Metodika vyšetřování kybernetické kriminality

Bc. Michal Sekanina

Diplomová práce

2022

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Michal Sekanina**
Osobní číslo:	**A18399**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Metodika vyšetřování kybernetické kriminality**
Téma práce anglicky:	**Methodology of Cybercrime Investigation**

Zásady pro vypracování

1. Vypracujte literární rešerši tématu vyšetřování kybernetické kriminality.
2. Nalezněte a analyzujte postupy řešení kyberkriminality.
3. Definujte obecné postupy vyšetřování kyberkriminality.
4. Navrhněte v praxi použitelnou metodiku.
5. Vyhodnoťte přínosy své práce a její reálnou použitelnost v praxi.

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

Seznam doporučené literatury:

1. JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 9788074543128. Dostupné také z: http://hdl.handle.net/10563/25821.
2. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 9788072514366.
3. KOLOUCH, Jan. *CYBERCRIME*. Praha: CZ.NIC, z.s.p.o., 2016. Edice CZ.NIC. ISBN 978-80-88168-18-8. Dostupné také z: https://knihy.nic.cz/files/edice/cybercrime.pdf.
4. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **15. července 2022**
Termín odevzdání diplomové práce: **19. srpna 2022**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 9. srpna 2022

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne 19. 8. 2022

Michal Sekanina v. r.
podpis studenta

ABSTRAKT

Cílem diplomové práce je se seznámit s problematikou kybernetické kriminality a uvést do problematiky vyšetřování kybernetické kriminality. Dále bylo cílem vytvořit stručnou metodiku pro vyšetřovatele trestné činnosti v kyberprostoru. Diplomová práce je rozdělena na část teoretickou a praktickou. V teoretické části jsou popsány základní pojmy, jak z hlediska kyberprostoru, počítačových systémů a síťové architektury, tak z hlediska kriminalistiky a kyberkriminality. V praktické části se zaměřuji na praktické použití a základní postupy, které se aplikují při ohledání místa kybernetického trestného činu a tím pomoci vyšetřovateli se orientovat v této problematice a získat věrohodné digitální důkazy.

Klíčová slova: počítačová kriminalita, trestný čin, digitální důkaz

ABSTRACT

The aim of the diploma thesis is to get acquainted with the issue of cybercrime and to introduce the issue of cybercrime investigation. Furthermore, the aim was to create a brief methodology for cybercrime investigators. The diploma thesis is divided into theoretical and practical part. The theoretical part describes the basic concepts, both in terms of cyberspace, computer systems and network architecture, as well as in terms of crime and cybercrime. In the practical part, I focus on the practical use and basic procedures that are applied in the search for the place of cybercrime and thus help the investigator to orientate in this issue and obtain credible digital evidence.

Keywords: computer crime, criminal offense, digital evidence

Tímto děkuji mému vedoucímu diplomové práce prof. Mgr. Romanu Jaškovi, Ph.D., DBA za odborné vedení, užitečné připomínky a poznatky při zpracovávání mé diplomové práce.

Dále bych chtěl poděkovat své rodině, především manželce, za trpělivost, kterou se mnou měli při mých studiích.

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

OBSAH

ÚVOD

Chápání světa kolem nás již není v dnešní době jen to, co je fyzicky viděno, ale jedná se i o svět, který by se dal definovat jako kyberprostor (cyberspace). Tento svět se začal rozvíjet s příchodem Internetu a zvětšuje se s množstvím přístrojů a zařízení do něj připojených. S tímto rozvojem souvisí ruku v ruce i zvětšující se nárůst páchání trestné činnosti v kyberprostoru, jen s tím rozdílem, že v „Internetu“ se pachatelé cítí více anonymní a tím i troufalejší. To, co by si nikdy nedovolili v „běžném“ světě, si zde s pocitem anonymity troufnou. A nejedná se jen o „mravnostní“ trestné činy, ale třeba i krádeže, protože, co je veřejně na internetu, je přece zadarmo.

V mé diplomové práci se budu snažit vysvětlit základní pojmy, které je nutno pochopit pro vyšetřování kybernetické kriminality. Popíšeme si vztah k legislativě, rozdělení kybernetických trestných činů a jejich možné řešení dle trestního zákoníku a procesní postupy vyplývající z trestního řádu.

V praktické části bude vytvořena metodika vyšetřování kybernetické kriminality pro praktické použití vyšetřovatele se zaměřením na prvotní ohledání místa činu. Jelikož si myslím, že tato problematika je velmi rozsáhlá, samotný vyšetřovatel, který nemá mnoho zkušeností s kybernetickým trestným činem, je až příliš odkázán na znalosti a zkušenosti odborníka či znalce v oboru ICT, jenž je při vyšetřování této trestné činnosti vždy na místě činu a provádí úkony potřebné k zajištění důkazního materiálu, v tomto případě digitálních stop. Má metodika by měla vyšetřovateli ukázat základní úkony potřebné při ohledání místa činu a tím mu pomoci v řízení vyšetřování a úspěšném zodpovězení všech sedmi základních kriminalistických otázek.

I. TEORETICKÁ ČÁST

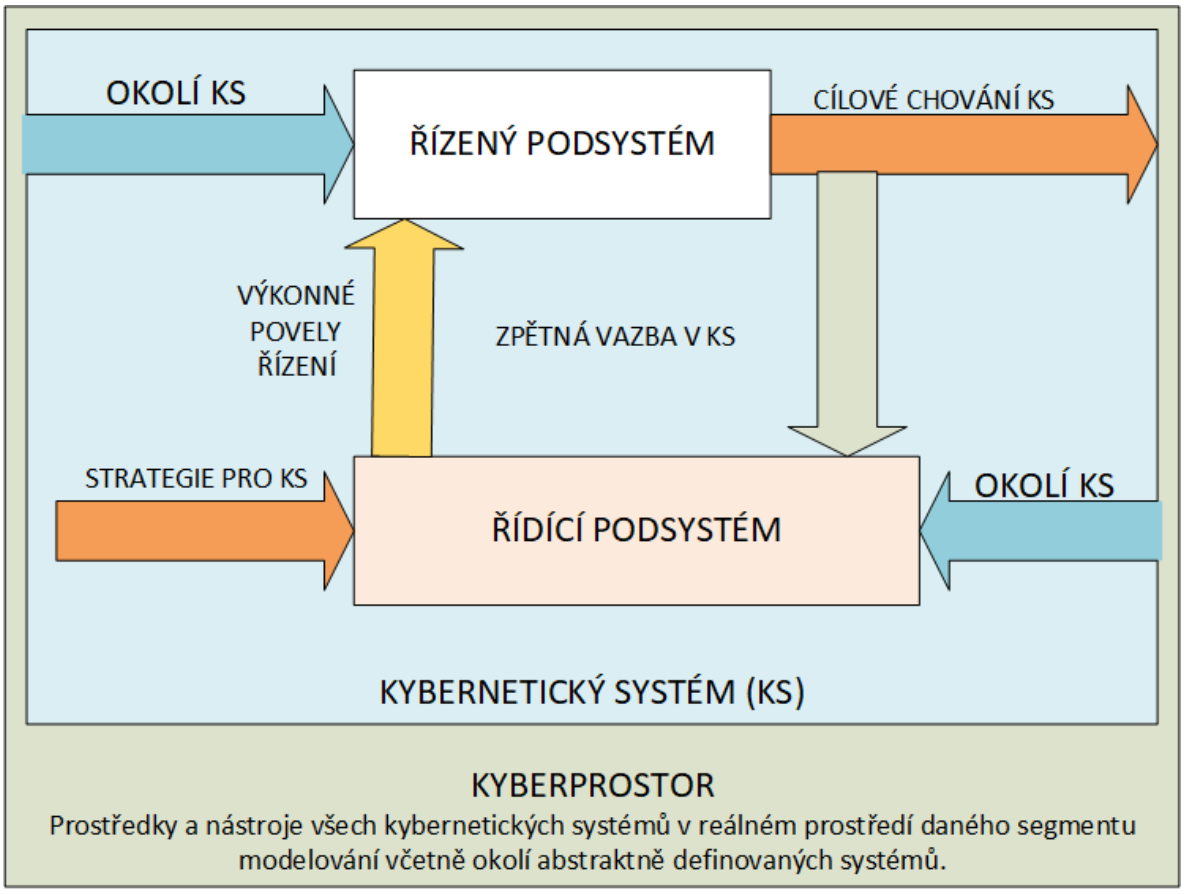
1 TEORETICKÁ VÝCHODISKA

Již dávné řecké mýty obsahují zmínku o mechanických lidech, kteří replikují lidské chování. První výpočetní zařízení byla vnímána jako logické stroje a byla navržena tak, aby re-produkovala lidské rysy, kterými jsou paměť a základní aritmetické dovednosti. Pokus vytvořit umělý mozek inženýři vnímali a stále vnímají jako svůj primární úkol.[1]

[1] SEKANINA, Michal. *Užití vybraných metod umělé inteligence pro robotické bezpilotní systémy*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2018, 59 s. (61047). Dostupné také z: http://hdl.handle.net/10563/42932. Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení, Ústav krizového řízení. Vedoucí práce Dvořák, Jiří.

1.1 TEORIE KYBERNETICKÝCH SYSTÉMŮ

Systémový pohled na svět se stává nyní základem pro vše v živých a neživých organismech. Dále rozvíjí specifické pohledy na svět s použitím systémové integrace a také vytváří zcela nové progresivní pohledy na informační a komunikační techniky a technologie s cílem poznávání světa s řízením objektů v kybernetice a využíváním v praxi technické kybernetiky jako prostředí pro moderní chápání systémového pojetí řízení v prostředí moderních disciplín a dalších teoretických přístupů k novým prostředím tvorby modelů a modelování s prostředky matematiky, fyziky a novými přístupy v dalších oblastech, například v kvantové fyzice, bionice, mechatronice apod.[2] Kybernetický systém v prostředí kybernetického prostoru znázorňuje obrázek č. 1.



Obrázek 1: Kybernetický systém[3]

[2] JANKOVÁ, Martina. *Možnosti systémového prostředí ICT v kyberprostoru podniku*. GRANT journal. 2015, 1, stránky 51-53. [Online]
[3] Vlastní.

1.2 KYBERPROSTOR

Kyberprostor je tvořen prvky informačních a komunikačních technologií *(ICT)*, které vytvářejí pomocí protokolu TCP/IP *(Transmission Control Protocol / Internet Protocol – „primární přenosový protokol/protokol síťové vrstvy)* celosvětovou počítačovou síť s jednotlivými počítačovými systémy, které jsou do této sítě připojeny a které v ní interagují.

Kyberprostor je zcela závislý na technologiích nacházejících se v reálném světě, i když on sám se nachází ve světě virtuálním. Tím vzniká paradox, že nehmotný kyberprostor je zcela závislý na materiálním médiu. Z toho vyplývá, že při kolapsu technologií z reálného světa dochází k nevratnému poškození či úplnému zániku světa kybernetického, virtuálního. [4]

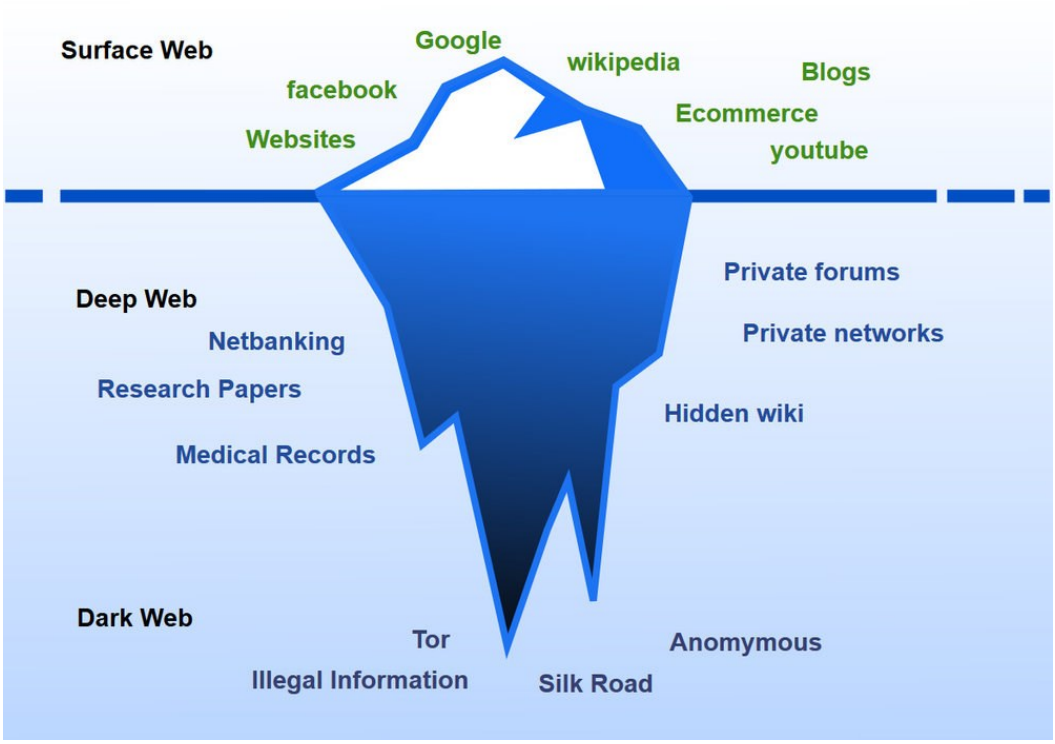
Pro kyberprostor je příznačné, že se do něj propojila značná část populace Země. Zároveň je třeba konstatovat, že k masovému zapojení společnosti začalo docházet teprve před cca 20–25 lety.[5]

Znaky kyberprostoru:

1. Decentralizovanost
2. Globálnost
3. Otevřenost
4. Množství informací
5. Interaktivnost
6. Možnost ovlivňování mínění skrze avatary (virtuální identity)

Kyberprostor si můžeme představit jako níže uvedený obrázek. Je to taková plovoucí kra, kde nám známý Internet s všeobecně známými službami, jako Google, Facebook, Youtube atd., jsou viditelné a zbytek, tedy větší část, je normálním uživatelům skryta pod hladinou.

[4] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
[5] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. CZ.NIC. ISBN 978-80-88168-15-7.



Obrázek 2: Zobrazení kyberprostoru[6]

Tato kra je rozdělena do tří částí:

1. **Surface web**
2. **Deep web**
3. **Dark web**

Je důležité si uvědomit, že **Surface web** (nám známý „Internet“) v kyberprostoru zaujímá pouze asi 4 % z celkového objemu, zbylých 96 % pak připadá na **Deep web** a **Dark web**, které se souhrnně nazývají **Darknets**.

[6] CISO PLATFORM: *CISO Guide: Surface Web, Deep Web and Dark Web - Are they different?*. CISO Platform [online]. Bangalore, Indie: CISO Platform, 2018, 18. 4. 2018 [cit. 2022-05-07]. Dostupné z: https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different

1.3 POČÍTAČ, OSOBNÍ POČÍTAČ (PC)

V souladu se zněním CSN 36 9001 se jedná o „stroj na zpracování dat provádějící samočinné posloupnosti různých aritmetických a logických operací“. Jinými slovy: stroj charakterizovaný prací s daty, která probíhá podle předem vytvořeného programu uloženého v jeho paměti.[7]

1.3.1 Hardware (technické prostředky)

Fyzické součásti systému (zařízení) nebo jejich část (např. Počítač, tiskárna, periferní zařízení).[8]

1.3.2 Software (programové vybavení)

Sada programů používaných v počítači, které vykonávají zpracování dat či konkrétních úloh. Software lze dále rozdělit na:

A) systémový software – vstupně/výstupní systémy, operační systémy nebo grafické operační systémy;

B) aplikační software – aplikace, jednoduché utility nebo komplexní programové systémy;

C) firmware – ovládací program hardwaru.[9]

1.3.3 Data a informace

Informace je každý znakový projev, který má smysl pro komunikátora i příjemce.

