rychle a bezchybně, tak, aby nebyl pachatel v kyberprostoru včas varován a získal tak prostor na likvidaci stop. Na základě toho je třeba stanovit taktiku a plán vyšetřování, který bývá z většiny případů různý. Ve vyšetřování kybernetické kriminality není možné použít jakýsi všeobecný plán, jelikož každé vyšetřování této problematiky se od sebe liší. Dění v kyberprostoru lze pozorovat pouze za použití komunikačních a informačních technologií. Při odhalování a objasňování trestných činů používá Policie České republiky sítě osob, prověřuje anonymní oznámení, pozoruje podivné inzeráty a brouzdá v kyberprostoru. Samotné vyšetřování kybernetické kriminality se dá rozvrhnout na dvě části. První část se dá rozdělit na pozorování, shromažďování a vyhodnocení získaných dat. Druhá část se zaměřuje na domovní prohlídku, ohledání informačních a komunikačních technologií, ohledání místa činu, výslechu obviněného, poškozených a svědků.[61]

5.4 Vyšetřovací situace kyberkriminality

Samotné vyšetřování kybernetické kriminality lze rozdělit do čtyřech typických vyšetřovacích situací. A to:

1. První typická kybernetická situace je založena na základě zjištěných skutečností, že byl spáchán čin, ve kterém je spatřována skutková podstata

[60] GŘIVNA, T.; POLČÁK, R, (eds.) *Kyberkriminalita a právo.* Praha: Auditorium. 2008. 86 s. ISBN 978-80-903786-7-4.
[61] GŘIVNA, T.; POLČÁK, R, (eds.) *Kyberkriminalita a právo.* Praha: Auditorium. 2008. 88 s. ISBN 978-80-903786-7-4.

trestného činu. Pachatel skutku není znám, jakožto i samotný způsob jeho provedení. V této situaci není potřeba znát způsobenou škodu ani motiv pachatele. Policejní orgán se při šetření této situace snaží zajistit veškeré informace, modus operandi, a to za účelem zjištění neznámého pachatele. V případě, že na základě iniciativy poškozené firmy byl již proveden rozbor napadeného cíle útoku, policejní orgán zažádá o revizní zprávu a vyzve k podání vysvětlení pracovníka, který provedl ohledání. Policejní orgán dále přibere znalce z oboru výpočetní techniky, který po odborné diskusi s policejním orgánem zajistí potřebný materiál k provedení kriminalistického odborného vyjádření. Pokud ještě nebyla ze strany poškozené firmy provedena analýza a nedošlo k prohlídce předmětu útoku, policejní orgán opět zajistí znalce z oboru výpočetní techniky, který provede ohledání a následně zajistí potřebný materiál k případné kriminalistické expertíze. Veškeré úkony musí být prováděny za účasti majitele poškozené firmy nebo jejich bezpečnostních kontrolních orgánů. Veškeré výše popsané skutečnosti jsou důležité pro zjištění informací a důkazů důležitých pro vyšetření, jakým způsobem byl útok proveden. Dále je nutné se zaměřit převážně na úzký okruh potenciálních pachatelů. Ve většině případů je třeba nalézt odpověď, kdo z útoku mohl získat prospěch.[62]

2. Druhá typická kriminalistická situace je založena na základě zjištěných skutečností, že byl spáchán skutek, ve kterém je spatřována skutková podstata trestného činu a je objasněn způsob, jak k němu došlo, pachatel však není znám. Opět jako v situaci č. 1 není potřeba znát výši způsobené škody ani není třeba znát motiv pachatele. V této situaci se policejní orgán kromě opatření důkazů objasňujících trestný čin v prvopočátku zaměřuje na skutečnosti odhalení neznámého pachatele. Okruh pachatelů je ve většině případů vymezen, a to právě způsobem jejich páchání. Důležitá je proto analýza za přítomnosti znalce z oblasti výpočetní techniky, která může vést k následnému vytipování možného pachatele. Policejní orgán

[62] PORADA, V. a kol. *Kriminalistika, Technické, forenzní a kybernetické aspekty.* Plzeň: Aleš Čeněk, 2016. 793 s. ISBN 978-807380-589-0.

dále spolupracuje s jinými orgány činnými v trestním řízení, a to zejména za účelem zjištění totožnosti pachatele.[63]

3. Třetí typická kriminalistická situace je založena na základě zjištěných skutečností, že byl spáchán skutek, ve kterém je spatřována skutková podstata trestného činu, lze vyslovit úsudek o pravděpodobném pachateli, ale není možné usoudit, jakým způsobem byla skutková podstata trestného činu naplněna. U této situace, jakožto i ve výše uvedených bodech, není důležité znát způsobenou škodu ani motiv. Policejní orgán při šetření této situace musí sdělit obvinění podezřelému a musí provést veškeré zajišťovací úkony, a to v kooperaci s přibranými znalci v oblasti výpočetní techniky, účetnictví apod. Na základě spolupráce dále policejní orgán stanoví kriminalistické verze, které mohou dopomoci k objasnění způsobu spáchání trestného činu. V této situaci je významným úkonem podání vysvětlení obviněného, výslech znalce nebo jiných expertů vedoucí k objasnění a dokazování způsobu spáchání trestného činu. V případě výslechu obviněného je třeba výslech předložit znalci z oboru výpočetní techniky, ke zjištění, zdali je vůbec popsaný způsob spáchání možný či nikoli. V případě, že obviněný odmítne výpověď, policejní orgán se zaměří na zajištění jiných důkazů důležitých k prokázání způsobu spáchání. Jako příklad důkazu lze uvést provedený vyšetřovací či expertizní experiment. V této situaci je již policejní orgán ve fázi dokazování, takže musí opatřovat veškeré důkazy, které mohou objasnit konkrétní skutkovou podstatu trestného činu.[64]

4. Čtvrtá typická kriminalistická situace je založena na základě zjištěných skutečností, že byl spáchán skutek, ve kterém je spatřována skutková podstata trestného činu, lze vyslovit úsudek o jeho pachateli a je objasněn pravděpodobný způsob trestného činu. Jako u výše předchozích není potřeba znát způsobenou škodu ani není třeba znát motiv pachatele. Tato situace je pro policejní orgán nejvýhodnější, jelikož na základě nashromážděných důkazů může sdělit obvinění pachateli. Nashromážděné

[63] PORADA, V. a kol. *Kriminalistika, Technické, forenzní a kybernetické aspekty.* Plzeň: Aleš Čeněk, 2016. 794 s. ISBN 978-807380-589-0.
[64] PORADA, V. a kol. *Kriminalistika, Technické, forenzní a kybernetické aspekty.* Plzeň: Aleš Čeněk, 2016. 794 s. ISBN 978-807380-589-0.

důkazy a informace předá k zajištění a vypracování expertizní činnosti v oboru výpočetní techniky, účetnictví atd. Dále policejní orgán vytýčí možné vyšetřovací verze o trestném činu a zaměří se na prokázání viny za protiprávní jednání pachatele.[65]

6 Praktická část

Empirická část práce je zaměřena na teritoriální výzkum pomocí kvantitativní metody dotazníkového šetření, který analyzuje připravenost a odborné znalosti příslušníků Policie České republiky, kteří jsou zařazeni na základních organizačních článcích pořádkové policie, a to služebny obvodních oddělení územních odboru Praha venkov – Východ a Nymburk v oblasti kybernetické kriminality.

6.1 Problematika práce

Většina příslušníků Policie České republiky zařazená na základních organizačních článcích pořádkové policie není dostatečně připravena a školena v oblasti kybernetické kriminality a s ní souvisejícími procesními úkony i přesto, že se s touto problematikou tito policisté často setkávají. Na základě zkušeností z praxe jsem se rozhodl pomocí teritoriálního výzkumu vyhodnotit nejen skutečnou odbornost policistů v kybernetické kriminalitě, ale také zájem o školení a vzdělávání se v této oblasti na zmíněných územních odborech.

6.2 Cíl práce

Teritoriálně analyzovat odborné znalosti a připravenost příslušníků Policie České republiky na stále vzrůstající hrozbu, kyberkriminalitu. Na základě vyhodnocení stanovit doporučení pro praxi.

[65] PORADA, V. a kol. *Kriminalistika, Technické, forenzní a kybernetické aspekty.* Plzeň: Aleš Čeněk, 2016. 795 s. ISBN 978-807380-589-0.

6.3 Hypotézy

H1: Policisté České republiky na základních organizačních článcích pořádkové policie nejsou dostatečně školení v oblasti kybernetické kriminality.

H2: Policisté České republiky na základních organizačních článcích pořádkové policie nejeví zájem o rozvíjení znalostí v oblasti kybernetické kriminality.

H3: Policisté České republiky na základních organizačních článcích pořádkové policie neradi vyšetřují případy spojené s kybernetickou kriminalitou.

6.4 Výzkumný vzorek

Kvantitativní výzkum práce byl osobně distribuován na konkrétní služebny Policie České republiky ve Středočeském kraji, na územní odbor Praha venkov – Východ, tedy na Obvodní oddělení policie Čelákovice (dále jen OOP), OOP Brandýs nad Labem, OOP Úvaly, OOP Odolena Voda. Dále na územní odbor Nymburk, tedy na OOP Milovice, OOP Nymburk, OOP Poděbrady a OOP Městec Králové. Dotazníkové šetření bylo určeno pro 125 policistů, kteří jsou zařazeni na výše uvedených útvarech Policie České republiky. Všichni respondenti byli předem informováni, že dotazník je zcela anonymní, dobrovolný a výsledky budou interpretovány pouze pro účely bakalářské práce. Kvantitativní šetření bylo určeno pro policisty v hodnosti od nadstrážmistr až do hodnosti nadpraporčík. Z výzkumného vzorku se dotazníkového šetření zúčastnilo 89 policistů a následně na základě odpovědi jsem dospěl k vyhodnocení, jenž interpretuji níže.