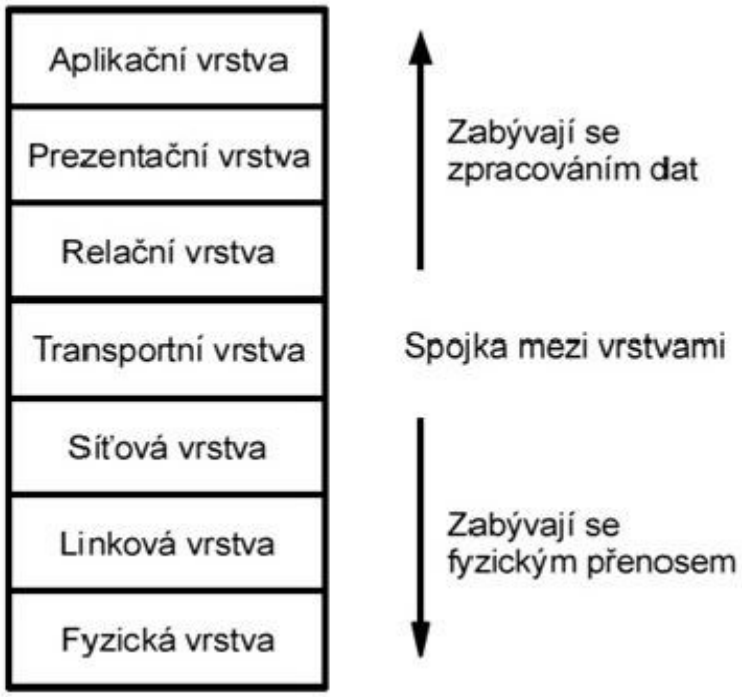
[7] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
[8] Taktéž.
[9] Taktéž.
.

1.4 SÍŤOVÁ ARCHITEKTURA

V dnešní době se používají převážně tzv. vrstvové architektury, protože jsou přehledné a vhodné pro popis toho, co se během přenosu dat v síti děje.

1.4.1 Model ISO/OSI

V současnosti nejspíš nejpoužívanějším standardem v počítačových sítích je tzv. referenční model ISO/OSI *(často také označován RM ISO/OSI)*, kde zkratky ISO patří standardizační organizaci, která normu vydala, tedy International *Organization for Standardization* a OSI je zkratka z anglického *Open System Interconnection*, neboli propojování otevřených systémů. Byl přijat v roce 1979 jako norma standardizační organizace ISO a posléze i jako doporučení X. 200 společnost CCITT. Tento model se skládá ze sedmi vrstev.[10]



Obrázek 3: Referenční model ISO/OSI [11]

[10] VOJTĚŠEK, Jiří. *Internet a jeho služby*. Ve Zlíně: Univerzita Tomáše Bati ve Zlíně, 2012, 106 s. ISBN 9788074542176. Dostupné také z: http://hdl.handle.net/10563/18588.
[11] Taktéž.

Níže ve zkratce uvádím přehled funkcí jednotlivých vrstev modelu ISO/OSI:

- **Fyzická vrstva (Physical layer)** – přenos bitů elektrickými nebo optickými signály;
- **Linková vrstva (Data link layer)** – vytvoření rámců a jejich vysílání;
- **Síťová vrstva (Network layer)** – vytvoření trasy a opatření packetů adresami a dalšími náležitostmi;
- **Transportní vrstva (Transport layer)** – dohled nad spolehlivým přenosem zpráv, opravy chyb, vytvoření packetů;
- **Relační vrstva (Session layer)** – vytvoření spojení s příjemcem a jeho údržba;
- **Prezentační vrstva (Presentation layer)** – převedení zprávy do srozumitelného formátu pro příjemce
- **Aplikační vrstva (Application layer)** – vytvoření zprávy v aplikaci.

Mnemotechnická pomůcka na zapamatování vrstev ISO/OSI modelu:

„Aplikace potkala prezentaci, zrealizovaly transport sítí, spojily se fyzicky.“ [12]

1.4.2 Model TCP/IP

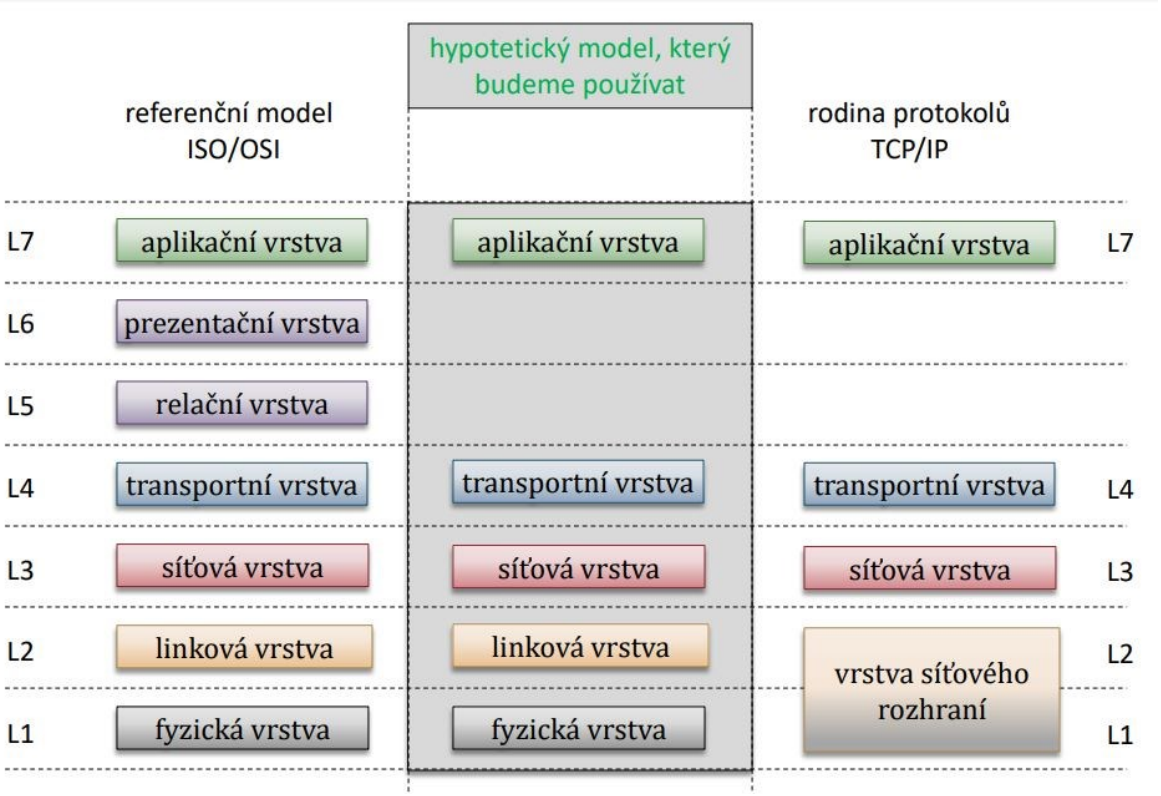
Dalším vrstvovou architekturou, která je využívána je tzv. TCP/IP *(Transmission Control Protocol/ Internet Protocol)* model. Je to model, jenž má jen čtyři vrstvy, a to aplikační, transportní, síťovou a vrstvu síťového rozhraní. Je využíván, protože nezahrnuje jen představu o vrstvách, ale i o konkrétních protokolech, které jsou ve vrstvách využívány.

Jednotlivé vrstvy a používané protokoly:

- **Vrstva síťového rozhraní**
    - Ethernet (100 Mb/s, 1 Gb/s);
    - Rychlejší – skleněná vlákna;
    - Pomalejší – dvoubodové sériové linky (DSL, PPP);
    - Bezdrátové (WIFI, mobilní).

[12] VOJTĚŠEK, Jiří. *Internet a jeho služby*. Ve Zlíně: Univerzita Tomáše Bati ve Zlíně, 2012, 106 s. ISBN 9788074542176. Dostupné také z: http://hdl.handle.net/10563/18588.

- **Síťová (internetová) vrstva**
  - IP (Internet Protocol) nespojovaný přenos datagramů;
  - ARP (Address Resolution Protocol) získání hardwarové adresy z IP;
  - RARP (Reserse Address Resolution Protocol) získání IP adresy z hardwarové;
  - ICMP (Internet Control Message Protocol) chybové a řídící zprávy routerů.
- **Transportní vrstva**
  - TCP (Transmission Control Protocol) spojovaná (potvrzovaná) služba;
  - UDP (User Datagram Protocol) nespojovaná služba.
- **Aplikační vrstva**
  - SSH přístup ke vzdáleným počítačům;
  - SMTP (Simple Mail Transfer Protocol) e-mail;
  - FTP (File Transfer Protocol) přenos souborů;
  - NFS (Network file System) sdílení disků;
  - HTTP, https přístup k webu;
  - DNS (Domain Name System) mapování doménových a IP adres;
  - BOOTPC (Bootstrap Protocol) získání síťové konfigurace při zavádení OS (DHCP);
  - NTP (Network Time Protocol) synchronizace času;
  - IPP (Internet Printing Protocol) přenos news;
  - Atd.



Obrázek 4: Porovnaní modelů ISO/OSI a TCP/IP[13]

1.4.3 IP adresa

Jedna z definic říká, že se jedná o *„Číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti, která používá IP (internetový protokol) slouží k rozlišení síťových rozhraní připojených k počítačové síti. V současné době nejrozšířenější verze ipv4 používá 32b číslo zapsané dekadicky po osmicích bitů (např. 123.234.111.222).“*[14]

Ipv4 dělíme na soukromé a veřejné. Kromě tří rozsahů, které byly v dokumentu RFC 1918 společnosti IETF určeny jako soukromé, jsou všechny adresy veřejné.

Jedná se o rozsahy:

- 10.0.0.0 – 10.255.255.255, neboli 10.0.0.0/8, počet adres 16 777 216;
- 172.16.0.0 až 172.31.255.255, neboli 172.16.0.0/12, počet adres 1 048 576;

[13] Vlastní.
[14] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

- 192.168.0.0 – 192.168.255.255, neboli 192.168.0.0/16, počet adres 65 536.

Jelikož protokol IPv4 již nenabízí takovou kapacitu nových IP adres jaká je potřeba, tak se v současnosti objevuje stále častěji protokol ve verzi IPv6, který se oproti předchozí verzi zvětšil čtyřikrát, na 128 bitů *(např. fdce:9f6a:995::47)*.

S přechodem na nový protokol se pojí řada problémů. Jedním z nejzávažnějších je vzájemná nekompatibilita obou protokolů, kvůli které je počítačům připojeným přes IPv4 nepřístupný internetový obsah využívající připojení pomocí IPv6 a naopak.[15] *(Řešení těchto problémů není v mé DP uvedeno.)*

Základní rozdíly mezi IPv4 a IPv6:

- délka adresy IPv6 má 128 bitů oproti 32 bitům IPv4, čímž se několika set násobně zvětšil počet dostupných IP adres, což pokryje potřeby adres pro budoucí rozvoj síťové infrastruktury;
- objevování sousedů (Neighbor discovering) nahrazuje starší ARP (Address resolution protocol), který slouží k vyhledání linkové adresy pro IP adresu sousedního počítače. K němu však přidává funkce směrování a automatickou konfiguraci;
- hlavička IPv6 paketu je jednodušší v porovnání s datagramem v IPv4. V porovnání s datagramem IPv4 u IPv6 můžeme vidět, že chybí například rozšiřující volby, jako kontrolní součet a fragmentace, TTL byl nahrazen maximálním počtem hopů (hop limit);
- bezpečnostní vylepšení IPv6 přináší hlavně IPsec, což je nejvýraznější bezpečnostní prvek, který je však jen silně doporučován, není povinný. IPsec využívá především AH (Authentication Header) a ESP (Encapsulating Security Payload).

[15] CZ.NIC, z. s. p. o.: *Ipv6 internet pomocí automatických tunelovacích technologií 6to4 a teredo* [online]. Praha: CZ.NIC, z. s. p. o., 2022 [cit. 2022-05-07]. Dostupné z: https://www.nic.cz/ipv6/

1.4.4 Síťový port

Pro rozlišení jednotlivých počítačů používají protokoly rodiny IP výše uvedené IP adresy. Protokoly UDP a TCP používají navíc k rozlišení služeb (procesů) na jednom počítači tzv. síťové porty. I když je technicky možné nastavit pro jednotlivou službu jakékoliv číslo portu od 0 až po 65535, zpravidla se využívají pro známé a velmi používané služby předem stanovená čísla (např. SMTP – 25, POP3 – 110, HTTP – 80, HTTPS – 443 atp.).

Čísla portů přidělovala organizace IANA. Od 21. března 2001 je touto funkcí pověřena organizace ICANN (Internet Corporation for Assigned Names and Numbers).

Porty dělíme do tří skupin:

- Známé porty – porty v rozsahu 0 až 1023; vyhrazené pro nejběžnější služby;
- Registrované porty – v rozsahu 1024 až 49151, použití portu by se mělo registrovat u ICANN;
- Dynamické a soukromé porty – v rozsahu 49152 až 65535, vyhrazené pro dynamické přidělování a soukromé využití, nejsou pevně přiděleny žádné aplikaci.

Kompletní seznam jednotlivých čísel síťových portů je na adrese *„http://www.iana.org/assignments/port-numbers“.*

1.4.5 MAC adresa

MAC (Media Access Control) adresa je celosvětově jednoznačný identifikátor většiny síťového zařízení, který používá mnoho síťových protokolů druhé vrstvy. Nejznámější je ethernet.

Ethernetová MAC adresa má 48 bitů a nejčastěji se zapisuje jako šestice dvou hexadecimálních čísel, tedy ve tvaru xx:xx:xx:xx:xx:xx. První tři dvojice určují výrobce zařízení. MAC adresa je uložena v ROM zařízení a někdy se označuje jako BIA (burned in address).

MAC adresa příjemce a odesílatele je součástí každého ethernetového rámce (frame; základní přenosová jednotka ethernetu). Ke zjištění MAC adresy cílového počítače z jeho IP adresy se používá protokol ARP.

V zabezpečování sítí se nelze na MAC adresu stoprocentně spolehnout, protože je poměrně jednoduché ji změnit.[16]

[16] ABCLINUXU: *MAC adresa* [online]. Praha: Nitemedia, 2009 [cit. 2022-05-07]. Dostupné z: https://www.abclinuxu.cz/slovnik/mac-adresa

2 KYBERKRIMINALITA (CYBERCRIME)

S růstem využívání informačních a komunikačních systémů (prostředků, zařízení) roste i možnost jejich užití k páchání trestných činů. Proto neexistuje obecně platná definice, která by vystihla celou hloubku pojmu kyberkriminalita.

Nejobecněji by bylo možné kyberkriminalitu definovat jako jednání, při kterém je počítačový (informační) systém využit jako nástroj pro páchání trestného činu vůči počítačovému systému, počítačové síti, datům či uživatelům. Musíme říci, že pokud chceme, aby výše uvedené bylo možné uplatnit, vše se musí odehrávat v kyberprostoru.

Do kyberprostoru se přesouvá i trestná činnost, jež se doposud odehrávala mimo něj, protože je zde možné tuto trestnou činnost páchat rychleji, efektivněji a s menším rizikem odhalení. Jedná se například o podvody, šíření materiálů zobrazujících zneužívání dětí, prodej drog aj.

Je třeba si uvědomit, že ne každý kybernetický útok musí být trestným činem, ale každý kybernetický trestný čin musí být zároveň kybernetickým útokem. Mnoho kybernetických útoků mají povahu správního či občanskoprávního deliktu, případně se nemusí jednat o jednání jakkoliv postižitelné právní normou, jde „pouze“ o nemorální jednání.[17]

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

2.1 ANALÝZA INFORMAČNÍCH ZDROJŮ

Kyberkriminalitě a spolu s ní kybernetické obraně je v současné době věnována veliká pozornost nejen organizacemi, které se kybernetickou bezpečností a vyšetřováním kyberkriminality zabývají (Policie, NÚKIB), ale i organizacemi, pro které není kybernetická kriminalita hlavní činností, např. finanční instituce (banky, pojišťovny aj.), soukromé společnosti, orgány státní správy a samosprávy. Za tímto účelem se pořádá velké množství kurzů, seminářů a školení.

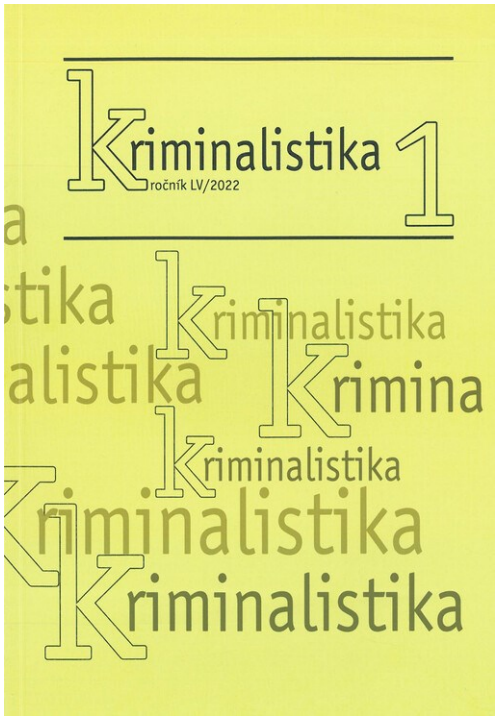
Bezpečností v kyberprostoru a i kyberkriminalitou se zabývá řada knih, časopisů, webových stránek, jež jsou na tuto problematiku zaměřeny. Odborníci na kybernetickou bezpečnost se podílí na realizaci výchovných a vzdělávacích programů v různých typech škol a školských zařízeních.