6.5 Výzkumná metodika

Výzkumná metodika práce byla provedena kvantitativní metodou s využitím dotazníkového šetření za pomoci uzavřených i jedné otevřené otázky. Pro lepší orientaci v bakalářské práci byly zpracovány grafy a tabulky, které znázorňují výsledky výzkumu. Dotazník obsahuje celkem 16 otázek strukturovaných pro dosažení výsledků a potvrzení či vyvrácení stanovených hypotéz.

6.6 Časový harmonogram

Dotazníkové šetření bylo osobně rozvezeno na služebny Územních odborů Policie České republiky Nymburk a Praha venkov – Východ, kde bylo ponecháno po dobu tří týdnů, aby měli dotazování policisté dostatečný čas pro jeho vyplnění.

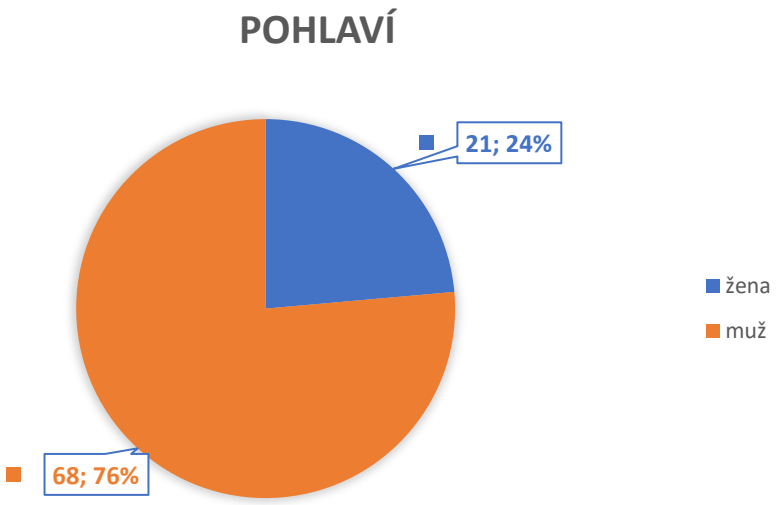
6.7 Interpretace výsledků bakalářské práce

Otázka č. 1 – Pohlaví účastníků dotazníkového šetření

Pohlaví	Absolutní četnost	Relativní četnost (%)
žena	21	24 %
muž	68	76 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 1- Pohlaví dotazovaných



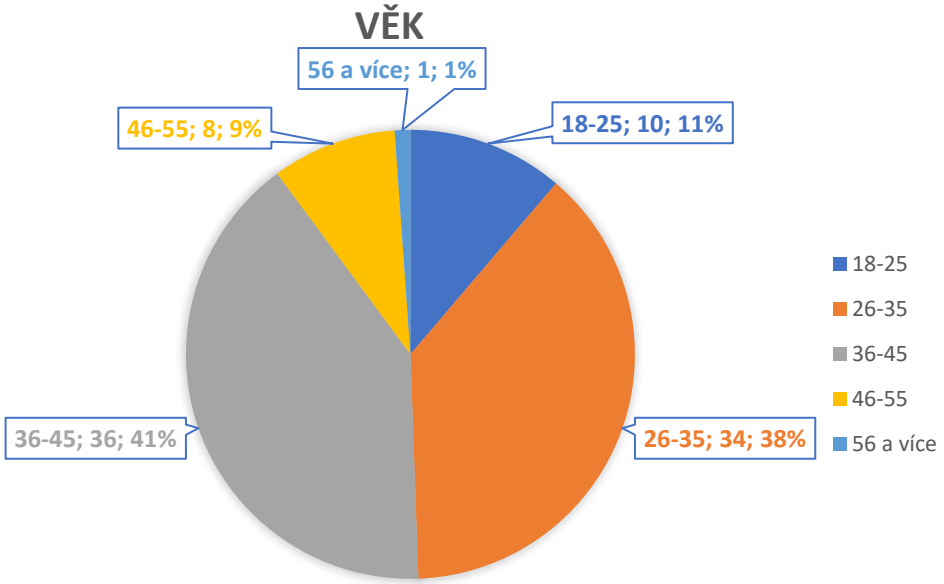
Na grafu č. 1 je zobrazeno pohlaví dotazovaných policistů, kdy následným zjištěním bylo vyhodnoceno, že dotazníkového šetření se zúčastnilo 68 mužů, což je 76 % dotazovaných a 21 žen, které tvoří zbylých 24 % dotazovaných.

Otázka č. 2 – Věkové rozpoložení respondentů

Věkové rozpoložení	Absolutní četnost	Relativní četnost (%)
18-25	10	11 %
26-35	34	38 %
36-45	36	41 %
46-55	8	9 %
56 a více	1	1 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 2 - Věk dotazovaných



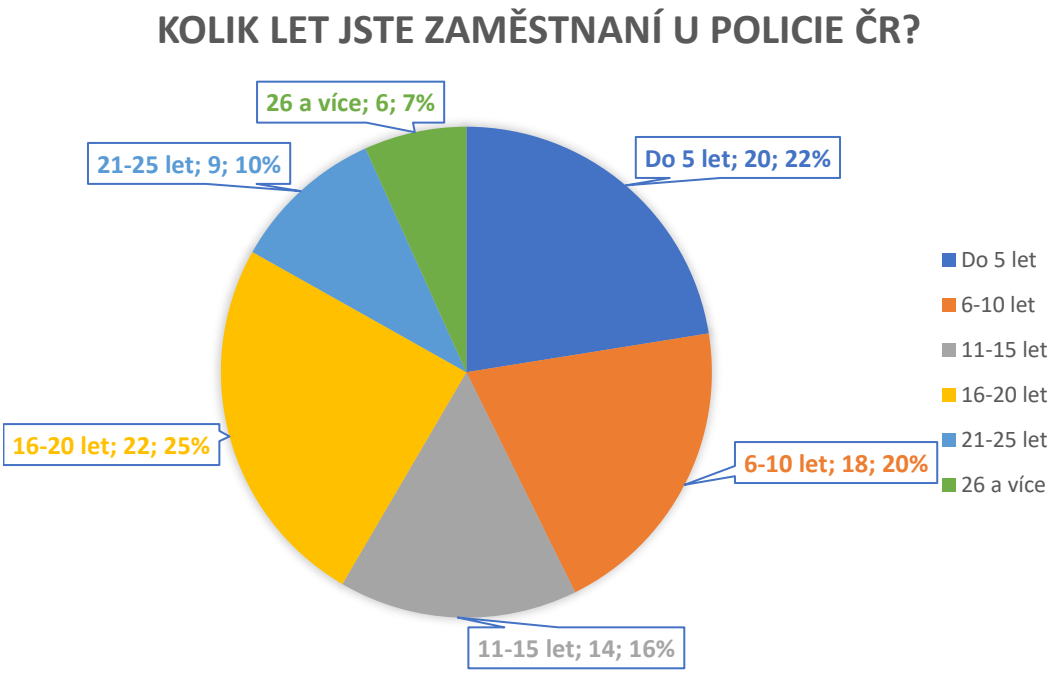
Graf č. 2 vyobrazuje věkové rozpoložení respondentů. Na základě vyhodnocení dotazníků bylo zjištěno, že dotazníkového šetření se nejvíce respondentů zúčastnilo ve věku mezi 36–45 let, což je 36 (41 %) dotazovaných. Dalšími nejvíce dotazovanými jsou respondenti ve věku od 26-35 lety, kterých odpovědělo 34 (38 %). Následuje věk respondentů od 18-25, kteří byli v zastoupení 10 (11 %) dotazovaných. Věk 46-55 tvoří 8 (9 %) dotazovaných. Nejméně respondentů zodpovědělo dotazník ve věku 56 a více, což byl 1 (1 %) respondent.

Otázka č. 3– Kolik let jste ve služebním poměru Policie České republiky?

Služba u Policie ČR	Absolutní četnost	Relativní četnost (%)
Do 5 let	20	22 %
6-10 let	18	20 %
11-15 let	14	16 %
16-20 let	22	25 %
21-25 let	9	10 %
26 a více	6	7 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 3 - Jak dlouho slouží respondenti u Policie ČR



Graf č. 3 zobrazuje, jak dlouho jsou jednotliví respondenti u Policie České republiky zaměstnáni ve služebním poměru. Vyhodnocením dotazníků bylo zjištěno, že nejvíce dotazovaných ve služebním poměru je od 16-20 lety, což je 22 (25 %) respondentů. Následně odpovídali respondenti do 5 let služby, což je 20 (22 %) respondentů. Poté odpovídali respondenti v tomto pořadí služby: 6-10 let 18 respondentů (20 %), 11-15 let 14 respondentů (16 %), 21-25 let 9 respondentů (10 %) a 26 a více let 6 respondentů (7 %).

Otázka č. 4 - Územní odbor, ve kterém jsou respondenti zařazeni

Územní odbor	Absolutní četnost	Relativní četnost (%)
Praha venkov – Východ	44	49 %
Nymburk	45	51 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 4 - Územní odbor respondentů

Graf č. 4 zobrazuje teritoriální rozložení respondentů podle územních odborů Policie České republiky. Vyhodnocením bylo zjištěno, že dotazníkového šetření se zúčastnilo 45 (51 %) respondentů z územního odboru Nymburk a 44 (49 %) respondentů z územního odboru Praha venkov – Východ.

Otázka č. 5 - Setkáváte se v práci s kybernetickou kriminalitou jako inzertní podvody, podvody se vzdáleným přístupem, podvodné e-maily, spam, m-platby, e-podvody atd.?

Styk s kyberkriminalitou	Absolutní četnost	Relativní četnost (%)
Ano	89	100 %
Ne	0	0 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 5 - Šetření respondentů v oblasti kybernetické kriminality

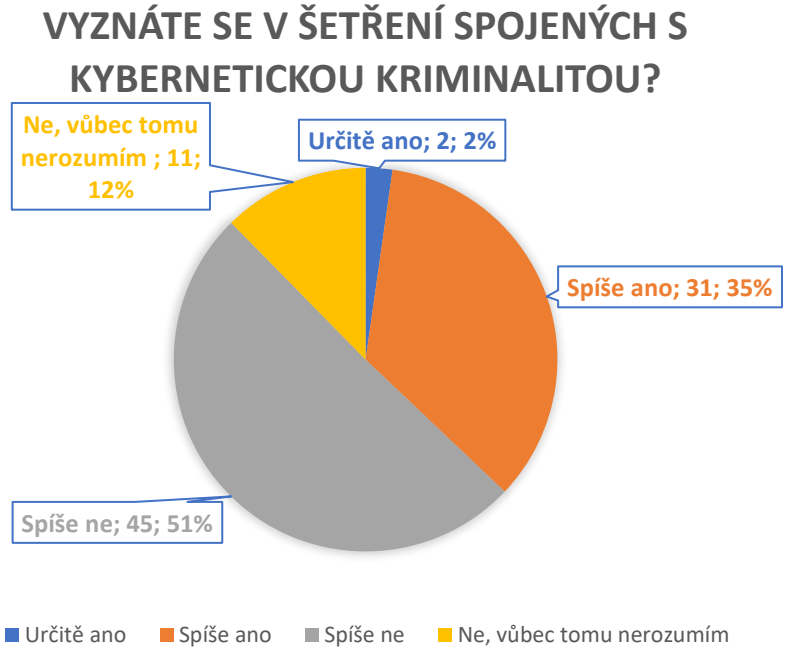
Graf č. 5 znázorňuje, že všichni z dotazovaných 89 (100 %) respondentů se ve svém zaměstnání setkává s kybernetickou kriminalitou.

Otázka č. 6 - Vyznáte se v šetření případů spojených s kybernetickou kriminalitou?

Znalost v šetření kyberkriminality	Absolutní četnost	Relativní četnost (%)
Určitě ano	2	2 %
Spíše ano	31	35 %
Spíše ne	45	51 %
Ne, vůbec tomu nerozumím	11	12 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 6 - Zkušenosti respondentů se šetřením kybernetické kriminality



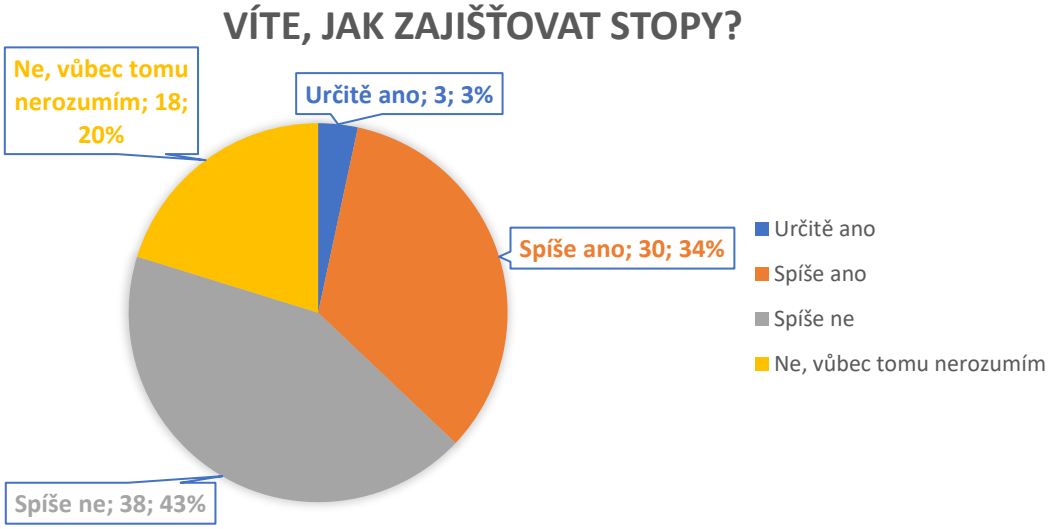
Graf č. 6 znázorňuje, jak se respondenti vyznají v šetření kybernetické kriminality. Vyhodnocením dotazníků bylo zjištěno, že nejvíce respondentů 45 (51 %) uvedlo, že se spíše nevyznají v šetření kybernetické kriminality. 31 (35 %) respondentů odpovědělo, že se spíše vyznají v šetření případů spojených s kybernetickou kriminalitou. Následně odpovědělo 11 (12 %) respondentů, že této problematické vůbec nerozumí a 2 (2 %) respondenti uvedli, že se určitě vyzná v šetření kybernetické kriminality.

Otázka č. 7 - Víte, jak zajišťovat kriminalisticky relevantní stopy v kyberprostoru?

Zajištění stop v kyberprostoru	Absolutní četnost	Relativní četnost
Určitě ano	3	3 %
Spíše ano	30	34 %
Spíše ne	38	43 %
Ne, vůbec tomu nerozumím	18	20 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 7 - Zda respondenti ví, jak zajišťovat kybernetické stopy



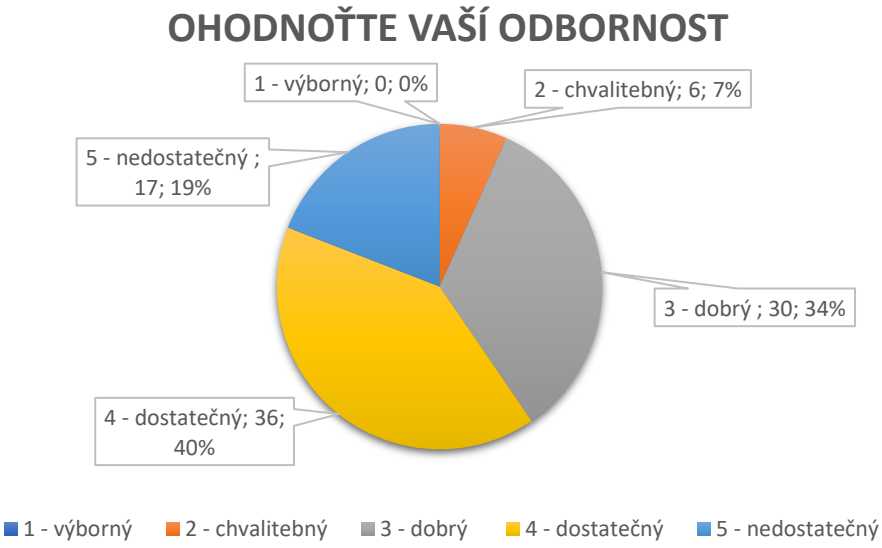
Graf č. 7 znázorňuje, zda jsou dotazovaní schopni zajistit kriminalisticky relevantní stopy v kyberprostoru. Vyhodnocením bylo zjištěno, že 38 (43 %) respondentů spíše neumí zajistit kriminalisticky relevantní stopy v kyberprostoru. Další ukazateli bylo zjištěno, že 30 (34 %) respondentů spíše ví, jak zajistit stopy v kyberprostoru, 18 (20 %) respondentů vůbec neví, jak zajistit tyto stopy a 3 (3 %) dotazovaných uvedlo, že ví, jak zajistit kriminalisticky relevantní stopy v kyberprostoru.

Otázka č. 8 - Na stupnici 1–5 ohodnoťte Vaši odbornost spojenou s kybernetickou kriminalitou a následnými procesními úkony

Vlastní odbornost	Absolutní četnost	Relativní četnost (%)
1 - výborný	0	0 %
2 - chvalitebný	6	7 %
3 - dobrý	30	34 %
4 - dostatečný	36	40 %
5 - nedostatečný	17	19 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 8 - Odbornost respondentů v oblasti kybernetické kriminality



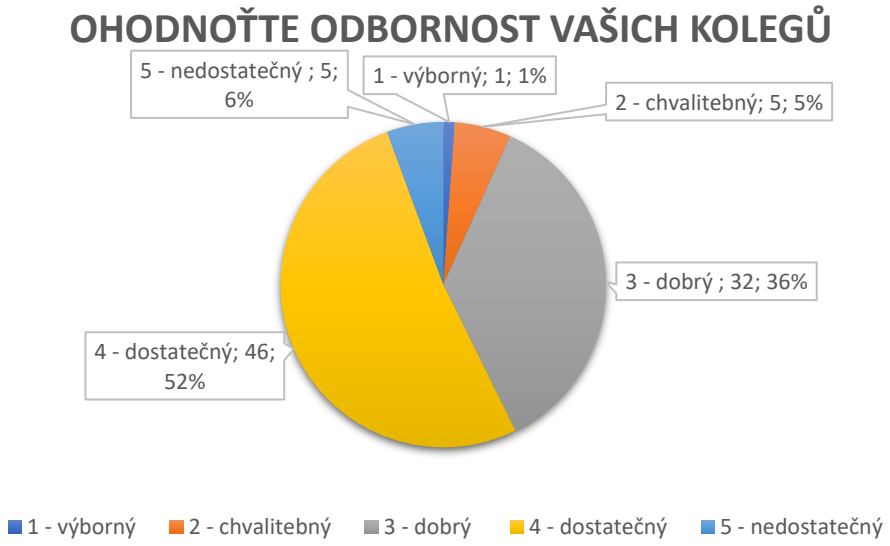
Graf č. 8 zobrazuje odbornost samotných dotazovaných spojenou s kybernetickou kriminalitou a jejími následnými procesními úkony. Odpovědi byly stanoveny podle klasifikace, která se užívá ve škole. Na základě odpovědí bylo zjištěno, že 36 (40 %) respondentů svoji odbornost stanovuje jako dostatečnou. Dále 30 (34 %) respondentů uvedlo, že jejich odbornost je dobrá. 17 (19 %) respondentů uvedlo, že jejich odbornost spojená s kybernetickou kriminalitou je nedostatečná. Chvalitebně se ohodnotilo 6 (7 %) respondentů. Nikdo z dotazovaných se neohodnotil známkou výborný.