2.1.1 Odborné časopisy a periodika

- *Bezpečnostní teorie a praxe* je odborné periodikum Policejní akademie České republiky v Praze (ISSN 1801-8211 pro tištěnou verzi a ISSN 2571-4589 pro online verzi). Je zařazený do databáze vědeckých časopisů European Reference Index for the Humanities and the Social Sciences (ERIH PLUS). Hlavním posláním časopisu je zveřejňovat výsledky vědecké a výzkumné činnosti, které jsou zaměřeny na současné bezpečnostní hrozby a vývojové trendy vybraných forem kriminality, postupy a spolupráci bezpečnostních sborů, bezpečnostní stránky řízení, správy a administrativy, specificky orientované do oblasti krizového řízení, bezpečnostního managementu, kriminalistiky, kriminologie a forenzní psychologie. A dále je zaměřen na publikování výzkumných výsledků v dané odborné oblasti.[18]
- *Kriminalistika: časopis pro kriminalistickou teorii a praxi* je odborný teoretický časopis, vydávaný Ministerstvem vnitra České republiky 4x ročně, zaměřený na výsledky vědeckovýzkumné činnosti v oblasti obecné teorie kriminalistiky, kriminalistické taktiky a techniky, metodiky odhalování, vyšetřování a prevence trestných činů,

[18] POLICEJNÍ AKADEMIE ČR: *Bezpečnostní teorie a praxe* [online]. Praha: Policejní akademie ČR, ISSN 1801-8211. Dostupné z: https://veda.polac.cz/

trestní právo hmotné a procesní, kriminologické učení, zkoumání zločinnosti, penelogie, soudní lékařství, psychiatrie, soudní psychologie, sexuologie, aktuální problémy boje s kriminalitou.[19]



Obrázek 5: Titulní strana časopisu Kriminalistika[20]

- *British Journal of Criminology: An International Review of Crime and Society* je jedním z nejlepších světových kriminologických časopisů. Publikuje práce nejvyšší kvality z celého světa a napříč všemi oblastmi kriminologie. Online ISSN 1464-3529, tisk ISSN 0007-0955.

2.1.2 Publikace

- Kniha *Kybernetická kriminalita,* jejímž autorem je *Vladimír Smejkal*, shrnuje autorovy dlouhodobé poznatky z oblasti právní teorie, ale i reálné praxe při odhalování a vyšetřování kybernetické kriminality. Kniha je široce a mezioborově koncipována tak, aby v ní našli potřebné informace právníci, odborníci na IT, manažeři a studenti

[19] *Kriminalistika: časopis pro kriminalistickou teorii a praxi*. Praha: Magnet-Press, 1993-. ISSN 1210-9150. Dostupné také z: https://www.mvcr.cz/clanek/kriminalistika.aspx
[20] Taktéž.

vysokých škol všech zaměření, ale také všichni, kdo se nějakým způsobem dostanou do styku s trestnou činností související s kybernetickou kriminalitou.

- Kniha *Kriminalistika: technické, forenzní a kybernetické aspekty* od autora Viktora Porady se zabývá základními pojmy a teoriemi, které vedou ke správné interpretaci stop trestného činu a pomohou identifikovat pachatele.
- Učebnice *Kriminalistika: kriminalistická taktika a metodiky vyšetřování* od kolektivu autorů Zdeňka Konráda, Viktora Porady, Jiřího Strause a Jaroslava Suchánka se snaží zachytit současný stav kriminalistického poznání. Je určena pro studenty bezpečnostních a právnických oborů, policisty, advokáty, či soudce.

2.1.3 Akademické práce

Bakalářská práce:

- Lukáš KEŇO, *Vyšetřování počítačové kriminality*, UTB FAI, 2016;
- Luboš PERNICA, *Kybernetická kriminalita*, UTB FLKŘ, 2018.

Diplomová práce:

- Bc. Lukáš HANZL, *Metodika vyšetřování počítačové kriminality*, UTB FAI, 2008;
- Michal MLČOUCH, *Počítačová kriminalita a specifika jejího dokazování*, Masarykova univerzita v Brně, Právnická fakulta, 2016;
- Kristina RADEMACHEROVÁ, *Právní rámec vyšetřování počítačové kriminality*, UK, Právnická fakulta, 2016.

2.2 TRESTNĚPRÁVNÍ OCHRANA PŘED KYBERKRIMINALITOU

Již od počátku vzniku negativních aktivit spojených s kyberprostorem je snahou policie postihovat tyto přestupky, delikty a trestné činy. Kyberkriminalita je však značně odlišná od „klasické“ kriminality. Její odlišnost spočívá hlavně v jejím dynamickém rozvoji a schopností se okamžitě přizpůsobovat změnám, což v legislativní tvorbě není tak jednoduché.[21]

Mnohdy nejsou legislativní normy na tyto trestné činy v kyberprostoru připraveny a nelze na ně aplikovat stávající normy ani ze zákonů již na kyberkriminalitu připravených, ani z legislativy zaměřené na „tradiční“ kriminální činnost. Proto je vždy spravedlnost a její možnost právo vymáhat minimálně jeden krok za kyberzločinem.

2.2.1 Právní rámec kybernetické kriminality

K trestným činům páchaným v prostředí kyberprostoru a s ní související kybernetickou bezpečností je třeba uvést právní normy, jež mají k této problematice vztah.

Jedná se zejména o:

- 1/1993 Sb., Ústava České republiky
- 2/1993 Sb., Listina základních práv a svobod
- 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- 40/2009 Sb., trestní zákoník
- 89/2012 Sb., občanský zákoník
- 101/2000 Sb., o ochraně osobních údajů
- 121/2000 Sb., autorský zákon
- 127/2005 Sb., o elektronických komunikacích
- 141/1961 Sb., o trestním řízení soudním
- 160/1999 Sb., o svobodném přístupu k informacím
- 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- 218/2003 Sb., o soudnictví ve věcech mládeže
- 227/2000 Sb., o elektronickém podpisu

[21] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. CZ.NIC. ISBN 978-80-88168-15-7.

- 273/2008 Sb., o Policii České republiky
- 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
- 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- 441/2003 Sb., o ochranných známkách
- 480/2004 Sb., o některých službách informační společnosti
- 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích

2.2.2 Základní podmínky uplatňování kriminalisticko-taktických metod, postupů a operací[22]

Za základní podmínky uplatňování kriminalisticko-taktických metod se považují zejména:

- **Zákonnost** – je nejdůležitější podmínka, jelikož veškerá činnost státních orgánů musí být vykonávána v souladu se zákonem (viz. čl. 2 odst. 2 z. č. 2/1993 Sb., Listina základních práv a svobod), pokud není v zákoně stanoveno jinak. Nelze zákonem postihnout celou šíři těchto nástrojů poznání a situací, za nichž může být aplikován, a proto je nutné zákonnost těchto kriminalisticko-taktických metod posuzovat v obecné a zvláštní rovině.
- **Vědecká odůvodněnost** – má zajistit, aby aplikace kriminalisticko-taktických metod vedla spolehlivě k poznání objektivní pravdy. Rozumí se tím především možnost posouzení metody, postupu či operace podle vědeckosti pramene jejich původu; prověření spolehlivosti metody praxí; soulad mezi postupem, metodou či operací a současnými poznatky vědních oborů, z nichž čerpají nebo na nichž jsou založeny; možnost vědeckého předvídání výsledků uplatnění taktických metod, postupů a operací a možnost určení validity těchto výsledků.

  Požadavkům vědecké odůvodněnosti neodpovídají metody založené s využitím věštců a psychotroniků.

[22] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování*. 2. rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4.

- **Praktická odůvodněnost** – představuje požadavek vhodnosti, finanční náročnosti a efektivnosti použití postupů a metod v určitých situacích. Je třeba posuzovat úspornost a efektivnost případ od případu.
- **Etika** – je potřeba brát v úvahu, zda aplikací metod, postupů či operací nemůže dojít ke zbytečnému snižování důstojnosti a cti účastníků úkonu. Tento požadavek musíme brát v úvahu vždy.
  A současně se hodnotí provádění určité metody, postupu či operace v podmínkách, kdy vzniká nebezpečí porušení obecně uznávaných etických a morálních norem.

2.2.3 Kriminalistická metodika vyšetřování kybernetické kriminality

Jelikož kyberkriminalita je svým pojetím specifická, až se vymyká běžnému chápání kriminality, bylo zapotřebí vyvinout zvláštní metodiku, která uzpůsobila běžné prostředky dokazování kybernetickému prostředí. Tato metodika se neustále vyvíjí a doplňuje tak, jak se zjišťují další, nové způsoby páchání kybernetické kriminality.

Samotné vyšetřování kyberkriminality by se mělo ponechat specializovaným týmům složených z odborníků na danou problematiku.

2.2.3.1 Digitální stopa

Jako součásti důkazního materiálu se stále častěji uplatňují tzv. digitální stopy, a to nejen při vyšetřování trestných činů kybernetických, ale i trestných činů zejména z oblasti hospodářské trestné činnosti, proti majetku a proti pořádku ve věcech veřejných.

Proto je nezbytné si tento nový pojem definovat. V některé literatuře je synonymum pro pojem digitální stopa uveden pojem počítačová stopa. Tento pojem působí zavádějícím dojmem, poněvadž informační systémy se neskládají pouze z počítačů. Definice digitální stopy se v různé literatuře liší, níže uvedu některé z nich:

- *„Počítačovou stopu lze charakterizovat jako změnu na nosiči informací, vzniklou v souvislosti s trestným činem, při jehož páchání byla použita výpočetní technika a která je zjistitelná za pomoci současných metod, prostředků a operací. Tyto stopy se*

nacházejí na pevném disku, vyměnitelných paměťových médiích, CD ROM, disketách atp.“[23]

- *„Každé technologické zařízení, které získává, zpracovává, předává nebo uchovává data, zanechává (odrazy) o své činnosti. Tyto záznamy z kriminalistického hlediska jsou stopami. V oblasti IT/IS jsou tedy především digitální stopy, které lze definovat podle SWGDE (Scientific Working Group on Digital Evidence) jako jakékoliv informace s vypovídající hodnotou, uložené nebo přenášené v digitální podobě. Z hlediska trestního či správního řízení je ale pro nás možná užitečnější definice International Organization of Computer Evidence (IOCE), která definovala původně digitální stopu jako jakoukoli informaci, uloženou nebo přenášenou v binární formě, která může být předložena soudu jako věcný důkaz.“*[24]

Z výše uvedeného se domnívám, že za digitální stopu lze označit jakákoliv data vytvořena, přenesená, uložená či modifikována za využití informačních (počítačových) systémů a to úmyslně i neúmyslně. Ne vždy se tato stopa stane důkazem u soudu, ale lze ji využít k získání dalších poznatků, které již jako důkaz posloužit mohou. Proto by se mělo ke každé digitální stopě přistupovat jako ke stopě, která může být u soudního procesu využita.

Tyto stopy se nacházejí v informačních systémech, na různých nosičích dat a v neposlední řadě v kyberprostoru. Avšak jejich vlastnosti jsou takové, že neusnadňují práci orgánům činných v trestním řízení, nebo jim ustanoveným znalcům *(IT odborníkům)*. Mezi tyto vlastnosti patří zejména:

- nehmotnost;
- latentnost;
- časová trasovatelnost, respektive manipulovatelnost s časem v informačních systémech;
- informační hodnota;
- velmi nízká životnost;
- uchování a kvalita archivních záznamů;
- velké objemy digitálních dat;

---

[23] STRAUS, Jiří. *Kriminalistická metodika.* 2., rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2008. ISBN 978-80-7380-124-3.
[24] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, ISBN 978-80-7380-501-2.

- vysoká datová hustota digitálních záznamů;
- dynamika vývoje informačních technologií;
- dynamika činnosti informačních systémů;
- komplexnost prostředí;
- velký geografický rozsah prostoru s digitálními stopami;
- dostupnost kvalitní ochrany digitálních dat;
- možnost automatizace při identifikaci digitálních stop;
- možnost změny identity pachatel v kyberprostoru;
- obnovitelnost digitálních stop;
- problém originality digitálních stop;
- nedůvěra v důkazní sílu digitálních stop.[25]

Základní zásada pro zajišťování digitálních stop je zachování jejich integrity a z toho vyplývá, že musí být pořízeny identické bitové kopie originálních nosičů dat a jejich autentizace pomocí kontrolních součtů *(hash)* a následné provádění forenzní analýzy na těchto bitových kopiích. Problém nastává u analýz dynamických pamětí informačních systémů *(operační paměť atp.)*, tzv. „živé" analýzy, kdy se do paměti musí nahrát program, který tuto analýzu provede, a tím dochází ke změně předmětu zkoumání.

Digitální *(počítačová)* stopa má oproti klasickým stopám významná specifika, neboť je zpravidla značně objemná *(co se velikosti dat týče)*, dynamická a může být rozmístěna kdekoli v kyberprostoru. Životnost takovéto stopy může být velmi krátká a jakékoli průtahy v postupu před zahájením trestního stíhání i ve vyšetřování nutně vedou k její ztrátě. I díky tomu se snižuje objasněnost kyberkriminality.[26]

2.2.3.2 Kriminální situace

Kriminální situace je tvořena souhrnem podmínek a okolnosti, které umožňuji páchání kyberkriminality. Tyto podmínky předurčuji nejen způsoby páchání trestných činů, ale i zákonitosti vzniku a zániku stop.[27]

---

[25] SMEJKAL, Vladimír. *Současné možnosti boje proti počítačové kriminalitě*. Data security management. Roč. XV, 2011, č. 4. ISSN 1211-8737.
[26] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. CZ.NIC. ISBN 978-80-88168-15-7.
[27] Taktéž.

Kriminalita v kyberprostoru je sice pojmově zúžena na tento prostor, ale její význam oproti jiným možným (kriminálním) útokům na celek výpočetní techniky, jak ji chápeme, je natolik závažný z celospolečenského a mezinárodního hlediska, že je dnes rozhodným těžištěm boje s jejími organisovanými projevy a následky.[28]

Jejími specifiky jsou právě snadné a rychlé uskutečnění útoku (trestného činu) v reálném čase kdekoliv po celém světě. Složité zachycení stop a důkazů po útocích a neméně složité dokazování dělají z takových útoků téměř dokonalé trestné činy.

2.2.3.3 Typické osobnostní rysy pachatelů kyberkriminality

Dle literárních zdrojů je například v USA typickým pachatelem počítačové trestné činnosti zaměstnanec poškozené firmy. V České republice je situace obdobná, pouze 6 % pachatelů jsou zaměstnanci jiných firem či organizací, asi jedna čtvrtina pachatelů je přímo zaměstnána v IT oddělení poškozené firmy a více než polovina je koncovým uživatelem výpočetní techniky v poškozené firmě (někde se uvádí, že v ČR převažuje více pachatelů z IT oddělení poškozené firmy).

Je překvapivé, že u pachatelů nedominuje vysoké IQ, ale spíše hamižnost, touha po moci, bezohlednost a vytrvalost. Mnozí z pachatelů jsou neurotiky se špatnou sociální komunikací a sexuálními problémy. Pachatelé kybernetických trestných činů nevidí ve svém jednání nic špatného a necítí za své činy vinu.[29]

Mezi specifické typy pachatelů patří tzv. „hackeři“. Hackování jako činnost má dlouhou a bohatou historii a samo o sobě zahrnuje řadu různých kultur a praktik. Etnografické studie hackingu jej chápou jako mnohem širší a starší soubor způsobů, jakými lidé vždy interagovali s technologiemi, zdůrazňují praktiky kreativního lámání, technické neplechy a přeměňování (sociálních i technických) systémů tak, aby produkovaly výsledky neočekávané jejich tvůrci. Základy hackerské kultury (jak je běžně chápáno) oceňují tvrdé technické mistrovství, kreativní přeměnu účelů systémů, samouk, antiautoritářský přístup a reflexivně

[28] PORADA, Viktor a Karel RAIS. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatel-ství CERM, 2021. ISBN 978-80-7623-065-1.
[29] PORADA, Viktor. Kriminalistika: technické, forenzní a kybernetické aspekty. 2. aktualizované a rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.

technolibertariánskou politiku. Podmnožina hackerů a hackerských praktik nachází svůj domov v tom, co se označuje jako subkultura „undergroundových hackerů“ – v komunitách, často organizovaných kolem online fór a chatovacích kanálů, které přizpůsobují hackerské praktiky pro páchání trestné činnosti.[30]

2.2.3.4 Typické motivy pachatelů kyberkriminality

Zjištění motivu je ve vyšetřování kybernetické trestné činnosti nesmírně důležité. Pokud najdeme odpověď na otázku, kdo má v souvislosti se spácháním trestného činu prospěch, zúží se nám okruh možných pachatelů. Zjištění motivu trestného činu má také obrovský význam pro posouzení společenské škodlivosti jednání a pro právní kvalifikaci provedeného trestného činu.

Za typické motivy lze v tomto případě považovat zejména:

- zištné motivy (rychlé a relativně bezpečné získání velkého finančního zisku),
- motivy vyplývající z konfliktů v mezilidských vztazích (msta, nenávist, závist atp.),
- touhu po získání moci či výsadního postavení (např. diskreditací konkurentů),
- touhu dokázat svou intelektuální převahu (např. nad nadřízeným, nad tvůrci ochranných programů),
- snahu ukázat své schopnosti, jež jsou nedoceněny („vytáhnout“ se před kamarády, spolupracovníky, nadřízenými atp.),
- krytí jiné trestné činnosti (např. daňové úniky, zpronevěra svěřených hodnot atp.),
- politické motivy (např. diskreditace politických odpůrců) nebo jiné ideologické motivy (náboženské, filozofické aj.).

Uvedené motivy se mohou vyskytovat samostatně i v různých kombinacích.[31]

---

[30] THE BRITISH JOURNAL OF CRIMINOLOGY: *AN INTERNATIONAL REVIEW OF CRIME AND SOCIETY: Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture* [online]. 2021. Oxford, UK: Oxford University Press, 2021 [cit. 2022-05-07]. ISSN 0007-0955. Dostupné z: https://academic.oup.com/bjc/article/61/5/1407/6226588?searchresult=1t

[31] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. 2. aktualizované a rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2

2.2.4 Trestněprocesní postup při odhalování, prověřování a vyšetřování kyberkriminality

Kybernetická kriminalita bývá dlouhou dobu neodhalena, jelikož její páchání se koná utajovaně. Základní činností k odhalování kybernetické kriminality proto bývá sběr a vyhledávání poznatků o ní a prověřování podezřelých osob.

Nejčastějšími **podněty** jsou zejména:

- výsledky operativně pátrací činnosti SKPV,
- oznámení kontrolních, inspekčních a revizních orgánů různých organizací,
- ústní, písemná a telefonická oznámení občanů,
- ostatní druhy podnětů (např. anonymní oznámení, poznatky zveřejněné sdělovacími prostředky).[32]

Vyšetřování je definováno jako úsek od zahájení trestního stíhání do podání obžaloby nebo jiných mimosoudních způsobů vyřízení. Trestní řád nicméně umožňuje, mimo některé úkony, opatřovat a provádět důkazy již ve stádiu před zahájením trestního stíhání.

Při vyšetřování kyberkriminality se setkáváme zejména s následujícími počátečními vyšetřovacími situacemi:

- **Zjištěné skutečnosti nasvědčují tomu, že se stal skutek, v němž lze spatřovat trestný čin, nedovolují však vyslovit jednoznačný závěr o totožnosti pachatele a způsobu spáchání trestného činu –** vyšetřovatel by se měl zaměřit na zjištění možného způsobu spáchání trestného činu.
- **Zjištěné skutečnosti nasvědčují tomu, že se stal skutek, v němž je spatřován trestný čin, a objasňuji spáchání předmětného trestného činu. Nedovolují však vyslovit závěr o totožnosti pachatele** – vyšetřovatel by se měl zaměřit mimo jiné na zjištění totožnosti pachatele. Okruh možných pachatelů by mohl vyšetřovateli vymezit způsob spáchání trestného činu, v čemž by měl asistovat vyšetřovateli znalec z oboru IT a provést analýzu způsobu spáchání trestného činu.

[32] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. 2. aktualizované a rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2

- **Zjištěné skutečnosti nasvědčují tomu, že se stal skutek, v němž je spatřován trestný čin, dovolují učinit závěr o totožnosti pachatele, nedovolují však vyslovit jednoznačný závěr o způsobu spáchání trestného činu** – vyšetřovatel by se měl zaměřit na shromáždění důkazů, které buď vyvrací, nebo potvrdí možné verze o způsobu páchání trestného činu a jeho motivu. K objasnění způsobu spáchání trestného činu a jeho motivu je nutné, aby vyšetřovatel využil pomoci znalců a jiných odborníků. Mezi tyto znalce a odborníky by neměli patřit odborníci z postižené firmy či organizace, jelikož takový postup byl opakovaně shledán nezákonným.
- **Zjištěné skutečnosti nasvědčují tomu, že se stal skutek, v němž je spatřován trestný čin, dovolují učinit závěr o totožnosti pachatele a objasňují i pravděpodobný způsob spáchání trestného činu** – pro vyšetřovatele nejvýhodnější situace, neboť nashromážděné důkazní materiály a výpovědi osob objasňují většinu podstatných otázek o spáchaném trestném činu. Vyšetřovatel se může, po sdělení obvinění konkrétní osobě, zaměřit na zprocesnění informací obsažených v dosud nashromážděných materiálech a zajištění objektů pro expertizní činnosti za využití specialistů v daném oboru.[33]

2.2.5 Specifika dokazování kyberkriminality

Obecně lze dokazování definovat jako: *„Dokazováním v procesním trestním právu se tedy rozumí zákonem upravený postup orgánů činných v trestním řízení, jehož cílem je umožnit těmto orgánům poznání skutečnosti důležitých pro jejich rozhodnutí, tedy vyhledat důkazy o nich, tyto důkazy provést, získané poznatky procesně zajisti a zhodnotit.“*[34]

V souvislosti s dokazováním, hlavně u tak složité problematiky jako ICT, vzniká otázka, zda je vůbec možné zjistit pomocí dokazování objektivní pravdu. Z některých pramenů vyplývá, že význam dokazování nelze jako prostředek poznání objektivní pravdy zpochybnit, právě s vyšetřováním v kyberprostoru tomu tak vůbec nemusí být. Velkým problémem nám při dokazování činí vzrůstající složitost informačních systémů a sítí. Při běžícím informačním systému probíhá mnoho různých paralelních procesů, které mezi sebou a i s uživateli komunikují, jejich stav se v každém okamžiku mění a mnohdy je neopakovatelný. Toto klade

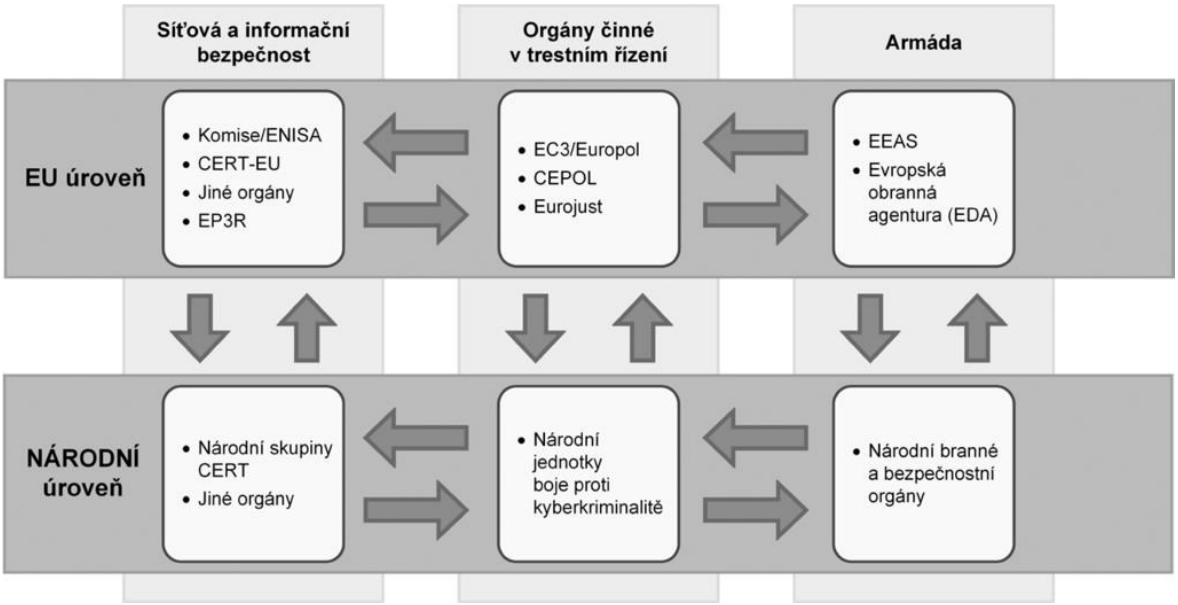
[33] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. 2. aktualizované a rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.
[34] SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, ISBN 978-80-7380-501-2.

velké překážky a mnohdy činí nemožné poznat vnitřní svět informačních systémů beze zbytku.

2.3 KYBERNETICKÁ BEZPEČNOST ČESKÉ REPUBLIKY

Pro kybernetickou bezpečnost byl 1. srpna 2017 na základě zákona zřízen **Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)**. Je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů kryptografické ochrany.

Ředitel NÚKIB je členem Výboru pro kybernetickou bezpečnost, který je stálým pracovním orgánem Bezpečností rady státu pro koordinaci plánování opatření k zajištění kybernetické bezpečnosti České republiky.



Obrázek 6: Pilíře zajišťování kybernetické bezpečnosti na evropské a národní úrovni[35]

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

Národní centrum kybernetické bezpečnosti (NCKB) je výkonnou sekcí NÚKIB a zajišťuje zejména:

- činnost Vládního CERT (Computer Emergency Response Team) České republiky (govcert.CZ);
- prevenci před kybernetickými hrozbami proti prvkům kritické informační infrastruktury, informačním systémům základní služby, proti významným informačním systémům a vybraným informačním systémům veřejné správy;
- řešení a koordinaci řešení kybernetických bezpečnostních incidentů u subjektů kritické infrastruktury, provozovatelů základní služby a orgánů veřejné správy;
- osvětovou a vzdělávací činnost v oblasti kybernetické bezpečnosti;
- spolupráci s národními i mezinárodními organizacemi podílejícími se na zajišťování bezpečnosti kybernetického prostoru;
- výzkum a vývoj v oblasti kybernetické bezpečnosti;
- ve spolupráci s kabinetem ředitele zastupování ČR v orgánech mezinárodních organizací působících v oblasti kybernetické bezpečnosti;
- vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímaní příslušných nápravných a preventivních opatření;
- v rozsahu své působnosti bezpečnostní politiku Úřadu, plnění mezinárodních závazků a spolupráci na mezinárodní úrovni při realizaci předpisů vyplývajících z členství ČR v NATO a členství v EU a členství v jiných mezinárodních organizacích;
- a další.[36]

CSIRT.CZ je Národní CSIRT (Computer Security Incident Response Team) České republiky. Národní CSIRT ČR je vykonávaný dle veřejnoprávní smlouvy uzavřené s Národním bezpečnostním úřadem. Ten se stal gestorem problematiky kybernetické bezpečnosti v říjnu 2011. Tým CSIRT.CZ plní úlohu národního CERT České republiky podle Zákona o kybernetické bezpečnosti.

[36] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST: *Kybernetická bezpečnost*. NCKB [online]. Brno: NÚKIB, 2022, [cit. 2022-05-07]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/t

Role CSIRT.CZ jsou v prostředí České republiky následující:

- udržování zahraničních vztahů – se světovou komunitou CERT/CSIRT týmů a organizacemi, které tuto komunitu podporují;
- spolupráce se subjekty v rámci ČR – ISP, poskytovateli obsahu, bankami, bezpečnostními složkami, akademickým sektorem, úřady státní správy a dalšími institucemi;
- poskytování služeb v oblasti bezpečnosti:
    - řešení a koordinace řešení bezpečnostních incidentů;
    - osvětová a školící činnost;
    - proaktivní služby v oblasti bezpečnosti.

Tým CSIRT.CZ je členem mezinárodních uskupení CSIRT/CERT týmů. U Trusted Introducer je akreditovaný od roku 2011. V roce 2015 se tým CSIRT.CZ stal taky členem organizace FIRST.

Polem působnosti týmu CSIRT.CZ je celá ČR, tzn. všichni uživatelé a všechny sítě provozované v České republice se nachází ve sféře vlivu CSIRT.CZ.[37]

Rozdíl mezi vládním a národním CERT je definován zákonem o kybernetické bezpečnosti. Zjednodušeně lze říci, že vládní CERT je určen pro řešení bezpečnostních incidentů v počítačových sítích státní správy, kritické informační infrastruktury a významných informačních systémů dle zákona o kybernetické bezpečnosti. Národní CERT je bezpečnostní tým pro koordinaci řešení ostatních bezpečnostních incidentů v počítačových sítích provozovaných v České republice.[38]

Dále vznikají CERT/CSIRT týmy na úrovni jednotlivých organizací, přičemž jde jednak o organizace, které zprostředkovávají chod Internetu (ISP - poskytovatelé připojení a služeb), a jednak o organizace, které prostředí Internetu používají ke své hlavní činnosti (např. IT firmy, poskytovatelé obsahu, banky).[39]

---

[37] CSIRT.CZ: *O týmu CSIRT.CZ* [online]. Praha: CZ.NIC, 2022 [cit. 2022-05-07]. Dostupné z: https://csirt.cz/cs/o-nas/

[38] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST: *NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC* [online]. Brno: NÚKIB, 2015, [cit. 2022-05-07]. Dostupné z: https://www.nbu.cz/cs/aktualne/820-621-nbu-vybral-provozovatele-narodniho-cert-csirtcz-je-jim-cznic/

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

2.4 DRUHY KYBERNETICKÉ KRIMINALITY[40]

Kybernetická kriminalita zahrnuje velké množství trestných činů, ale jedno mají vždy společné. Tím je spojení kriminality s výpočetní technikou. Buď je „počítač“ terčem trestného činu, nebo je trestný čin proveden s jeho pomocí.

V zákoně č. 40/2009 Sb., trestní zákoník (TZ) jsou v § 230 až 232 definovány trestné činy v souvislosti s využitím počítače, kybernetické trestné činy. Níže uvádím statistiku těchto trestných činů v procesu od zjištění po odsouzení pachatele.

Tabulka 1: Přehled statistický údajů o skutcích dle § 230-232 TZ[41]

ROK	ZJIŠTĚNO	OBJASNĚNO	MÍRA OBJASNĚNOSTI (%)	STÍHÁNO	OBŽALOVÁNO	ODSOUZENO
2000	11	11	100	18	15	0
2001	24	20	83	22	14	2
2002	27	8	30	22	14	8
2003	33	5	15	14	7	0
2004	35	16	46	17	14	7
2005	37	17	46	33	27	1
2006	32	11	34	18	16	3
2007	48	13	27	14	12	1
2008	51	15	29	35	30	2
2009	62	20	32	21	16	4
2010	101	30	30	8	5	5
2011	134	54	40	41	31	17
2012	178	45	25	44	29	27
2013	301	76	25	49	42	27
2014	669	192	29	75	55	46
2015	707	144	20	167	113	51
2016	638	157	25	184	127	73
2017	784	206	26	176	116	111
2018	893	231	26	189	123	173
2019	1096	208	19	185	139	146

[40] POLICIE ČR: *Jednotlivé druhy kyberkriminality* [online]. Praha: Policie ČR, 2017 [cit. 2022-05-07]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[41] VLACH, Jiří, Kateřina KUDRLOVÁ a Viktorie PALOUŠOVÁ. Kyberkriminalita v kriminologické perspektivě. Praha: Institut pro kriminologii a sociální prevenci, 2020. Studie (Institut pro kriminologii a sociální prevenci). ISBN 978-80-7338-189-9.

2.4.1 Trestné činy proti autorskému právu

Dle trestního zákoníku zde patří:

- § 270 porušení autorského práva, práv souvisejících s právem autorským a práv k databázi.

Zde se jedná převážně o sdílení filmů, hudby a softwaru v rozporu s autorským právem.