Otázka č. 9 - Na stupnici 1-5 ohodnoťte odbornost Vašich kolegů na oddělení spojenou s šetřením kybernetické kriminality a následnými procesními úkony

Odbornost kolegů	Absolutní četnost	Relativní četnost (%)
1 - výborný	1	1 %
2 - chvalitebný	5	5 %
3 - dobrý	32	36 %
4 - dostatečný	46	52 %
5 - nedostatečný	5	6 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 9 - Odbornost kolegů respondenta v oblasti kybernetické kriminality



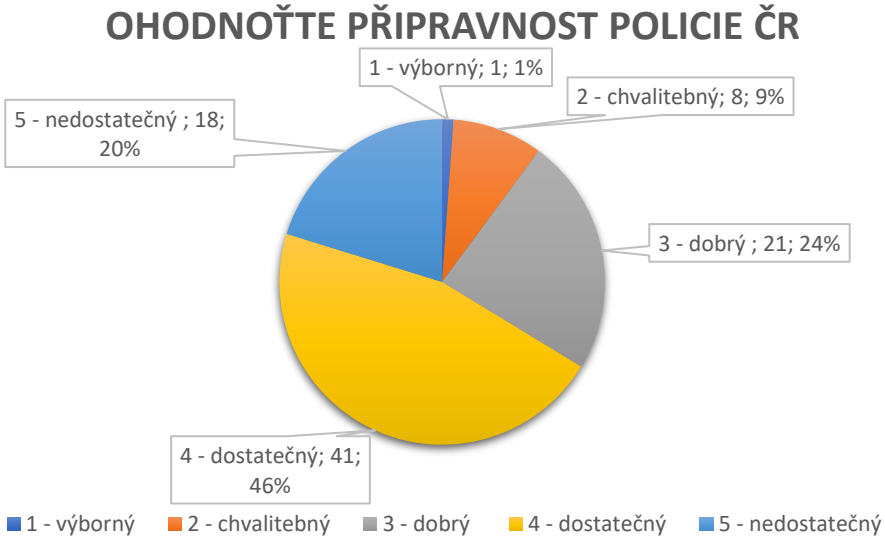
Graf č. 9 zobrazuje odbornost kolegů na oddělení dotazovaného spojenou s kybernetickou kriminalitou a jejími následnými procesními úkony. Odpovědi byly stanoveny podle klasifikace, která se užívá ve škole. Na základě vyhodnocení bylo zjištěno, že 46 (52 %) respondentů ohodnotilo odbornost svých kolegů na oddělení jako dostatečnou. 32 (36 %) respondentů ohodnotilo odbornost svých kolegů známkou dobrý. 5 (5 %) respondentů ohledně odbornosti svých kolegů na služebně ohodnotilo nedostatečnou známkou. Taktéž 5 (5 %) respondentů ohodnotilo odbornost svých kolegů jako chvalitebnou. Jeden respondent (1 %) uvedl, že jeho kolegové na oddělení jsou na tom s odborností okolo kybernetické kriminality na výborné úrovni.

Otázka č. 10 - Na stupnici 1-5 ohodnoťte připravenost Policie České republiky na úrovni obvodních oddělení Policie České republiky spojenou s šetřením kybernetické kriminality a následnými procesními úkony

Připravenost Policie ČR	Absolutní četnost	Relativní četnost (%)
1 - výborný	1	1 %
2 - chvalitebný	8	9 %
3 - dobrý	21	24 %
4 - dostatečný	41	46 %
5 - nedostatečný	18	20 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 10 - Připravenost Policie ČR v oblasti kybernetické kriminality dle respondentů



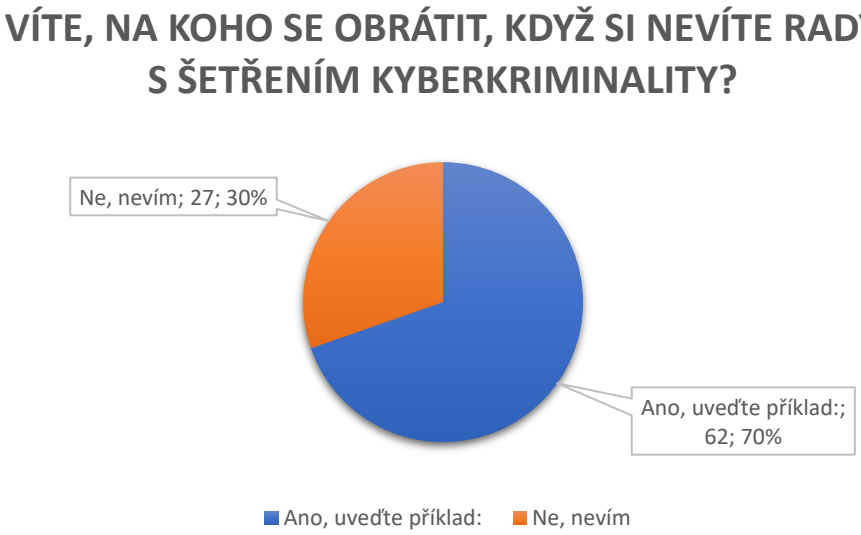
Na grafu č. 10 je vyobrazena připravenost Policie České republiky na úrovni obvodního oddělení spočívající s problematikou kybernetické kriminality dle respondentů. Odpovědi byly stanoveny podle klasifikace, která se užívá ve škole. Vyhodnocením bylo zjištěno, že 41 (46 %) dotazovaných uvedlo, že vnímá připravenost Policie České republiky na úrovni obvodních oddělení jako dostatečnou. 21 (24 %) respondentů uvedlo, že vnímá připravenost jako dobrou. 18 (20 %) respondentů vnímá připravenost známkou nedostatečný. 8 (9 %) respondentů uvedlo, že hodnotí připravenost chvalitebně a jeden (1 %) respondent uvedl, že vnímá připravenost známkou výborně.

Otázka č. 11 - Víte, na který orgán se obrátit v případě, že si nevíte s řešením případu v oblasti kybernetické kriminality rady?

Pomoc při šetření	Absolutní četnost	Relativní četnost (%)
Ano, uveďte příklad:	62	70 %
Ne, nevím	27	30 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 11 - Znalost respondentů, na koho se mají obrátit o radu v šetření kybernetické kriminality



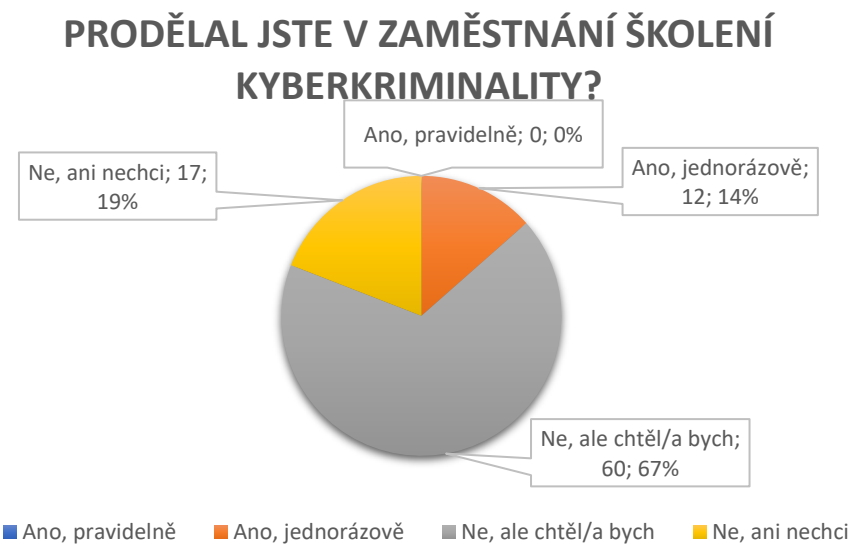
Graf č. 11 poukazuje na to, jak jsou policisté informováni o tom, na koho se mají obrátit v případě, že si neví rady se šetřením kybernetické kriminality. Jedná o otevřenou otázku. Po zaškrtnutí odpovědi ano, měl respondent uvést příklad, na jaký útvar se může obrátit. Na základě vyhodnocení bylo zjištěno, že 62 (70 %) respondentů ví, na jaký orgán Policie České republiky se obrátit. Ve většině příkladů byla uvedena služba kriminální policie a vyšetřování, oddělení analytiky a kybernetické kriminality daných územních odborů. Dále jako příklady byly uváděny hospodářské kriminální služby územních odborů. Následně bylo uváděno krajská služba kriminální policie a vyšetřování, oddělení kybernetické kriminality. Dále bylo z dotazníkového šetření zjištěno, že 27 (30 %) respondentů neví, na jaký orgán Policie České republiky se obrátit v případě, že si neví rady s řešením kybernetické kriminality.

Otázka č. 12 - Prodělal/a jste v zaměstnání školení v oblasti kybernetické kriminality?