2.4.2 Násilné a extremistické projevy

Dle trestního zákoníku zde patří:

- § 175 vydírání;
- § 353 nebezpečné vyhrožování;
- § 354 nebezpečné pronásledování;
- § 355 hanobení národa, rasy, etnické nebo jiné skupiny osob;
- § 356 podněcování k nenávisti vůči skupině osob nebo omezování jejich práv a svobod;
- § 357 šíření poplašné zprávy.

Pachatelé těchto trestných činů se schovávají za anonymitu kyberprostoru, většinou s využitím sociálních sítí *(Facebook, Twitter, Instagram, Snapchat atd.).* Právě zde šíří své názory a postoje, které jsou v rozporu se zákonem.

2.4.3 Mravnostní trestné činy

Dle trestního zákoníku zde patří:

- § 191 šíření pornografie;
- § 192 výroba a jiném nakládání s dětskou pornografii;
- § 193 zneužití dítěte k výrobě pornografie;
- § 193 a) účast na pornografickém představení;
- § 193 b) navazování nedovolených kontaktů s dítětem;
- § 201 ohrožování výchovy dítěte.

Zde se jedná o kontaktování osob mladších osmnácti let, tedy dětí a mladistvých, s úmyslem pořízení jejich intimních fotografií, videa nebo vylákání k osobní schůzce. Ke kontaktu jsou nejčastěji využívány sociální sítě, chaty anebo online hry. Po získání takového intimního

materiálu je tento dále šířen osobně v komunitě, v uzavřených fórech nebo za pomoci Darknetu.

Do této kategorie trestných činů spadají i delikty, které jsou směřovány vůči osobám zletilým. Zde se jedná o sexuální nátlak, kuplířství či obchodování s lidmi.

2.4.4 Kyberšikana[42]

Jedná se o šikanování jiné osoby pomocí informačních technologií – internetu, mobilních telefonů apod. *(např. vydírání, ubližování, ztrapňování, obtěžování, ohrožování, zastrašování)*.

Jako taková v trestním zákoníku definována není, ale její projevy se dají zařadit do několika trestných činů, například:

- § 175 vydírání;
- § 180 neoprávněné nakládání s osobními údaji;
- § 184 pomluva;
- § 192 výroba a jiném nakládání s dětskou pornografii;
- § 354 nebezpečné pronásledování.

Projevy šikany jsou především různé formy zastrašování, vydírání zasíláním urážlivých nebo pomlouvačných zpráv pomocí emailu, chatu, SMS či MMS. Řadíme sem i vytváření fotografií, videí nebo zvukových nahrávek, které jsou po různých úpravách urážlivé a mají za cíl poškodit oběť. Tyto materiály jsou následně veřejně umístěny nejčastěji na sociálních sítích typu Facebook, Instagram atp. Další variantou je vytvoření falešných profilů na sociálních sítích či internetových stránkách. Projevem kyberšikany může být i napadání, urážení či provokování na diskuzních fórech a chatech, které může být spojeno i s vydíráním oběti. Nelze opomenout ani obtěžování, které se projevuje neustálým voláním na mobilní telefon, psaní SMS, MMS, posíláním zpráv na Messenger, Twitter atp., takové jednání by se dalo označit jako kyberstalking.

Do kategorie kyberšikany je možné zařadit i tzv. sexting, což je rozesílání fotografií a videí se sexuální tématikou, kdy dochází k obtěžování, poškození nebo vydírání oběti.

---

[42] POLICIE ČR: *Víte co je KYBERŠIKANA?* [online]. Policie ČR, 2009 [cit. 2022-05-07]. Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

Nejvíce nebezpečné jednání, jež se zařazuje pod kyberšikanu je tzv. kybergrooming. Tento termín označuje jednání osoby, která se snaží zmanipulovat vyhlédnutou oběť *(nejčastěji pomocí chatu, SMS zpráv, ICQ a Skypu)* a donutit ji k osobní schůzce. Výsledkem schůzky může být sexuální zneužití oběti, fyzické mučení, nucení k terorismu apod.

2.4.5 Podvodná jednání

Dle trestního zákoníku zde patří:

- § 209 podvod;
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací.

Mezi tyto skutky lze zařadit podvodné e-shopy, které vznikají pod záminkou vylákání finančních prostředků a po krátké existenci takový e-shop zaniká. Současně jsou finanční prostředky zpravidla vyvedeny mimo území našeho státu za účelem anonymizace finančních toků, případně jsou využívány virtuální měny. Obdobný je postup v rámci podvodných inzerátů, sbírek a také jednání známé jako tzv. Nigerijské podvody.

Do daného jednání lze zahrnovat také podvody prostřednictvím podvržených emailů nebo krádeže peněz z bankovních účtů za pomoci phishingu. Phishing je forma útoku, kdy se pomocí technik sociálního inženýrství útočník vydává za důvěryhodnou autoritu s cílem získat citlivá data (přihlašovací údaje).

Nigerijské podvody – pod falešnými záminkami *(falešné výhry, falešné dědictví, celní poplatky, falešní vojáci, falešné dary, získání půjčky, snadný výdělek)* se pachatel snaží z oběti vylákat finanční prostředky. Oběť osloví pomocí emailu, na sociálních sítích nebo na různých seznamkách, kdy jim sdělí, že mohou získat značnou sumu peněz a jediné, co je třeba udělat, je zaplatit malý obnos, poplatek. Poplatků bývá ve většině případů několik. A nezřídka se stává, že si na tyto poplatky oběť vezme i úvěr.

2.4.6 Hacking

Dle trestního zákoníku zde patří:

- § 175 vydírání;
- § 180 neoprávněné nakládání s osobními údaji;
- § 182 porušení tajemství dopravovaných zpráv;
- § 209 podvod;
- § 230 neoprávněný přístup k počítačovému systému a nosiči informací;

- § 354 nebezpečné pronásledování.

Nejčastěji prošetřovaným trestným činem z této kategorie je jednání pachatele, který překoná zabezpečení počítačového systému a získá přístup k údajům oběti, s nimiž může dál libovolně nakládat. Součástí těchto jednání bývá mimo jiné šíření škodlivých kódů, implementace tzv. backdoorů do volně přístupných software atp. Stále častější formou je napadení emailových účtů, účtů na sociálních sítích, účtů internetového bankovnictví. Následkem je průnik do soukromí, získávání citlivých informací s možností jejich poškození či zničení nebo získání finančního prospěchu.

S tím souvisí i další navazující trestná činnost *(vydírání, nebezpečné pronásledování, krádeže z účtů, podvody)*. Součástí tohoto druhu trestné činnosti jsou i kybernetické útoky *(např. Ddos)* nebo vydírání prostřednictvím ransomware.

Další formou může být zachytávání probíhající komunikace, což se označuje jako sniffing. Pachatel získává citlivé údaje nejen o provozu, ale i obsahu komunikace. Děje se tak často na nezabezpečených wi-fi připojeních *(tzv. Freewifi, jež jsou běžné v kavárnách, obchodních centrech či v centrech měst)*, na straně zmanipulovaných emailových serverů a poslední dobou i na napadených domácích routerech. Pachatelé se pak dostávají k citlivým údajům, jako jsou hesla, platební údaje či citlivý osobní případně intimní obsah, který pak využívají k nátlaku na oběť se snahou o vlastní finanční obohacení nebo alespoň poškození pověsti oběti.

2.4.7 Blagging

Dle trestního zákoníku zde patří:

- § 209 podvod.

Blagging využívá sociálního inženýrství k získání finanční hotovosti pomocí podvodu. Riziku jsou zde vystaveni nejen jednotlivci, ale také obchodní společnosti. Jedním z hlavních představitelů těchto podvodů, který využívá sociálního inženýrství je tzv. CEO – Command Executive Order – jde o fiktivní příkaz oprávněného k provedení nějaké činnosti, v tomto případě platby na účet. Tyto typy podvodů jsou ve většině případů vytvořeny na základě velmi dobrých znalostí trhu, struktury a zákazníků dané společnosti. Získané informace bývají zneužívány k přesvědčivé argumentaci, aby byly oběti snáze zmanipulovány k provádění požadovaných aktivit. Jedním z typických scénářů je, že se pachatelé pro navázání kontaktu vydávají např. za ředitele firmy *(např. Prezident, CEO, CFO)* nebo důvěryhodného

partnera společnosti *(např. právníci, notáři, auditoři, účetní)*. Pod touto záminkou pak kontaktují konkrétního zaměstnance firmy s tím, že byli osloveni např. výkonným ředitelem ve věci splatnosti jisté pohledávky či uzavření smlouvy. Takový postup přiměje zaměstnance firmy k proplacení pohledávky, faktury či jiné interakci.

2.4.8 Odcizení výpočetní techniky

Dle trestního zákoníku zde patří:

- § 205 krádež.

Z hlediska kriminality se jedná o jednání na pomezí mezi klasickou kriminalitou a kyberkriminalitou, ale nelze ji opomíjet. Krádeží výpočetní techniky se rozumí odcizení počítače (serveru, routeru, switche atp.), souvisejícího HW, instalovaného SW a dat v něm obsažených. Většinou nejcennější pro majitele odcizené výpočetní techniky není HW ani SW, ale data v něm obsažená, pokud nejsou uživatelem pravidelně ukládána na cloud. Z hlediska pachatele je nejcennější právě odcizený HW.

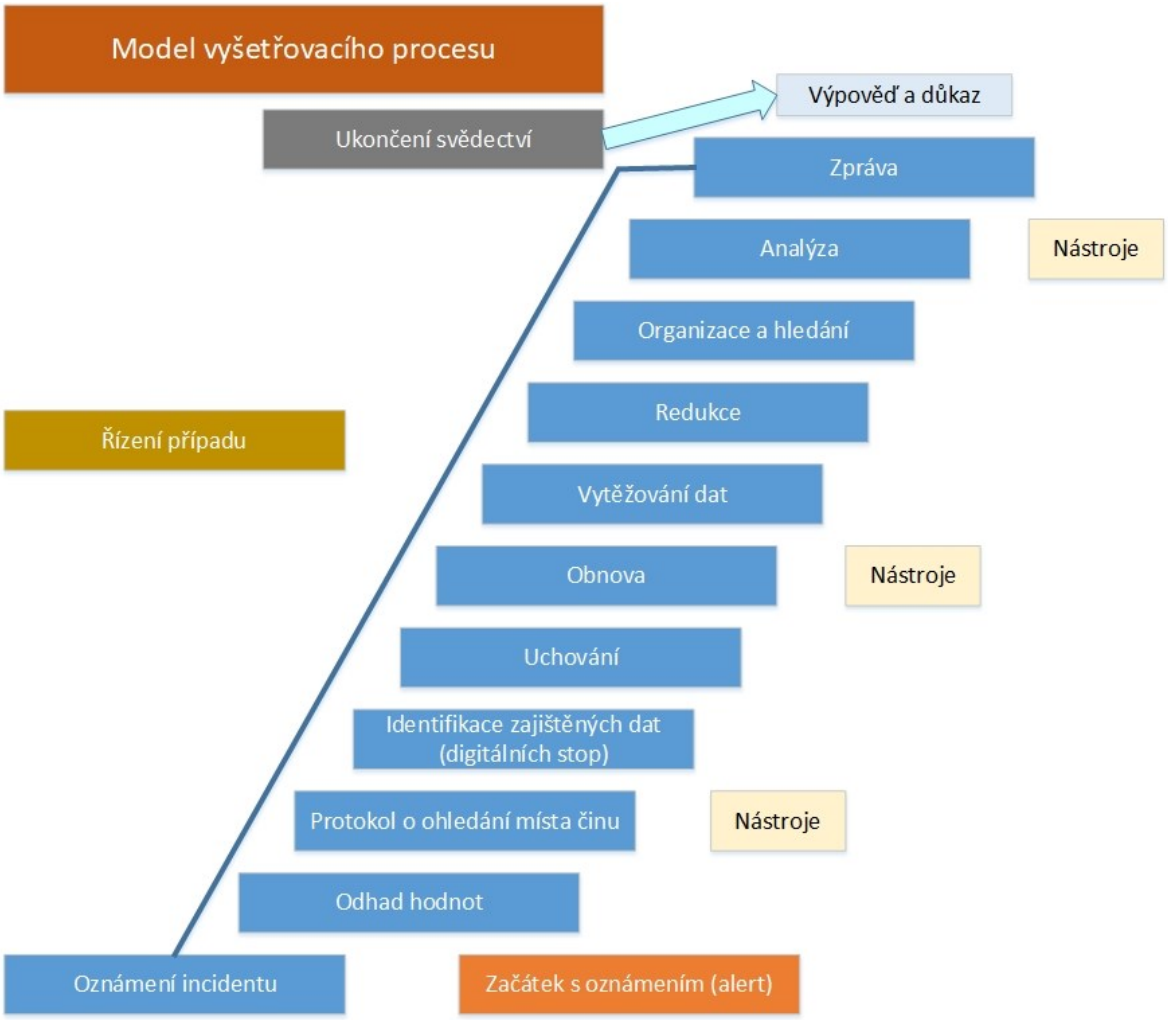
DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

V první části mé diplomové práce jsem se věnoval objasnění teorie a základních pojmů, jejichž znalost považuji za velmi důležitou pro orientaci v problematice kybernetické kriminality. Podstatné je především definování kyberprostoru a jeho chápání při užití k závadné činnosti. Uváděné definice z kybernetického prostředí a z oblasti kriminalistiky vnímám jako nezbytné pro pochopení a využití praktické části práce, jejíž těžiště spočívá ve vytvoření metodiky vyšetřování kybernetické kriminality.

II. PRAKTICKÁ ČÁST

3 METODIKA VYŠETŘOVÁNÍ KYBERNETICKÉ KRIMINALITY

Vyšetřování kybernetického trestného činu je obtížná činnost, která s sebou nese hodně problémů. Nejdůležitějším problémem je problém legislativní, kdy sice máme kvalitní nástroje hmotného práva k potírání kybernetické trestné činnost, ale neřeší a nemohou řešit vše, mimo jiné jsou i omezeny procesně právní stránkou, jež se týká zákonné možnosti získávání a zajišťování důkazů, jejich vyhodnocování, průkaznosti forenzních analýz a znaleckých posudků stanovených trestním řádem.



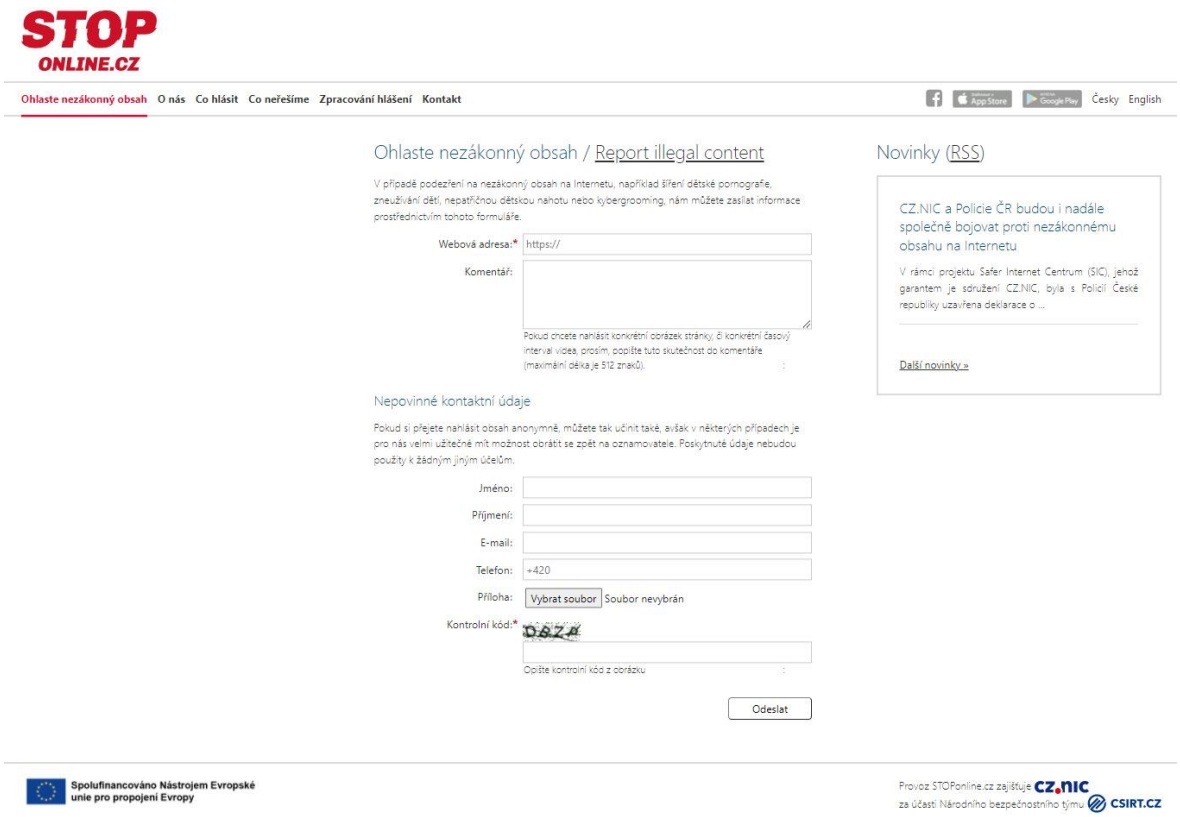
Obrázek 7: Model vyšetřovacího procesu [43]

[43] POŽÁR, Josef a Václav HNÍK, *Specifické problémy boje s kybernetickou kriminalitou* [online]. Praha: Policejní akademie ČR. Dostupné z: https://slideplayer.cz/slide/11176990/

3.1 Zjištění trestného činu

Jednou z nejzákladnějších částí procesu vyšetřování, nejen kybernetické kriminality, je její zjištění. Nejčastěji bývá zjištěna formou oznámení ze strany poškozeného, ale může být realizována formou operativně pátrací činnosti služby kriminální policie a vyšetřování, oznámením kontrolních, inspekčních, či revizních orgánů různých institucí, zejména v bankovním sektoru.

Oznámit kybernetický trestný čin na Policii ČR či u jiného z orgánů činného v trestním řízení (OČTŘ) lze formou ústní, telefonicky, písemně i elektronicky využitím formuláře. Hlášení prostřednictvím formuláře již není na internetových stránkách Policie ČR. Z praktických důvodů se od 24. května 2018 přesunulo pod sdružení CZ.NIC, s nímž Policie ČR spolupracuje. Formulář je dostupný na adrese *„https://www.stoponline.cz“*.[44]



Obrázek 8: Formuláře hlášení nezákonného obsahu na internetu[45]

[44] POLICIE ČR: *Ukončení provozu HOTLINE* [online]. Praha: Policie ČR, 2018 [cit. 2022-05-07]. Dostupné z: https://www.policie.cz/clanek/ukonceni-provozu-hotline.aspx

[45] STOPONLINE.CZ: *Ohlaste nezákonný obsah / Report illegal content* [online]. Praha: CZ.NIC, z. s. p. o., 2022 [cit. 2022-05-07]. Dostupné z: https://www.stoponline.cz/cs/

Řada skutků, které by mohly být kvalifikovány jako trestné činy, bývá policií i poškozenými neodhalena nebo neoznámena. Jelikož je v podmínkách ČR kladen důraz na objasněnost trestných činů a objasněnost kybernetických trestných činů je nízká, bývají případy s malou nadějí na objasnění a dopadení pachatele často neevidovány. Poměrně časté je neohlášení skutků, které by snižovaly důvěryhodnost instituce nebo firmy v očích společníků, zaměstnanců, ale především zákazníků, typickým příkladem jsou banky a jiné finanční instituce.

Podle TŘ ČR mají státní orgány povinnost neprodleně oznamovat státnímu zástupci nebo policejním orgánům (OČTŘ) skutečnosti nasvědčující tomu, že byl spáchán trestný čin.

Obrázek 9: Zjednodušené schéma zahájení úkonů trestního řízení[46]

Při přijetí oznámení od oznamovatele je při řešení kyberkriminality velmi důležité precizní zpracování a zajištění prvotních informací a důkazů, tzn. co nejpodrobněji zajistit informace týkající se kybernetického útoku, jenž možnému trestnému činu předcházel. Nejlépe je zajistit od oznamovatele nezměněná data ve formě originálních e-mailových zpráv, nosiče dat (paměťové disky atp.) nebo celý počítačový systém. Pokud uvedené není možné, zajišťujeme alespoň kopie.

Pokud je z obsahu trestního oznámení patrné, že se jedná o trestný čin, postupuje policejní orgán se svou věcnou příslušností. V prvních fázích je sepsán Záznam o zahájení úkonů trestního řízení (dle TŘ). Bez výše uvedeného dokumentu není možné provádět další trestněprocesní úkony. Obecně je doporučováno postupovat u kybernetických trestných činů obdobně jako v případech běžných trestných činů.

Na základě analýzy trestního oznámení a přihlédnutí ke všem informacím získaným během prověřování oznámení by měl orgán činný v trestním řízení určit, o jaký druh kybernetického útoku se jedná a zařadit skutkovou podstatu pod některý z trestných činů.

---

[46] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. CZ.NIC. ISBN 978-80-88168-15-7.

Orgán činný v trestním řízení by se měl po celou dobu vyšetřování snažit odpovědět na základní kriminalistické otázky, které směřují k objasnění trestného činu a odhalení totožnosti pachatele a jeho motivu.

Sedm základních kriminalistických otázek:

- **Kdo** je potenciální podezřelý?
- **Co** za zločin bylo spácháno?
- **Kdy** byl zločin spáchán?
- **Kde** mohou být umístěny fyzické nebo digitální důkazy?
- **Jak** byl čin spáchán?
- **Proč**?
- **S kým**?

Dále se uvádí otázka „**Za kolik**?“, která nám vyčísluje škodu způsobenou trestným činem.

Problémem při zjištění trestného činu v kyberprostoru je určení místní příslušnosti orgánu činného v trestním řízení. Určení místní příslušnosti je uvedeno v trestním řádu, kde se píše že:

1) Řízení koná soud, v jehož obvodu byl trestný čin spáchán.
2) Nelze-li místo činu zjistit nebo byl-li čin spáchán v cizině, koná řízení soud, v jehož obvodu obviněný bydlí, pracuje nebo se zdržuje; jestliže se nedají tato místa zjistit nebo jsou mimo území České republiky, koná řízení soud, v jehož obvodu čin vyšel najevo.

Ad. 1) nelze ve většině případů aplikovat z důvodů celosvětového charakteru Internetu, nelze zjistit místo spáchání trestného činu (místem spáchání trestného činu je kyberprostor). Z výše uvedeného se aplikuje ad. 2) – koná řízení soud (OČTŘ), v jehož obvodu čin vyšel najevo.[47]

[47] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. CZ.NIC. ISBN 978-80-88168-15-7.

3.2 Zajištění důkazního materiálu

Dle § 89 TŘ lze za důkaz považovat vše, co může přispět k objasnění věci, zejména výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a ohledání. Pro objasnění trestného činu je cílem zajistit co možná nejvíce věrohodných. Mezi procesy, jež nám mohou přispět k získání důkazů, je i ohledání místa činu. Tzv. prvotní ohledání by mělo být co nejefektivnější, jelikož OČTŘ má k dispozici nezměněnou strukturu ohledávaného objektu. Dále lze provádět opakované či doplňující ohledání místa činu.

Místem činu se rozumí výchozí bod vyšetřování, často jde o jediné místo, kde je možné nalézt stopy po činnosti pachatele trestného činu. V kybernetické kriminalitě se bude nejčastěji jednat o místo s počítačovým systémem, kde byla podezřelá činnost zjištěna poškozeným.

Při tomto procesu může být využit institut domovní prohlídky dle § 82 TŘ. Dle § 83 TŘ může domovní prohlídku nařídit předseda senátu a v přípravném řízení na návrh státního zástupce soudce. V neodkladných případech tak může namísto příslušného předsedy senátu nebo soudce učinit předseda senátu nebo soudce, v jehož obvodu má být prohlídka vykonána. Příkaz k domovní prohlídce musí být vydán písemně a musí být odůvodněn.

Obdobně (dle § 83 TŘ) jako institut domovní prohlídky může být k zajištění důkazního materiálu nařízen i příkaz k prohlídce jiných prostor a pozemků.

Na místě ohledání mohou být nalezeny důkazy, které by se daly zařadit do dvou kategorií:

1) fyzické důkazy;
2) digitální důkazy.

3.2.1 Fyzické důkazy

Mezi fyzické důkazy můžeme zařadit důkazy věcné a listinné. V kybernetické kriminalitě by věcné důkazy byly samotné počítačové systémy (servery) nebo paměťová média (CD, DVD, flash disky, pevné disky, datová uložiště, mobilní telefony, tiskárny atp.), jež obsahují určitá data a informace, které by mohly mít vztah k vyšetřovanému trestnému činu. Nelze opomenout ani tzv. listinné důkazy. Listina v TŘ není definována, tudíž lze za listinu považovat jakýkoli předmět, kde je uveden písemný či grafický projev. Z toho vyplývá, že za listinný důkaz lze považovat nejen papír, ale jakékoli médium schopné zaznamenat písemný či grafický projev.

Při zajišťování fyzických důkazů se postupuje obdobně jako při zajišťování důkazů běžných trestných činů (pořízení podrobné fotodokumentace, videodokumentace, vytvoření náčrtku atp.). Je důležité zaznamenat, jak byl počítačový systém zapojen (jednotlivá propojení kabelů), o jaký druh kabelu se jedná, identifikace ISP poskytujících připojení a jiné služby, zda je do zařízení připojeno paměťové médium a druh tohoto paměťového média. Platí základní pravidlo: nic nevytahovat a vše konzultovat na místě se znalcem v oboru. Ten je schopen nejen poradit, ale především určit a zaznamenat topologii sítě na místě činu (při domovní prohlídce či prohlídce jiných prostor a pozemků).

Dle trestního řádu může vyšetřovatel při vyšetřování využít i úkony vydání a odnětí věci, které jsou vymezeny v ustanovení § 78 a 79 TŘ. Za věc se v rozumí vše, co je rozdílné od osoby a co slouží potřebě lidí. V § 78 TŘ je zakotvena povinnost každého předložit věc důležitou pro trestní řízení na výzvu OČTŘ, případně tuto věc vydat. Výzva k vydání věci není nijak formalizována a v přípravném řízení ji může policejní orgán vydat písemně i ústně. Pokud osoba věc nevydala dobrovolně, může být na příkaz předsedy senátu a v přípravném řízení na příkaz státního zástupce či policejního orgánu odňata. Při odnětí věci by měla být přítomna nezúčastněná osoba. O vydání věci musí být sepsán protokol dle § 55 TŘ, ve kterém je nutné detailně popsat odebranou věc. Dále je nutné vydat písemné potvrzení o převzetí věci, a to i v případě, že jej osoba nevyžaduje.

Seznam protokolů, jež mohou být využity při provádění úkonů trestního řízení, je uveden níže:

- Protokol o ohledání místa činu, dle § 113 TŘ;
- Protokol o provedení domovní prohlídky, dle § 82 TŘ;
- Protokol o provedení prohlídky jiných prostor a pozemků, dle § 82 TŘ;
- Protokol o odnětí věci, dle § 79 TŘ;
- Protokol o vydání věci, dle § 78 TŘ.

3.2.2 Digitální důkazy

Digitální důkazy jako takové nejsou v TŘ definovány a subsumpce pod věcné ani listinné důkazy není vhodná. V knize „Cybercrime“ Kolouch uvádí, že by bylo vhodné zavést novou kategorii důkazů, kterou by definoval následovně:

„Digitálním důkazem jsou jakákoli data či informace, jež byly přeneseny, vytvořeny, uloženy či modifikovány za použití počítačového systému a které prokazují nebo vyvracejí dokazovanou skutečnost a mohou být prostředkem k odhalení a zjištění trestného činu a jeho pachatele, jakož i stopy trestného činu.“[48]

Digitální důkazy jsou obsaženy ve formě různých typů souborů (txt, jpg, jpeg. Gif, mp4, doc, xml, ppt, avi, iso, rar, zip, exe, bat, pdf atd.). Tyto soubory jsou obsaženy v zařízeních ICT, které jsou zařazeny pod věcné důkazy. Je třeba s nimi zacházet obezřetně, a pokud možno využívat při jejich zajištění odborníka z oboru ICT. V dnešní době je téměř každé elektronické zařízení schopno zaznamenat a dále šířit některá data, jež mohou být dále využita jako digitální důkazy. V tabulce níže uvedu příklady vybraných elektronických zařízení obsahující možné digitální důkazy:

Tabulka 2. Elektronická zařízení obsahující možné digitální důkazy[49]

Zařízení	**Možné digitální důkazy**	**Příklady koncovek souborů**
Počítač,	Dokumenty	Doc, txt, docx, pdf
Mobilní telefon (smartphone),	Archivy	Zip, rar, arj
	Obrázky	Jpg, jpeg, gif, png, bmp
Tablet	Videa	Waw, avi, wmv, flv
	Lokace	Loc
	Procesní logy	Log
	Audio záznamy	Mp3, ogg, wma
	Historie prohlížení	Html
	E-maily / chat	Eml, msg
Herní konzole	Obrázky	Jpg, jpeg, gif, png, bmp
	Videa	Waw, avi, wmv, flv
	Dokumenty	Doc, txt, docx, pdf

[48] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. CZ.NIC. ISBN 978-80-88168-15-7.
[49] Vlastní.

Digitální fotoaparát	Obrázky Videa Lokace	Jpg, jpeg, gif, png, bmp, raw Waw, avi, wmv, flv

Výše uvedená tabulka ukazuje, že v každém zařízení je možné zjistit mnoho rozdílných digitálních důkazů, které nám mohou pomoci určit lokaci pachatele či oběti, jeho historii procházení Internetu (webových stránek), telefonické, e-mailové a chatovací kontakty i historii připojení k internetovým providerům, jejich rozmístění a čas připojení.

Všechny takto získané informace nám mohou pomoci při odhalení kybernetického trestného činu. Vedle toho jsou užitečné i při odhalování běžných trestných činů.

Obecný postup zajištění digitálních důkazů:

1. Ihned zamezit jakékoliv činnosti uživatele na zajišťovaném zařízení, jenž může být nositelem digitálních důkazů.
2. Pořízení fotodokumentace nebo videozáznamu aktuálního stavu zařízení v místě nálezu, fyzického stavu, zapojení kabelů a všech ostatních periferií k zařízení připojených (monitory, klávesnice, myši, flash disky, přenosné disky atp.).
3. Pokud je zařízení spuštěno, přítomný znalec v oboru ICT nebo specialista na zajišťování dat, v přítomnosti nezúčastněné osoby, provede prvotní ohledání zařízení se zaměřením na spuštěný software, připojené síťové disky, nastavení systému apod.
4. Pokud je to možné, vyslechnout uživatele zařízení se zaměřením na způsob užívání zařízení, sdělení přístupových hesel, zdali je v zařízení užito šifrování atd.
5. Jedná-li se o PC a je spuštěn a není zjištěno užití šifrování, které by po vypnutí PC znemožnilo provedení další analýzy, je možné PC vypnout, a to pouze vytažením napájecího kabelu ze zásuvky elektrické sítě. Tím se zachová obsah dočasné paměti na pevném disku počítače.

   Pokud je v PC nějaká možnost, že by po jeho vypnutí mohl být spuštěn nějaký šifrovací nástroj, který by poté nebylo možné rozšifrovat, nebo by hrozila možná ztráta digitálních důkazů z jiného důvodu, zajistí se data z tzv. živého zařízení. To lze například vytvořením bitové kopie disku nebo forenzní analýzy zařízení. Tento postup provádí znalec na místě, případně se celé spuštěné zařízení převeze do znalecké laboratoře.

6. Při vypnutém PC se ze zařízení zajistí pouze vlastní skříň PC, ve které je umístěna procesorová jednotka a pevné disky. Pokud se jedná o notebook, tablet a mobilní telefon, vždy se zajišťuje jako celek i s napájecím zdrojem. Zajištěné zařízení se zabalí proti neautorizované manipulaci (příklad viz obrázek níže) a zdokumentuje se.
7. O provedených úkonech se sepíše protokol obsahující přesný popis zařízení, jeho typ, sériové či výrobní číslo, technické parametry aj. Pokud je možné k zařízení zajistit i technickou dokumentaci od výrobce, přiloží se k protokolu.

Obrázek 10: Příklady zabalení proti neautorizované manipulaci[50]

Tento zobecněný postup k zajištění digitálních důkazů je možné aplikovat na většinu zařízení ICT, které by mohly přispět k objasnění kybernetického trestného činu. Pokud to okolnosti případu dovolí, při prvotním ohledání je vhodná osobní přítomnost majitele či uživatele zařízení. Pokud jejich přítomnost není možná, využívá se institutu nezúčastněné osoby.