Školení v oblasti kyberkriminality	Absolutní četnost	Relativní četnost (%)
Ano, pravidelně	0	0 %
Ano, jednorázově	12	14 %
Ne, ale chtěl/a bych	60	67 %
Ne, ani nechci	17	19 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 12 - Školení v oblasti kybernetické kriminality dle respondentů



Graf č. 12 je vyobrazeno, jak jsou či byli policisté školení v zaměstnání v oblasti kybernetické kriminality. Na základě vyhodnocení bylo zjištěno, že 60 (67 %) nebylo v zaměstnání školeno v oblasti kybernetické kriminality, ale respondenti by o takového školení měli zájem. Z toho 17 (19 %) uvedlo, že školeno nebylo, ani by nechtělo být školeno v popisované problematice. 12 (14 %) respondentů uvedlo, že v zaměstnání bylo školeno v oblasti kybernetické kriminality pouze jednou. Dále bylo zjištěno, že žádný (0 %) z dotazovaných respondentů není školen pravidelně v problematice spojené s kybernetickou kriminalitou.

Otázka č. 13 - Vzděláváte se mimo zaměstnání sami s problematikou spojenou s kybernetickou kriminalitou?

Vzdělávání mimo zaměstnání s kyberkriminalitou	Absolutní četnost	Relativní četnost (%)
Ano, čerpám z odborných zdrojů	17	19 %
Ne, nevzdělávám se	72	81 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 13 - Vzdělávání v kybernetické kriminalitě mimo zaměstnání

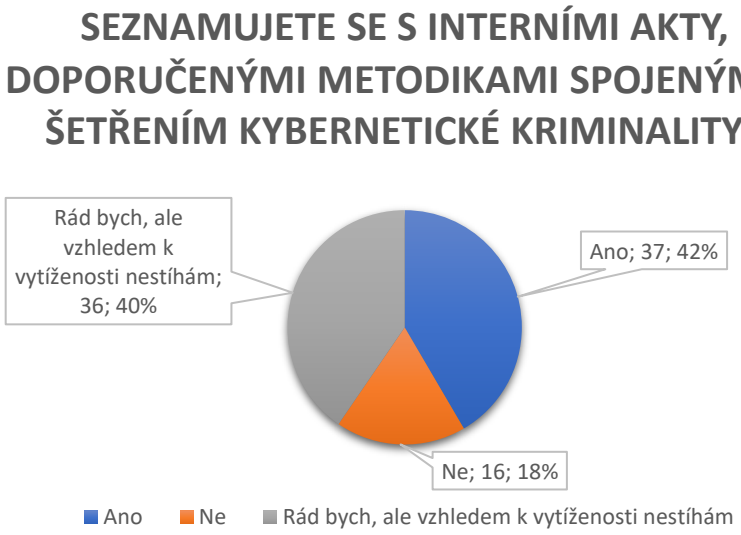
Na grafu č. 13 vyobrazuje vzdělávání respondentů mimo zaměstnání spojenou s kybernetickou kriminalitou. Na základě vyhodnocení bylo zjištěno, že 72 (81 %) respondentů se v této problematice nevzdělává vůbec mimo zaměstnání a 17 (19 %) respondentů uvedlo, že se mimo zaměstnání sama vzdělává.

Otázka č. 14 - Seznamujete se pravidelně s interními akty řízení, doporučenými metodikami spojenými s šetřením kybernetické kriminality?

Seznamujete se s metodikami a akty řízení	Absolutní četnost	Relativní četnost (%)
Ano	37	42 %
Ne	16	18 %
Rád bych, ale vzhledem k vytíženosti nestíhám	36	40 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 14 - Zda se respondenti seznamují s metodikami v oblasti kybernetické kriminality



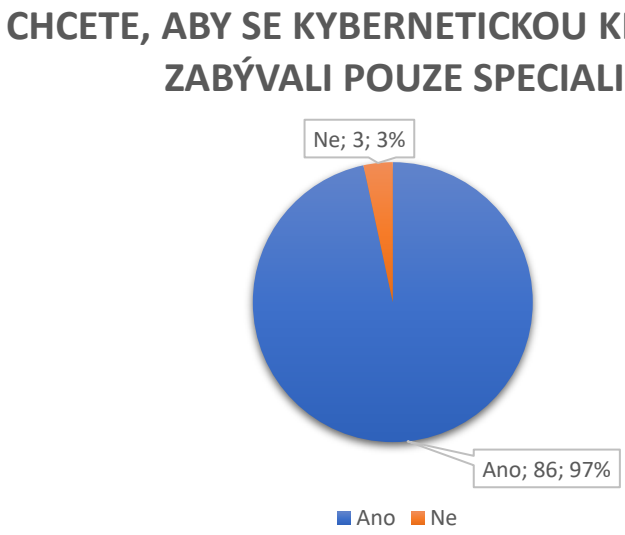
Na grafu č. 14 je zobrazeno seznamování se respondentů s interními akty řízení a metodikami spojenými s šetřením kybernetické kriminality. Na základě vyhodnocení bylo zjištěno, že 37 (42 %) respondentů se seznamuje s interními akty řízení a doporučenými metodikami, 36 (40 %) respondentů by se rádo seznamovalo s metodikami a interními akty, ale vzhledem k vytíženosti v práci nestíhají a 16 (18 %) respondentů se neseznamuje s metodikami a interními akty řízení související s kybernetickou kriminalitou.

Otázka č. 15 - Chtěli byste, aby se oblasti kybernetické kriminality zabývali pouze na to odborně školení specialisté?

Odborně vyškolení specialisté	Absolutní četnost	Relativní četnost (%)
Ano	86	97 %
Ne	3	3 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 15 - Zda respondenti chtějí, aby se kybernetickou kriminalitou zabývali pouze specialisté



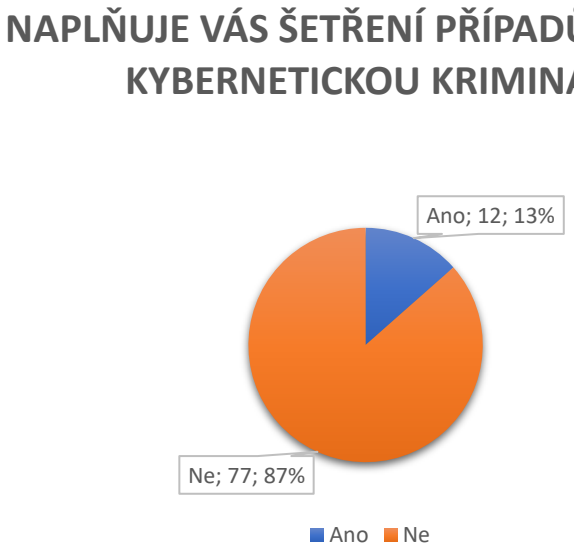
Na grafu č. 15 jsou znázorněny odpovědi respondentů, kteří byli dotazováni na to, zda by uvítali, aby se kybernetickou kriminalitou zabývali na to odborně vyškolení specialisté. Na základě vyhodnocení bylo zjištěno, že 86 (97 %) respondentů by to uvítalo a oproti tomu byli 3 (3 %) respondentů, kteří by si vystačili sami.

Otázka č. 16 - Naplňuje Vás šetření případů spojených s kybernetickou kriminalitou?

Šetření kyberkriminality	Absolutní četnost	Relativní četnost (%)
Ano	12	13 %
Ne	77	77 %
Celkem	89	100 %

Zdroj: autor práce, 2022 (vlastní šetření)

Graf 16 - Zda respondenty naplňuje šetření kybernetické kriminality



Na grafu č. 16 je vyobrazení, zda respondenty naplňuje šetření případů spojených s kybernetickou kriminalitou. Na základě výsledků bylo zjištěno, že 77 (87 %) respondentů nenaplňuje šetření případů kybernetické kriminality a 12 (13 %) respondentů naplňuje takovéto šetření.

7 Shrnutí výsledku výzkumu

Empirický výzkum byl proveden za pomocí kvantitativní metody. Ke sběru potřebných dat byl užit dotazník, na který dotazovaní policisté odpovídali zcela anonymně a dobrovolně. Na základě analýzy dotazníkového šetření byly stanovené hypotézy potvrzeny či vyvráceny.

H1: Policisté České republiky na základních organizačních článcích pořádkové policie nejsou dostatečně školení v oblasti kybernetické kriminality. (Data jsou použita z odpovědí 5, 6, 7, 8, 9, 10, 11)