Další možností získání digitálních důkazů je přímé zajištění dat, které se provádí tzv. vykopírováním konkrétních dat, např. ze síťového serveru (mail server, cloud server) na paměťové médium. Takto získaná data je nutno opatřit, kvůli autentizaci, kontrolními otisky hash (MD5, SHA-1 nebo SHA-2). Při těchto úkonech je opět nezbytná přítomnost nezúčastněné osoby, vlastníka nebo správce dat. Výjimkou je zajišťování dat z veřejných zdrojů, zde se přítomnost výše uvedených osob nevyžaduje. Způsob zajištění dat pro získání digitálních důkazů navrhuje, s přihlédnutím na typ zajišťovaných dat, znalec v oboru nebo specialista

[50] VYSKOČIL, Ladislav. *Zajišťování a analýza digitálních důkazů*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 105 s. Dostupné také z: http://hdl.handle.net/10563/24882. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav informatiky a umělé inteligence. Vedoucí práce Malaník, David.

na zajišťování dat a vyšetřovatel se na základě informací od odborníků rozhoduje, jaký způsob zvolí.

3.3 Vytěžení získaných důkazů

Po zajištění věcí, jež by mohly být nápomocny k vyšetření trestného činu, v našem případě kybernetického trestného činu, je nutné získat digitální důkazy. Postupů forenzní analýzy digitálních dat je nepřeberné množství. Ke každému digitálnímu médiu se přistupuje individuálně s přihlédnutím k charakteru případu a k otázkám, na něž hledáme odpověď.

Při forenzní analýze má znalec k dispozici velké množství komerčních i volně šiřitelných nástrojů. Volba konkrétního nástroje záleží pouze na uvážení znalce a jeho zhodnocení dané situace. Nikde není stanoveno pravidlo uvádějící, který nástroj by se měl či neměl v konkrétním případě používat. Nesmíme opomenout, že k forenzní analýze se nepoužívá zajištěné digitální médium. Samozřejmostí je využití vytvořené bitové kopie daného média či dokonce kopie této kopie.

3.3.1 Vytvoření bitové kopie digitální stopy

Vlastnímu vytváření bitových kopií předchází příprava. Zde si zjistíme všechny potřebné údaje, tedy kapacity jednotlivých paměťových médií a jejich datové rozhraní. Tyto informace použijeme k přípravě technologického disku, na kterém bude bitová kopie vytvářena. Technologický disk musí mít větší kapacitu než paměťové médium, u kterého bude bitová kopie vytvářena. Před zahájením uváděného postupu je nezbytné technologický disk vymazat, zde se nepoužívá formátování, ale vymazání dat, protože pouze takový postup je skutečným procesem odstranění dat a je nemožné získat data z vymazaného disku. K tomuto účelu je mnoho nástrojů, pro OS Windows software WipeDisk nebo jako další varianta použití příkazu v příkazovém řádku „diskmgmt.msc“ s následným výběrem disku, který chceme vymazat a další.

K vytvoření bitové kopie je možné využít několik způsobů, vždy záleží na okolnostech a na rozhodnutí znalce, jenž tyto bitové kopie dat bude vytvářet. Znalec nejčastěji pracuje se čtyřmi základními postupy vytvoření bitové kopie dat:

1) pomocí jednoúčelového zařízení, tzv. „disk duplicator“ nebo taky „disk imager“;
2) pomocí zkoumaného zařízení;
3) prostřednictvím počítačové sítě;
4) ze „živého“ (zapnutého) zkoumaného zařízení.

Způsob vytvoření bitové kopie dat dle ad 1) je hojně využíván při zajištění jednotlivých paměťových médií (hard disky počítačů, SSD i HDD, externí disky). Lze jej využít i při zajištění celého počítače, kdy po zadokumentování jsou z počítače vyjmuty jednotlivé disky (pokud jich je více) a jsou vytvořeny jednotlivé bitové kopie pomocí jednoúčelového zařízení, disk duplikátoru. Tento jednoúčelový stroj nám vytvoří bitovou kopii disku a poté provede výpočet kontrolního součtu MD5, SHA-1 či SHA-2 dle nastavení. Výhoda použití disk duplicatoru je v jeho jednoduché obsluze, nevýhodou je jeho vysoká pořizovací cena.

Obrázek 11: Disk duplicator TABLEAU TD3 Forensic Imager[51]

[51] Vlastní foto.

Obrázek 12: Disk duplicator CRU WiebeTech Forensic UltraDock[52]

Jako další varianta se nabízí využití investigativního technologického počítače a následné provedení bitové kopie disku. Uvedený technologický počítač by měl být schopen připojení pomocí všech rozhraní paměťových médií, výhodou pro další práci je nainstalování některé z distribucí OS Linux, např. Kali, Onion, které se pro investigaci využívají.

[52] Vlastní foto.

Obrázek 13: Příklad investigativního technologického počítače[53]

Při vytváření bitové kopie pomocí investigativního počítače je důležité neopomenout rozdíly v připojení datového média pod operačním systémem Microsoft Windows a některou z distribucí Linuxu. Při použití OS Microsoft Windows je charakteristické, že při připojení disku dochází ihned k zápisu na toto médium, což považujeme za problematické a nežádoucí. Tento problém se při využívání operačního systému Linux neobjevuje, systém je konstruován tak, aby k zápisu na paměťové médium bez vědomí uživatele nikdy nedocházelo. Právě proto jsou ve forenzní praxi tak oblíbené různé distribuce investigativních Linuxů.

To ale neznamená, že bychom OS Microsoft Windows nemohli použít, jen je nutné zápisu na zajištěné paměťové médium zabránit. Existují speciální hardwarová zařízení či softwary pro blokování zápisu, které neumožní, aby k zápisu na médium došlo.

Několik příkladů zajištění digitálních uložišť z různých zařízení (nejčastěji počítač) pro další forenzní analýzu k získání digitálních stop pro potřeby vyšetřování kybernetické kriminality je uvedeno v příloze P I: Návrh metodiky k zajištění digitálních důkazů, která je součástí této práce. Způsoby uvedené v příloze jsou doporučovány Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) a jsou zveřejněny na jeho internetových stránkách.

[53] Vlastní foto.

3.3.2 Autentizace digitální stopy

Už při zajišťování zařízení nebo paměťového média musíme brát na zřetel, že obsahuje digitální stopu nebo stopy, které můžou být předloženy jako důkazy soudu. Jako každý důkazní materiál musí být zabezpečena jejich pravost a musí být zajištěno, aby data v nich obsažena nebyla nijak pozměňována. Z výše uvedeného je patrné, že i digitální stopy se musí autentizovat. Při tomto se používá několik metod:

1) Zabalení a zapečetění média či zařízení obsahující digitální stopu. Zde se využívá postupů jako u každé materiální stopy, tj. jejím zabalením a zapečetěním a podpisem zajišťující osoby. Autentizací se v tomto případě rozumí kontrola neporušenosti obalu, ověření pravosti podpisu a pečeti.
2) Dále se u zajištění digitálních stop vytváří kontrolní otisk hash. Toto se používá při přímém zajištění dat, např. u „živého“ zařízení, a vytváření bitové kopie či vykopírování souborů z něj. Výpočet kontrolního otisku může být proveden několika hlasovacími funkcemi. Vhodnost použití konkrétní hashovací funkce volíme tak, aby její použití mělo nejvyšší možnou míru bezpečnosti. Nejčastěji se v praxi používají hashovací algoritmy MD5, SHA-1 a SHA-2.

Hashovací algoritmy:

- **MD-5** (Message-Digest algorithm) – vytváří se otisk o velikosti 128 bitů a je popsán v internetovém standardu PFC 1321. Jeden z nejvíce užívaných hashovacích algoritmů. Využívá se pro svou rychlost, ale již bývá nahrazován bezpečnějšími algoritmy skupiny SHA.
- **SHA-1** (Secure Hash Algorithm) – kontrolní otisk o velikosti 160 bitů. Byl navržen NSA (Národní bezpečnostní agentura USA). I tento kontrolní otisk (součet) je v dnešní době považován za méně bezpečný a je doporučeno jej nahradit algoritmy rodina SHA-2.
- **SHA-2** – do skupiny algoritmů SHA-2 se řadí hashe, které jsou nazývány podle své délky v bitech. Jedná se o: SHA-224, SHA-256, SHA-384 a SHA-512. V praxi se nejvíce používá SHA-256 a SHA-512. U skupiny hashovacích algoritmů SHA-2 doposud nebyly nalezeny bezpečnostní kolize.

Kontrolní součty jsou vytvářeny již při vytváření bitových kopií, což jsme si ukázali při použití jednoúčelového zařízení, disk duplicatoru či při vytváření bitové kopie za pomoci OS Linux.

Kontrolní otisky a způsob zabalení a zapečetění média či zařízení musí být uveden v „Protokolu o zajištění dat“.

4 PŘÍNOS METODIKY A JEJÍ REÁLNÁ POUŽITELNOST V PRAXI

Problematika vyšetřování kybernetické kriminality je velmi rozsáhlá a ke každému případu, který je odhalen, se musí přistupovat zcela individuálně. Z tohoto důvodu je předkládaná metodika obecným doporučením pro vyšetřovatele, která mu ukazuje základní principy postupu na místě činu a pomáhá se v problematice lépe zorientovat.

V teoretické části uvádím všechny základní prvky a názvosloví, bez nichž se vyšetřovatel v této oblasti neobejde.

Za hlavní přednost své metodiky považuji zjednodušení a zpřehlednění popisované problematiky a tím její snadnou využitelnost v praxi. Reálné využití spatřuji zejména v přílohách P I. a P II. Obě jsou navrženy i pro samostatné použití.

DÍLČÍ ZÁVĚR PRAKTICKÉ ČÁSTI

Do praktické části diplomové práce jsem se pokusil přenést své poznatky z praxe a tím pomoci vyšetřovateli kybernetického trestného činu v jeho nelehké práci.

V textu se zabývám postupy směřujícími k zjištění možných digitálních stop, základními způsoby jejich zajištění a ochranou proti neautorizovanému zásahu. Nastínil jsem možnosti vytvoření bitových kopií za použití jednoúčelového zařízení, technologického investigativního počítače i s využitím vlastního zajišťovaného zařízení. Pro popis postupů jsem zvolil dva nejčastěji využívané operační programy – OS Microsoft Windows a OS Linux.

V předkládané práci se snažím projít úkony, jež je nutné provést při prvotním ohledání místa činu a které by měl mít vyšetřovatel vždy pod kontrolou, neboť mu pomohou při řízení ohledání a vyšetřování kybernetického trestného činu.

Svou metodu považuji za odlišnou, protože se snažím vžít do situace vyšetřovatele, projít s ním celým procesem na místě činu a pomoci mu při prvotních úkonech vyšetřování. Jsem přesvědčen, že praktická část této práce může vyšetřovateli sloužit jako užitečná příručka a základní návod pro jeho práci.

Páchání kybernetické kriminality je stále se vyvíjející činností a není v mých schopnostech ani v rozsahu této diplomové práce nastínit všechny možnosti, které vyšetřování těchto činů vyžaduje. Ke každému kybernetickému trestnému činu se musí přistupovat individuálně, s maximální pečlivostí a odpovědností.

ZÁVĚR

Internet je všudypřítomný a získává si stále větší množství lidí i věcí. V dnešním světě je téměř vše možné připojit k Internetu. Nejedná se jen o počítače, mobilní telefony a tablety. K internetové síti připojíme televize, ledničky, bez jeho fungování se dnes neobejdou dodavatelé energií, finanční instituce, orgány státní správy a samosprávy, soukromé firmy ani nemocnice.

S rozmachem Internetu a jeho využíváním v čím dál běžnějších denních činnostech stoupá i kybernetická trestná činnost a je třeba mít na paměti, že se kdykoli může dotknout každého z nás. Proti tomuto se nelze bránit pouze jako jednotlivec a musí v být nápomocen i stát.

V České republice již proběhla částečná implementace problematiky kybernetické kriminality do trestního práva a napomáhá vyšetřovatelům ke stanovení skutkové podstaty trestného činu. Tato implementace se stále ukazuje jako nedostatečná, neboť kybernetická trestná činnost je mezi ostatní trestnou činností stále na chvostu v objasněnosti, odhalení pachatele a jeho odsouzení.

Smyslem předkládané diplomové práce bylo nastínění problematiky kybernetické kriminality a vytvoření metodických postupů pro vyšetřovatele. Jejich cílem je poskytnutí základních znalostí, které považuji za potřebné pro zdárné ukončení vyšetřování, odhalení pachatele a jeho odsouzení.

Věřím, že Internet a jeho možnosti jsou pro lidstvo obrovským přínosem, pomáhají nám při každodenních činnostech, práci a jsou i prostředníkem pro zábavu. Proto by toto prostředí mělo být bezpečné a nekalá činnost v on-line prostoru důsledně potírána.

CITOVANÁ LITERATURA

[1] ABCLinuxu: *MAC adresa* [online]. Praha: Nitemedia, 2009 [cit. 2022-05-07]. Dostupné z: https://www.abclinuxu.cz/slovnik/mac-adresa

[2] CISO Platform: *CISO Guide: Surface Web, Deep Web and Dark Web - Are they different?*. CISO Platform [online]. Bangalore, Indie: CISO Platform, 2018, 18. 4. 2018 [cit. 2022-05-07]. Dostupné z: https://www.cisoplatform.com/profiles/blogs/surface-web-deep-web-and-dark-web-are-they-different

[3] CSIRT.CZ: *O týmu CSIRT.CZ* [online]. Praha: CZ.NIC, 2022 [cit. 2022-05-07]. Dostupné z: https://csirt.cz/cs/o-nas/

[4] CZ.NIC, z. s. p. o.: *Ipv6 internet pomocí automatických tunelovacích technologií 6to4 a teredo* [online]. Praha: CZ.NIC, z. s. p. o., 2022 [cit. 2022-05-07]. Dostupné z: https://www.nic.cz/ipv6/

[5] GitHub: *LiME*. GitHub.com [online]. GitHub, 2021, 21. 5. 2021 [cit. 2022-05-07]. Dostupné z: https://github.com/504ensicsLabs/LiME

[6] GŘIVNA, Tomáš, Miroslav SCHEINOST a Ivana ZOUBKOVÁ. *Kriminologie.* 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. ISBN 978-80-7598-554-5.

[7] HANZL, Lukáš. *Metodika vyšetřování počítačové kriminality*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2008, 82 s. Dostupné také z: http://hdl.handle.net/10563/7467. Tomas Bata University in Zlín. Faculty of Applied Informatics, Ústav elektrotechniky a měření. Vedoucí práce Štefka, Vladislav.

[8] JANKOVÁ, Martina. *Možnosti systémového prostředí ICT v kyberprostoru podniku*. GRANT journal. 2015, 1, stránky 51-53. [Online]. Dostupné z: https://www.grantjournal.com/issue/0401/PDF/0401jankova.pdf, ISSN 1805-0638.

[9] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 1 online zdroj. ISBN 9788074543128. Dostupné také z: http://hdl.handle.net/10563/25821.

[10] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[11] KEŇO, Lukáš. *Vyšetřování počítačové kriminality*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2016, 67 s. (97 712 znaků). Dostupné také z: http://hdl.handle.net/10563/38964. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství. Vedoucí práce Štefka, Vladislav.

[12] KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[13] KOLOUCH, Jan a Pavel BAŠTA. *Cybersecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

[14] KONRÁD, Zdeněk, Viktor PORADA, Jiří STRAUS a Jaroslav SUCHÁNEK. *Kriminalistika: kriminalistická taktika a metodiky vyšetřování.* 2. Rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2021. ISBN 978-80-7380-859-4.

[15] *Kriminalistika: časopis pro kriminalistickou teorii a praxi*. Praha: Magnet-Press, 1993-. ISSN 1210-9150. Dostupné také z: https://www.mvcr.cz/clanek/kriminalistika.aspx

[16] Národní úřad pro kybernetickou a informační bezpečnost: *Kybernetická bezpečnost*. NCKB [online]. Brno: NÚKIB, 2022, [cit. 2022-05-07]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/

[17] Národní úřad pro kybernetickou a informační bezpečnost: *Návody. Návod na zajištění dat pro forenzní analýzu - Linux* [online]. Brno: NÚKIB, 2019, 21. 8. 2019 [cit. 2022-05-07]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/navody/

[18] Národní úřad pro kybernetickou a informační bezpečnost: *Návody. Návod na zajištění dat pro forenzní analýzu - Windows* [online]. Brno: NÚKIB, 2019, 21. 8. 2019 [cit. 2022-05-07]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/navody/

[19] Národní úřad pro kybernetickou a informační bezpečnost: *NBÚ vybral provozovatele národního CERT (CSIRT.CZ), je jím CZ.NIC* [online]. Brno: NÚKIB, 2015, [cit. 2022-05-07]. Dostupné z: https://www.nbu.cz/cs/aktualne/820-621-nbu-vybral-provozovatele-narodniho-cert-csirtcz-je-jim-cznic/

[20] PERNICA, Luboš. *Kybernetická kriminalita*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2018, 75 s. Dostupné také z: http://hdl.handle.net/10563/42928. Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení, Ústav krizového řízení. Vedoucí práce Dvořák, Jiří.