Na základě analýzy samotného dotazníku bylo zjištěno, že všech 89 zúčastněných respondentů dle otázky č. 5 se v práci setkává s kybernetickou kriminalitou, tzn. v těchto věcech by měli respondenti provádět úkony spojené s šetřením či prověřováním tohoto druhu kriminality tak, aby mohla být skutková podstata přestupku či trestného činu řádně objasněna. Následně byli v dotazníku v otázce č. 6 respondenti dotazováni, jak se vyznají dle subjektivního pocitu v oblasti šetření případů spojených s kybernetickou kriminalitou. Na základě vyhodnocení bylo zjištěno, že 56 respondentů, což je 63 %, uvedlo, že se spíše nevyznají nebo se vůbec neorientují v šetření spojené s kyberkriminalitou a naopak 33 respondentů 37 % uvedlo, že se spíše vyznají nebo se určitě vyznají v šetření předmětné problematiky. Další otázka č. 7 byla směřována na to, zda respondenti ví, jak zajišťovat kriminalisticky relevantní stopy v kyberprostoru. Na základě vyhodnocení bylo zjištěno, že 56 respondentů, což je opět 63 % uvedlo, že spíše neví nebo vůbec neví, jak zajišťovat kriminalisticky relevantní stopy v kyberprostoru a naopak 33 respondentů 37 % spíše ví nebo určitě ví, jak tyto stopy zajišťovat. Další otázka č. 8 k vyvrácení či potvrzení H1 byla směřována na subjektivní ohodnocení respondenta, co se týče jeho odbornosti spojené s kybernetickou kriminalitou a s ní spojenými procesními úkony. Hodnocení této otázky bylo stanoveno stupnici od 1-5, tedy jako ve škole. Na základě vyhodnocení bylo zjištěno, že žádný z respondentů se neohodnotil v odbornosti spojenou s kybernetickou kriminalitou známkou 1 (0 %), známkou 2 se ohodnotilo 6 (7 %) respondentů, známkou 3 se ohodnotilo 30 (34 %) respondentů, známkou 4 se ohodnotilo 36 (40 %) respondentů a známkou 5 se ohodnotilo 17 (19 %) respondentů. Otázka č. 9 byla cílena na subjektivní ohodnocení respondenta, co se týče odbornosti jeho kolegů na oddělení spojených

s kybernetickou kriminalitou a následnými procesními úkony. Hodnocení této otázky bylo stanoveno jako u předchozí otázky, tedy známkou 1-5. Samotným vyhodnocením bylo zjištěno, že jeden (1 %) respondent si cení známkou 1 odbornosti svých kolegů na oddělení spojenou s kyberkriminalitou. Známkou 2 odpovídalo 5 (5 %) respondentů, známku 3 uvedlo 32 (36 %) respondentů, známku 4 uvedlo 46 (52 % respondentů) a 5 (6 %) respondentů si cení práci svých kolegů spojenou s kyberkriminalitou známkou 5. Následnou otázkou č. 10 bylo cíleno na předchozí otázky, kde byli respondenti dotazování, jak hodnotí připravenost Policie České republiky na úrovni obvodních odděleních spojených s šetřením kybernetické kriminality a následnými procesními úkony. Hodnocení této otázky bylo stanoveno jako u předchozí otázky. Vyhodnocením bylo zjištěno, že známkou jedna odpověděl 1 (1 %) respondent, tudíž předpokládá, že Policie České republiky je na tom výborně s připraveností policistů zařazených na obvodních odděleních Policie České republiky s problematikou kyberkriminality. Známkou 2 ohodnotilo připravenost 8 (9 %) respondentů, známkou 3 hodnotilo 21 (24 %) respondentů), známku 4 uvedlo 41 (46 %) respondentů a známkou 5 hodnotilo 18 (20 %) respondentů. Další otázka č. 11 byla směřována na respondenty ohledně toho, zda při šetření kybernetické kriminality ví, na koho se obrátit v případě, že si neví rady s touto problematikou. Odpovědi této otázky byly „Ne, nevím“ a jedna otevřená odpověď „Ano vím, uveďte příklad“. Vyhodnocením otázky bylo zjištěno, že 27 (30 %) respondentů uvedlo, že neví, na koho se obracet v případě šetření problematiky spojené s kybernetickou kriminalitou a 62 (70 %) respondentů uvedlo, že ví, na koho se obrátit. Tato odpověď byla otevřená, respondenti převážně odpovídali, že při šetření kybernetických případů se převážně obracejí na oddělení analytiky a kybernetické kriminality, které působí na územním odboru respondenta. Dále se obracejí na policisty (specialisty) zařazených na oddělení kybernetické kriminality na krajských ředitelstvích Středočeského kraje a na Útvar zvláštních činností Policie České republiky. Další otázka č. 12, která mohla vyvrátit či potvrdit H1 byla směřována na respondenty, zda prodělali v zaměstnání školení v oblasti kybernetické kriminality. Na základě vyhodnocení bylo zjištěno, že ani jeden respondent (0 %) se v zaměstnání pravidelně neškolí v oblasti kybernetické kriminality. 12 (14 %) respondentů uvedlo, že v zaměstnání se účastnilo školení jednorázově, 60 (67 %) respondentů uvedlo, že se v zaměstnání nikdy neúčastnili žádného školení, ale rádi by se v této problematice školili a 17 (19 %) respondentů uvedlo, že v zaměstnání nikdy školeni nebyli, ani by o školení zájem neměli.

Hypotéza H1 byla vyhodnocena na základě výše uvedených výsledků. Dotazníkovým šetřením bylo zjištěno, že většina respondentů vnímá odbornost policistů zařazených na základních organizačních článcích pořádkové policie České republiky negativně. Při samotném šetření případů spojených s kybernetickou kriminalitou respondenti ve většině ví, na koho se obrátit v případě, že si neví rady. Pouze necelá 1/5 respondentů byla v zaměstnání školena v oblasti kybernetické kriminality. Na základě uvedeného bylo konstatováno, že hypotéza (H1) „Policisté České republiky na základních organizačních článcích pořádkové policie nejsou dostatečně školení v oblasti kybernetické kriminality“ se potvrzuje.

H2: Policisté České republiky na základních organizačních článcích pořádkové policie nejeví zájem o rozvíjení znalostí v oblasti kybernetické kriminality. (Data jsou použita z odpovědí 12, 13, 14)

Na základě vyhodnocení otázky č. 12 viz. předchozí H1 bylo zjištěno, že většina respondentů sice nebyla v zaměstnání školena s problematikou spojenou s kybernetickou kriminalitou, ale respondenti z větší části tedy 60 (67 %) by měli o školení zájem a 12 (14 %) respondentů již bylo školeno alespoň jednorázově. Pouze 17 (19 %) respondentů nejeví zájem o školení, tedy o rozvíjení znalostí v oblasti kybernetické kriminality. Další otázka č. 13 byla cílena na respondenty, zda se mimo zaměstnání sami vzdělávají s problematikou spojenou s kybernetickou kriminalitou. Šetřením bylo zjištěno, že pouze 17 (19 %) respondentů se mimo zaměstnání vzdělává v oblasti kybernetické kriminality a 72 (81 %) respondentů nikoli. Otázkou č. 14 byli respondenti dotazováni, zda se pravidelně seznamují s interními akty řízení, doporučenými metodikami spojenými s šetřením kybernetické kriminality. Vyhodnocením bylo zjištěno, že 37 (42 %) respondentů se seznamuje s interními akty, metodikami spojenými s šetřením kybernetické kriminality. 36 (40 %) respondentů by se rádo seznamovalo, ale vzhledem k enormní vytíženosti v zaměstnání nestíhají a pouze 16 (18 %) respondentů uvedlo, že se neseznamují vůbec.

Hypotéza H2 se opírá o výše uvedené otázky. Na základě vyhodnocení bylo konstatováno, že respondenti mají ve většině zájem o školení, tudíž zájem o rozvíjení znalostí v oblasti kybernetické kriminality ve svém zaměstnání. Taktéž bylo zjištěno, že většina respondentů se seznamuje nebo by se alespoň chtěla seznamovat s interními akty řízení, doporučenými metodikami spojenými s kybernetickou kriminalitou. Většina respondentů nejeví zájem o rozvíjení znalostí v oblasti kybernetické kriminality mimo

zaměstnání. Na základě výše lze konstatovat, že hypotéza (H2) „Policisté České republiky na základních organizačních článcích pořádkové policie nejeví zájem o rozvíjení znalostí v oblasti kybernetické kriminality“ se nepotvrzuje, jelikož respondenti jeví zájem o rozvíjení znalostí v této problematice, avšak v zaměstnání.

H3: Policisté České republiky na základních organizačních článcích pořádkové policie neradi vyšetřují případy spojené s kybernetickou kriminalitou. (Data jsou použita z odpovědí 15, 16)

Otázka č. 15 byla směřována na respondenty, zdali by chtěli, aby se oblasti kybernetické kriminality zabývali pouze na to odborně školení specialisté. Vyhodnocením této otázky bylo zjištěno, že většina respondentů, tedy 86 (97 %) by chtěla, aby se problematice kybernetické kriminality zabývali pouze na to odborně školení specialisté a 3 (3 %) respondenti uvedli, že nechtějí, aby se kybernetickou kriminalitou zabývali specialisté. Dále v otázce č. 16 bylo na respondenty cíleno, zda je naplňuje šetření případů spojených s kybernetickou kriminalitou. Na základě vyhodnocení bylo zjištěno, že 77 (87 %) respondentů toto šetření nenaplňuje a pouze 12 (13 %) respondentů šetření naplňuje.

Hypotéza H3 je vyhodnocována z výše uvedených výsledků. Vyhodnocením bylo zjištěno, že respondenti chtějí, aby se problematikou spojenou s kyberkriminalitou zabývali na to odborně školení specialisté. Dále respondenty ve větší míře nenaplňuje šetření případů spojených s kybernetickou kriminalitou. Na základě toho lze konstatovat, že hypotéza (H3) „Policisté České republiky na základních organizačních článcích pořádkové policie neradi vyšetřují případy spojené s kybernetickou kriminalitou“ se potvrzuje.

7.1 Shrnutí praktické části

Praktická část byla zaměřena na dotazníkovém šetření, které mělo za úkol teritoriálně zmapovat, jak jsou příslušníci na základních organizačních článcích policie České republiky seznamování či školení s problematikou kybernetické kriminality. Šetření se zaměřilo na příslušníky Policie České republiky s teritoriálním umístěním na Praze venkov – Východ a s teritoriálním umístěním Nymburk. Data dotazníkového šetření by mohla být užita jako základ pro návrhy a doporučení pro využití praxe do budoucnosti. Samotnou analýzou dat bylo zjištěno, že všichni policisté se ve svém

zaměstnání setkávají s jakýmkoli druhem kybernetické kriminality. Už po tomto zjištění by bylo možno se domnívat, že odbornost policistů v tomto duhu popisované kriminality je na dobré úrovni, a to vzhledem k tomu, že s tímto druhem kriminality se policisté setkávají a vzhledem ke vzrůstající tendenci kybernetické kriminality setkávat budou. Z dotazníkového šetření vyplynulo, že se více než polovina policistů, tedy 63 %, nevyzná v šetření případů spojených s kybernetickou kriminalitou. Dále je z dotazníkového šetření patrné, že větší polovina tedy 63 % policistů neví, jak zajišťovat kriminalisticky relevantní stopy v kyberprostoru. Dalším negaci z dotazníku lze shledat v samotném ohodnocení odbornosti samotných policistů, kdy 59 % policistů hodnotí svoji odbornost spojenou s kybernetickou kriminalitou na úrovni dostatečný a nedostatečný. Taktéž negaci lze shledat v odbornosti kolegů na služebně, kdy 58 % policistů uvedlo, že jejich kolegové na oddělení mají odbornost v kybernetické kriminalitě na úrovni dostatečný, nedostatečný. Další negativní prvek lze shledat v tom, že 66 % policistů hodnotí připravenost Policie České republiky na úrovni základních organizačních článků policie dostatečně, nedostatečně. Jako pozitivum lze uvést, že policisté z 70 % ví, na koho se obrátit v případě, že si neví rady s šetřením spojeným s kybernetickou kriminalitou. Další negativní prvek lze shledat v tom, že policisté zařazení na základních organizačních článcích Policie České republiky z 86 % nejsou školení v popisované problematice. Z toho je třeba uvést kladný poznatek v tom, že z toho 67 % policistů má zájem o školení v dané problematice, pokud by nějaké bylo. Jako kladné zjištění je třeba uvést i to, že alespoň 19 % policistů mimo zaměstnání rozvíjí své znalosti v předmětné problematice. Další pozitivum je skutečnost, že policisté z 82 % dotazovaných se seznamuje nebo by se chtělo seznamovat s interními akty řízení a doporoučenými metodikami spojenými s kybernetickou kriminalitou. Z dotazníkového šetření bylo dále zjištěno, že většina tedy 97 % policistů by chtěla, aby se případy spojenými s kybernetickou kriminalitou věnovali pouze na to odborně školení policisté. Dalším v celku jasným zjištěním bylo to, že policisty z 87 % nenaplňuje šetření případů spojených s kybernetickou kriminalitou.

7.2 Doporučení pro praxi

Z teritoriálního výzkumu vyplynulo, že příslušníci Policie České republiky zařazení na základním organizačním článku pořádkové policie nejsou dostatečně školení v oblasti kybernetické kriminality. Dotazníkovým šetření však bylo zjištěno, že většina

policistů na předmětných útvarech jeví o vzdělávání v oblasti kybernetické kriminality zájem, nedostává se jim však dostatečného školení, které by napomohlo k jejich další orientaci v této problematice. Na základě provedeného výzkumu lze doporučit vedení Policie České republiky, aby zajistilo pro příslušníky zařazených na základních organizačních článcích Policie České republiky dostatečné školení, jelikož právě policisté zařazeni na základních organizačních článcích pořádkové policie se s touto problematikou setkávají téměř denně a vzhledem ke vzrůstající tendenci tohoto druhu trestné činnosti se s ní setkávat budou i nadále. Toto by mohlo napomoci ke zkvalitnění vyšetřování a větší objasněnosti trestných činů spojených s kyberkriminalitou. Další možností je využít na šetření kyberkriminality pouze na to odborně vyškolené policisty, kteří by se zabývali pouze vyšetřováním kybernetické kriminality, což by vedlo k větší efektivitě v předmětné problematice, a tím by se mohli ostatní policisté na odděleních věnovat problematice, kterou z praxeologického hlediska znají, než relativně novou popisovanou trestnou činnost, ve které se musí sami zdokonalovat.

Závěr

Bakalářská práce byla vypracována v souladu se stanovenými cíli a vznikla na základě vlastní zkušenosti z praxe, kdy se autor práce rozhodl prozkoumat, jak jsou policisté České republiky zařazeni na základních organizačních článcích pořádkové policie proškolováni v oblasti kybernetické kriminality. V praxi často vyplývalo, že policisté nejsou v této oblasti dostatečně školeni a neví si s řešením případů spojených s kyberkriminalitou rady. Proto se autor práce rozhodl teritoriálně prověřit i ostatní kolegy, jaké mají znalosti v tomto oboru.

Hlavním cílem praktické části je tedy empirický výzkum za pomocí dotazníkového šetření, který teritoriálně analyzuje odborné znalosti a připravenost příslušníků Policie České republiky zařazených na základních organizačních článcích pořádkové policie. V rámci dotazníkového šetření byly předem stanoveny tři hypotézy, díky jejichž vyhodnocení se dospělo k závěru, že policisté České republiky nejsou dostatečně školeni v oblasti kybernetické kriminality, přestože mají o vzdělávání v této oblasti zájem. Po vyhodnocení hypotéz, bylo sepsáno doporučení pro praxi, které by napomohlo zlepšit efektivnost při vyšetřování případů spojených s kybernetickou kriminalitou. Dle dat z výzkumu autor práce doporučuje vedení Policie České republiky, aby dostatečně zaškolilo pracovníky pořádkové policie či zajistilo specialisty, kteří by se touto problematikou zabývali. Policisté by tento krok dle dotazníkového šetřeni uvítali, jelikož si v mnoha případech s šetřením neví rady a napomohlo by to k větší efektivitě řešení případů spojených s kybernetickou kriminalitou i k možné lepší objasněnosti případů.

Teoretická část bakalářské práce se také zaměřuje na seznámení s vybranými pojmy, projevy a formami kybernetické kriminality v oblasti majetkových trestných činů. Práce se zároveň zabývá vybranými kybernetickými útoky orientující se na majetek, jejich odhalování a vyšetřování. Bakalářská práce se opírá o odbornou českou a zahraniční literaturu, která pojednává o kybernetické kriminalitě.

Seznam použitých zdrojů

Literární zdroje

1. GŘIVNA, T.; POLČÁK, R, (eds.) *Kyberkriminalita a právo.* Praha: Auditorium. 2008. 220 s. ISBN 978-80-903786-7-4.
2. JELÍNEK, J. GŘIVNA, T. POLČÁK, R. *Kybernetická kriminalita.* 1. vyd. Praha 2013. 120 s. ISSN 0323-0619.
3. JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualizované. Vydání. Praha: AFCEA, 2015. 262 s. ISBN 978-80-7251-397-0. Dostupné z: https://cybersecurity.cz/data/slovnik_v310.pdf
4. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha. 288 s. ISBN: 978-80-247-1766-1.
5. KLIMEK, L. ZÁHORA, J., HOLCR, K. *POČÍTAČOVÁ KRIMINALITA v európskych súvislostiach*. 2016. Bratislava. Wolters Kluwer s.r.o. 448 s. ISBN: 978-80-8168-5358-5.
6. KONRÁD, Z.; PORADA, V.; STRAUS, J.; SUCHÁNEK, J. *Kriminalistika. Kriminalistická taktika a metodiky vyšetřování.* Plzeň: Aleš Čeněk, 2015. 414 s. ISBN: 978-80-7380-547-0.
7. KONRÁD, Z.; PORADA, V.; STRAUS, J.; SUCHÁNEK, J. *Kriminalistika, Teorie, metodologie a metody kriminalistické techniky.* Plzeň: Aleš Čeněk, 2014. 318 s. ISBN 978-80-7380-535-7.
8. KOLOUCH, J., BAŠTA a kol. *CyberSecurity*. 1. vyd. Praha 2019: CZ.NIC, z. s. p. o. 560 s. ISBN 978-80-88168-31-7.
9. KOLOUCH, J. *CyberCrime*. 1. vyd. Praha: CZ.NIC, z. s. p. o. 524 s. ISBN 978-80-88168-15-7.
10. PAČKA, R. *CSIRT: v přední linii boje proti kybernetickým hrozbám.* 1. vydání- Brno 2019. 132 s. ISBN: 978-80-7325-473-5.
11. POLČÁK, R. a kol. *Právo informačních technologií.* Praha: Wolters Kluwer ČR, 2018, 656 s. ISBN: 978-80-7598-045-8 (váz.)
12. PORADA, V. a kol. *Kriminalistika, Technické, forenzní a kybernetické aspekty.* Plzeň: Aleš Čeněk, 2016. 1024 s. ISBN 978-807380-589-0.
13. RYAN, J. *A HISTORY OF THE INTERNET AND THE DIGITAL FUTURE*. 1. papírové vyd. 2013. London. 248 s. ISBN 978-1-78023-112-9

14. ŠKODA, J.; VAVERA, F.; ŠMERDA, R. *Zákon o policii s komentářem.* 2. vyd. Plzeň: Aleš Čeněk, 2013. 479 s. ISBN 978-80-7380-447-3.
15. SMEJKAL, V. *Kybernetická kriminalita*, 2. vyd. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.
16. ŠULC, V. *Kybernetická bezpečnost.* Plzeň: Aleš Čeněk, 2018, 147 s. ISBN 978-80-7380-737-5.
17. ZAVRŠNIK, A. *Kyberkriminalita*. Praha: Wolters Kluwer ČR, 2017. 148 s. ISBN 978-80-7552-759-2.

Elektronické zdroje

1. HACKERS LEAGUE BOOKS. *WhatisSurface Web, Deep Web and Dark Web?* [online]. [cit. 2022-01-29]. Dostupné z: https://medium.com/@hackersleaguebooks/what-is-surface-web-deep-web-anddark-web-cdbaf71b30d5
2. Internet a jeho služby: Historie internetu. [online]. [cit. 2022-01-11]. Dostupné z: http://ijs.8u.cz/index.php/internet/historie-internetu
3. KASÍK, P., iDNES.cz: Český internet slaví 20. Narozeniny, vzpomíná skromné začátky. [online]. [cit. 2012-02-13]. Dostupné z: https://www.idnes.cz/technet/internet/cesky-internet-slavi-20-narozeniny-vzpomina-na-skromne-zacatky.A120213_000221_sw_internet_pka
4. NÁRODNÍ CENTRÁLA PROTI ORGANIZOVANÉMU ZLOČINU SLUŽBY KRIMINÁLNÍ POLICIE A VYŠETŘOVÁNÍ. *VÝROČNÍ ZPRÁVA.* [online]. [cit. 2022-01-29]. Dostupné z: www.policie.cz ›soubor ›vyrocni-zprava-ncoz-2020
5. PETERKA, J., *EaRCHIV.CZ, Na počátku byl ARPANET ….* . [online]. [cit. 2022-01-28]. Dostupné z: http://www.earchiv.cz/a95/a504c502.php3
6. POLICIE ČESKÉ REPUBLIKY, *Kyberkriminalita* [online]. [cit. 2022-01-29]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx
7. POLICIE ČESKÉ REPUBLIKY, *Vývoj registrované kriminality v roce 2021*. [online]. [cit. 2022-01-29]. Dostupné z: https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2021.aspx
8. Směrnice Evropského parlamentu a Rady (EU) 2019/713 ze dne 17. dubna 2019. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32019L0713&qid=1643569660363
9. *World Internet Users and 2021 PopulationStars.* [online]. [cit. 2021-12-23]. Dostupné z: https://www.internetworldstats.com/stats.htm

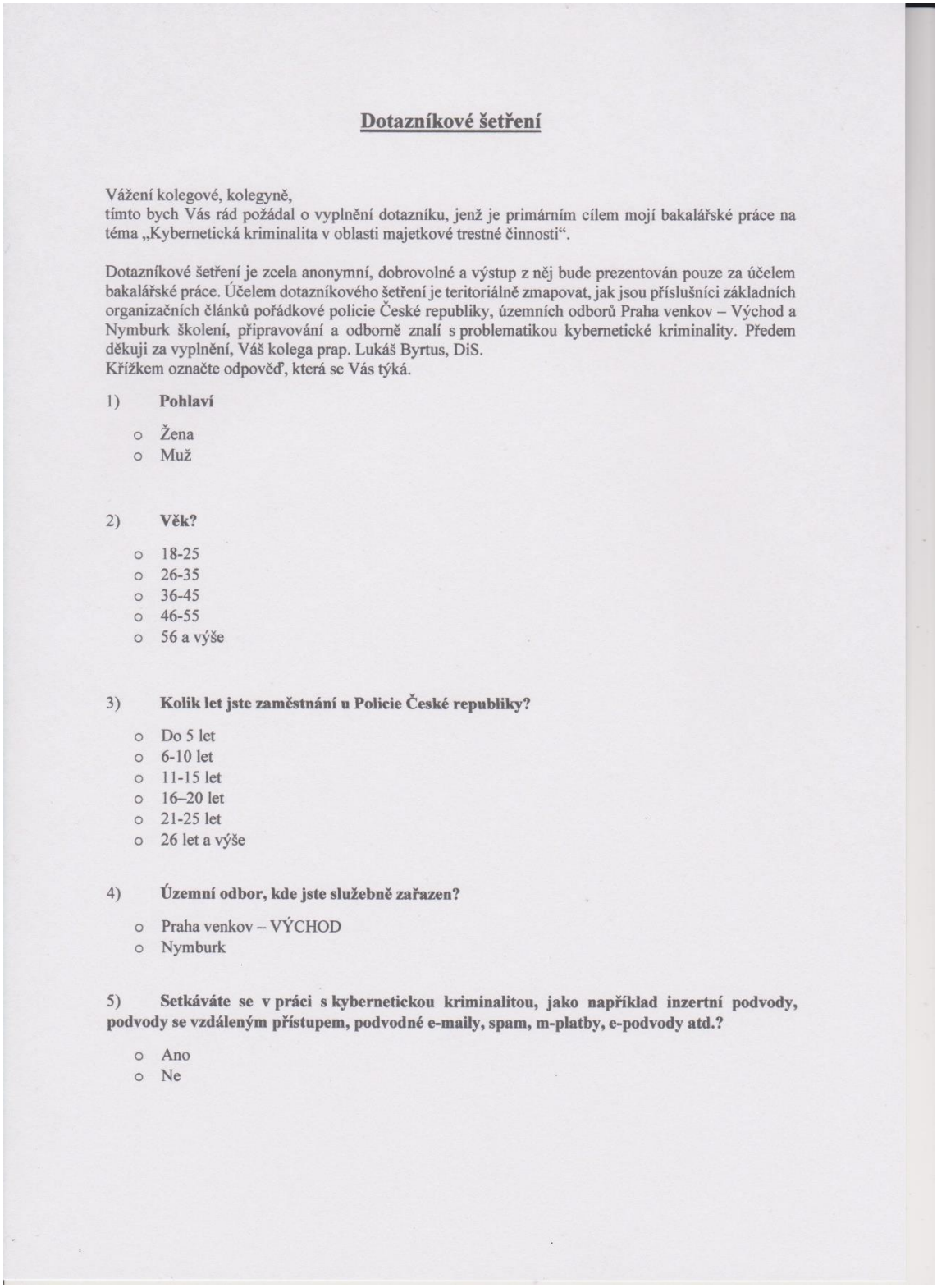
Seznam obrázků a grafů

Obrázky

Grafy

Přílohy

Dotazník stránka 1



Dotazníkové šetření

Vážení kolegové, kolegyně,
tímto bych Vás rád požádal o vyplnění dotazníku, jenž je primárním cílem mojí bakalářské práce na téma „Kybernetická kriminalita v oblasti majetkové trestné činnosti".

Dotazníkové šetření je zcela anonymní, dobrovolné a výstup z něj bude prezentován pouze za účelem bakalářské práce. Účelem dotazníkového šetření je teritoriálně zmapovat, jak jsou příslušníci základních organizačních článků pořádkové policie České republiky, územních odborů Praha venkov – Východ a Nymburk školení, připravování a odborně znalí s problematikou kybernetické kriminality. Předem děkuji za vyplnění, Váš kolega prap. Lukáš Byrtus, DiS.
Křížkem označte odpověď, která se Vás týká.

1) **Pohlaví**

- o Žena
- o Muž

2) **Věk?**

- o 18-25
- o 26-35
- o 36-45
- o 46-55
- o 56 a výše

3) **Kolik let jste zaměstnání u Policie České republiky?**

- o Do 5 let
- o 6-10 let
- o 11-15 let
- o 16–20 let
- o 21-25 let
- o 26 let a výše

4) **Územní odbor, kde jste služebně zařazen?**

- o Praha venkov – VÝCHOD
- o Nymburk

5) **Setkáváte se v práci s kybernetickou kriminalitou, jako například inzertní podvody, podvody se vzdáleným přístupem, podvodné e-maily, spam, m-platby, e-podvody atd.?**

- o Ano
- o Ne

Dotazník stránka 2

6) **Vyznáte se v šetření případů spojených s kybernetickou kriminalitou?**

- o Určitě ano
- o Spíše ano
- o Spíše ne
- o Ne, vůbec tomu nerozumím

7) **Víte, jak zajišťovat kriminalisticky relevantní stopy v kyberprostoru?**

- o Určitě ano
- o Spíše ano
- o Spíše ne
- o Ne, vůbec tomu nerozumím

8) **Na stupnici od 1–5 ohodnoťte Vaši odbornost spojenou s kybernetickou kriminalitou a následnými procesními úkony.**

- o 1 – Výborný
- o 2 – Chvalitebný
- o 3 – Dobrý
- o 4 – Dostatečný
- o 5 – Nedostatečný

9) **Na stupnici od 1–5 ohodnoťte odbornost Vašich kolegů na oddělení spojenou s šetřením kybernetické kriminality a následnými procesními úkony.**

- o 1 – Výborný
- o 2 – Chvalitebný
- o 3 – Dobrý
- o 4 – Dostatečný
- o 5 – Nedostatečný

10) **Na stupnici od 1–5 ohodnoťte připravenost Policie České republiky na úrovni obvodních oddělení Policie České republiky spojenou s šetřením kybernetické kriminality a následnými procesními úkony.**

- o 1 – Výborný
- o 2 – Chvalitebný
- o 3 – Dobrý
- o 4 – Dostatečný
- o 5 – Nedostatečný

11) **Víte, na který orgán se obrátit, v případě, že si nevíte s řešením případu v oblasti kybernetické kriminality rady?**

- o Ne, nevím
- o Ano, uveďte příklad (zde se můžete vyjádřit) –

Dotazník stránka 3

12) **Prodělal/la jste v zaměstnání školení v oblasti kybernetické kriminality?**

- o Ano, pravidelně
- o Ano, jednorázově
- o Ne, ale chtěl/a bych
- o Ne, ani nechci

13) **Vzděláváte se mimo zaměstnání sami s problematikou spojenou s kybernetickou kriminalitou?**

- o Ano, čerpám z odborných zdrojů (literatura, přednášky, konference atd.)
- o Ne, nejevím o tuto problematiku zájem

14) **Seznamujete se pravidelně s interními akty řízení, doporučenými metodikami spojenými s šetřením kybernetické kriminality?**

- o Ano
- o Ne
- o Rád bych, ale vzhledem k vytíženosti nestíhám

15) **Chtěli byste, aby se oblasti kybernetické kriminality zabývali pouze na to odborně školení specialisté?**

- o Ano
- o Ne

16) **Naplňuje Vás šetření případů spojených s kybernetickou kriminalitou?**

- o Ano
- o Ne