[21] Policejní akademie ČR: *Bezpečnostní teorie a praxe* [online]. Praha: Policejní akademie ČR, ISSN 1801-8211. Dostupné z: https://veda.polac.cz/

[22] Policie ČR: *Jednotlivé druhy kyberkriminality* [online]. Praha: Policie ČR, 2017 [cit. 2022-05-07]. Dostupné z: https://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx

[23] Policie ČR: *Ukončení provozu HOTLINE*. Praha: Policie ČR, 2018 [cit. 2022-05-07]. Dostupné z: https://www.policie.cz/clanek/ukonceni-provozu-hotline.aspx

[24] Policie ČR: *Víte co je KYBERŠIKANA?* [online]. Policie ČR, 2009 [cit. 2022-05-07]. Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

[25] PORADA, Viktor a Jiří STRAUS. *Kriminalistika: (výzkum, pokroky, perspektivy)*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-80-7380-477-0.

[26] PORADA, Viktor a Karel RAIS. *Právní, kriminalistické a kybernetické aspekty kybernetické kriminality a bezpečnosti: pocta Vladimíru Smejkalovi*. Brno: Akademické nakladatelství CERM, 2021. ISBN 978-80-7623-065-1.

[27] PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty.* 2. Aktualizované a rozšířené vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.

[28] POŽÁR, Josef a Václav HNÍK, *Specifické problémy boje s kybernetickou kriminalitou* [online]. Praha: Policejní akademie ČR. Dostupné z: https://slideplayer.cz/slide/11176990/

[29] SEKANINA, Michal. *Užití vybraných metod umělé inteligence pro robotické bezpilotní systémy.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2018, 59 s. (61047). Dostupné také z: http://hdl.handle.net/10563/42932. Univerzita Tomáše Bati ve Zlíně. Fakulta logistiky a krizového řízení, Ústav krizového řízení. Vedoucí práce Dvořák, Jiří.

[30] SMEJKAL, Vladimír. *Současné možnosti boje proti počítačové kriminalitě.* Data security management. Roč. XV, 2011, č. 4. ISSN 1211-8737.

[31] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. Rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-720-7.

[32] Stoponline.cz: *Ohlaste nezákonný obsah / Report illegal content* [online]. Praha: CZ.NIC, z. s. p. o., 2022 [cit. 2022-05-07]. Dostupné z: https://www.stoponline.cz/cs/

[33] STRAUS, Jiří. *Kriminalistická metodika*. 2., rozš. vyd. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2008. ISBN 978-80-7380-124-3.

[34] The British Journal of Criminology: An International Review of Crime and Society: *Cybercrime is (often) boring: Infrastructure and alienation in a deviant subculture* [online]. 2021. Oxford, UK: Oxford University Press, 2021 [cit. 2022-05-07]. ISSN 0007-0955. Dostupné z: https://academic.oup.com/bjc/article/61/5/1407/6226588?searchresult=1t

[35] VAŠEK, Martin. *Využití forenzních metod k odhalování počítačové kriminality*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 91 s. Dostupné také z: http://hdl.handle.net/10563/25390. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav elektroniky a měření. Vedoucí práce Hromada, Martin.

[36] VLACH, Jiří, Kateřina KUDRLOVÁ a Viktorie PALOUŠOVÁ. *Kyberkriminalita v kriminologické perspektivě*. Praha: Institut pro kriminologii a sociální prevenci, 2020. Studie (Institut pro kriminologii a sociální prevenci). ISBN 978-80-7338-189-9.

[37] VYSKOČIL, Ladislav. *Zajišťování a analýza digitálních důkazů*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 105 s. Dostupné také z: http://hdl.handle.net/10563/24882. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav informatiky a umělé inteligence. Vedoucí práce Malaník, David.

[38] ZAVRŠNIK, Aleš. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017. Právní monografie (Wolters Kluwer ČR). ISBN 978-80-7552-758-5.Vydavatelství a nakladatelství Aleš Čeněk, 2013. ISBN 978-80-7380-477-0.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
Dos, ddos	Denial of Service. Distributed Denial of Service
GPS	Global Positioning System
HASH	Matematická funkce (resp. algoritmus) pro převod vstupních dat do (relativně) malého čísla. Jeho hlavní vlastností je, že malá změna na vstupu vede k velké změně na výstupu, tj. k vytvoření zásadně odlišného otisku (čísla).
HTML	Hyper Text Markup Language. Jde o název značkovacího jazyka používaného pro tvorbu webových stránek.
HTTP	Hypertext Transfer Protocol. Internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML.
IANA	Internet Assigned Numbers Authority je organizace, která dohlíží celosvětově na přidělování IP adres
ICANN	Internet Corporation for Assigned Names and Numbers. Jedná se o neziskovou organizaci, aby dohlížela na množství věcí souvisejících s internetem, které dříve spravovaly jiné organizace, například IANA.
ICT	Informační a komunikační technologie
IS	Informační systém / systémy
ISP	Internet Service Provider. Specificky k českému právu je využíván pojem poskytovatel služeb informační společnosti.
IT	Informační technologie
LiME	Linux Memory Extractor. Linuxový modul používaný k extrakci paměti RAM
MD5	Message-Digest algorithm, je popsán v internetovém standardu RFC 1321 a vytváří otisk o velikosti 128 bitů.
NAT	Network Adress Translation. Překlad síťových adres.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost

OS	Operační systém
OČTŘ	Orgán činný v trestním řízení
P2P	Peer-to-peer
PC	Personal Computer. Osobní počítač.
SHA-1	Secure Hash Algorithm, vytváří 160bitový obraz zprávy s maximální délkou $2^{64} - 1$ bitů.
SHA-2	Secure Hash Algorithm, algoritmy společně označované jako SHA-2, mezi které patří SHA-224, SHA-256, SHA-384 a SHA-512, pojmenovány jsou podle své délky v bitech.
TŘ	Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů
TZ	Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
URL	Uniform Resource Locator. Jednotná adresa zdroje.
Wi-Fi	Bezdrátová technologie pro šíření dat („vzduchem“), vhodná pro tvorbu sítových infrastruktur tam, kde je výstavba klasické kabelové sítě nemožná, obtížná nebo nerentabilní. Pro přenos dat postačí vhodně umístěné navazující přístupové body, lemující cestu od vysílače k příjemci.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: NÁVRH METODIKY K ZAJIŠTĚNÍ DIGITÁLNÍCH DŮKAZŮ

Níže uvádím příklady k zajištění digitálních důkazů, a to především zajištění obsahů fyzických pamětí (RAM) a vytvoření bitových kopií disků.

PŘÍKLAD ZAJIŠTĚNÍ DAT S VYUŽITÍM OS WINDOWS (ZE „ŽIVÉHO" ZAŘÍZENÍ)[54]

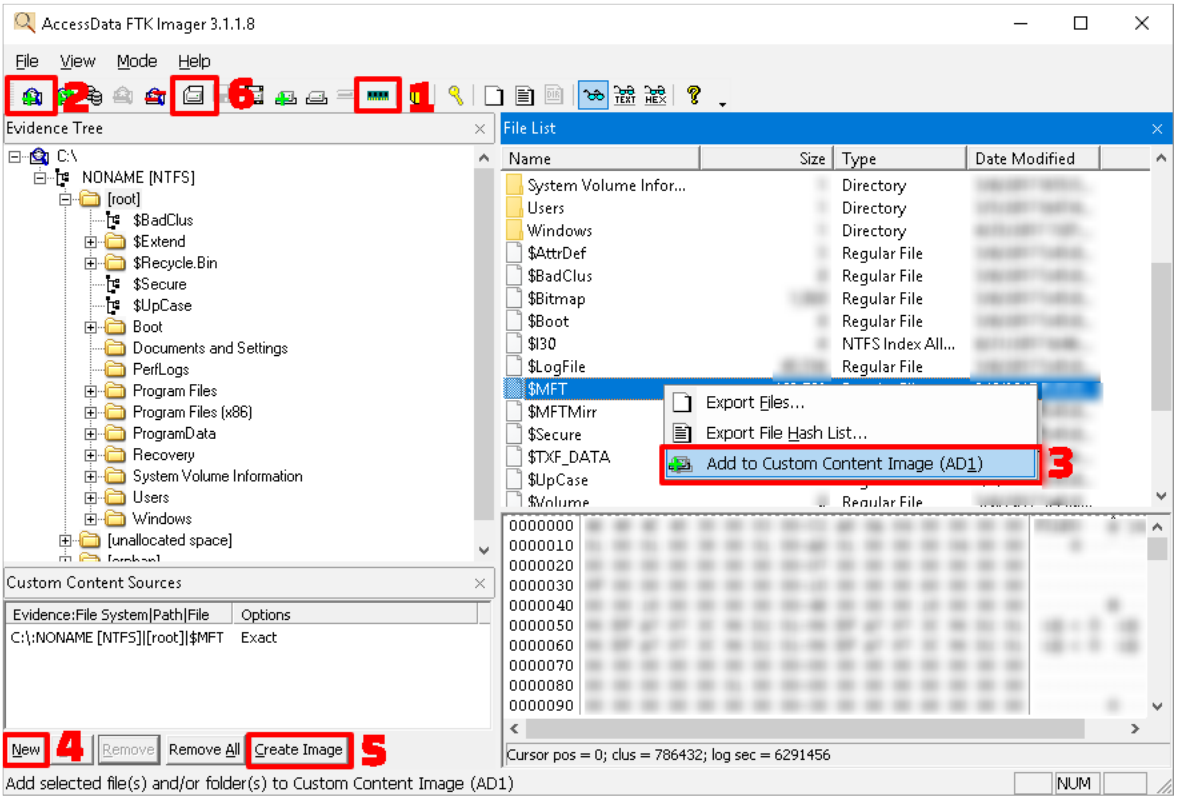
Vždy použijte externí uložiště pro spouštění nástrojů, pro akvizici dat i pro ukládání získaných souborů. Tímto se omezí zápisy na interní uložiště a přepsání informací v nealokovaných blocích. Důležité je použití vhodného souborového systému pro úložiště, např. FAT32 nám neumožní uložení souboru většího než 4 GB.

Společně se získanými daty je nutné předat i tyto informace:

- seznam dokumentovaných uživatelů systému a jejich oprávnění;
- čas zajištění hash a všech souborů;
- nástroje použité k akvizici;
- identifikátory externího uložiště.

Níže uvádím ukázku popsaného postupu s využitím softwaru FTK IMAGER. Software FTK Imager je možné spustit pouze s právy administrátora.

[54] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST: *Návody. Návod na zajištění dat pro forenzní analýzu - Windows* [online]. Brno: NÚKIB, 2019, 21. 8. 2019 [cit. 2022-05-07]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/navody/



Obrázek 14: Postup v programu FTK IMAGER[55]

1) Klikněte na ikonu "Capture Memory", vyberte "Destination path", zaškrtněte "Include pagefile", klikněte na "Capture Memory"
2) Klikněte na ikonu "Add Evidence Item", vyberte "Logical Drive", "Next", vyberte systémový disk, klikněte "Finish"
3) Vyberte následující položky do "Custom Image" (klikněte pravým tlačítkem na danou položku, vyberte "Add to Custom Image (AD1)")
    - [root]\pagefile.sys
    - [root]\hiberfil.sys
    - [root]\$MFT
    - [root]\$LogFile
    - [root]\$Extend\$UsnJrnl
    - [root]\$Recycle.Bin

[55] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST: *Návody. Návod na zajištění dat pro forenzní analýzu - Windows* [online]. Brno: NÚKIB, 2019, 21. 8. 2019 [cit. 2022-05-07]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/navody/

- [root]\Windows\System32\config\SAM
- [root]\Windows\System32\config\SYSTEM
- [root]\Windows\System32\config\SOFTWARE
- [root]\Windows\System32\config\DEFAULT
- [root]\Windows\Prefetch
- [root]\Windows\inf\setupapi.dev.log
- [root]\Windows\LogFiles
- [root]\Windows\Appcompat\Programs
- [root]\Windows\Tasks
- [root]\ProgramData\Microsoft\Search\Data\
- Applications\Windows\Windows.edb

4) Pro následující položky klikněte na "New", vyberte nově přidanou položku, doplňte text a klikněte "Edit", zaškrtněte "Match all occurences" a "Include Subdir ectories".
    - NTUSER.DAT
    - UsrClass.dat
    - AppData
    - *.lnk
    - *.evtx
5) Klikněte na "Create Image", "Add" pro výběr cílového umístění, zaškrtněte "Verify image after they are created", klikněte na "Start“.
   Oba vytvořené soubory (obraz paměti RAM a přehledový soubor) předejte k analýze.
   Zasažený systém můžete nyní odpojit od sítě.
   Pokračujte vytvořením kopie celého interního úložiště.
6) Klikněte na ikonu "Create Disk Image", vyberte “Physical Drive”, "Next", vyberte jednotku interního úložiště, "Finish"
    - Klikněte na "Add", vyberte formát "Raw (dd)", "Next", "Next", vyberte cílové umístění, "Finish", zaškrtněte "Verify images after they are created", klikněte na "Start".
    - Opakujte pro všechny jednotky interního úložiště.

Při použití šifrování předejte také klíče pro obnovení. Vytvořený obraz interního úložiště předejte k analýze. S přemazáním systému vyčkejte na potvrzení analytického týmu.

Pokud je počítač vypnutý, je nezbytné držet se již uváděného pravidla – v žádném případě nezapínat. Pokud je to v dané situaci možné, interní úložiště vyjmeme a vytvoříme jeho bitovou kopii. K tomu využíváme např. jednoúčelové zařízení (tzv. disk duplicator).

PŘÍKLAD ZAJIŠTĚNÍ DAT S VYUŽITÍM OS LINUX (ZE „ŽIVÉHO" ZAŘÍZENÍ)[56]

Základní pravidla pro použití nástrojů se od OS Windows neliší. Pracujeme s nástroji na externích discích a veškerá data ukládáme pouze na externí disky. Neliší se ani předání důležitých informací (seznam dokumentovaných uživatelů systému a jejich oprávnění, čas zajištění hash a všech souborů, nástroje použité k akvizici a identifikátory externího uložiště).

Příkazy použité v tomto linuxovém návodu jsou psány kurzívou.

1) Paměť RAM – Obraz paměti je možné vytvořit pomocí nástroje LiME (Linux Memory Extractor)[57].
    a) Stažení, kompilace a zavedení do jádra provedeme příkazem:
        - *git clone https://github.com/504ensicsLabs/LiME.git*
        - *cd LiME*
        - *make*
    b) Pro zápis obrazu paměti RAM do souboru použijeme příkaz:
        - *sudo insmod lime-*.ko "path=/out/memory.img format=lime"*
    c) Příkaz pro přenos po síti:
        - *sudo insmod lime-*.ko "path=tcp:4444 format=lime"*
    d) Na jiném počítači je možné tento obraz uložit do souboru příkazem:
        - *nc <IP> 4444 > memory_RAM.img*, kde *<IP>* je IP adresa počítače, ze kterého je zajišťován obraz
        - pozn.: Netcat (nc) posílá data nešifrovaným kanálem!
    e) Odebrání modulu z jádra se provede příkazem:

---

[56] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST: *Návody. Návod na zajištění dat pro forenzní analýzu - Linux* [online]. Brno: NÚKIB, 2019, 21. 8. 2019 [cit. 2022-05-07]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/navody/

[57] GITHUB: *LiME*. GitHub.com [online]. GitHub, 2021, 21. 5. 2021 [cit. 2022-05-07]. Dostupné z: https://github.com/504ensicsLabs/LiME

- *sudo rmmod lime*

2) Pro vytvoření obrazu interní paměťové jednotky, nejčastěji pevného disku, počítače je potřeba nejprve zjistit, které zařízení *„/dev“* odpovídá kterému disku. To je možné provést příkazem:
   - *df –Th*
   - nebo *fdisk –l*

   Obvykle se jedná o první disk, např. *„/dev/sda“*.

   Dalším krokem je vytvoření obrazu disku. K tomu je nejčastěji používán program „*dd“*. Tento program je již základní součástí instalace většiny distribucí Linuxu. Pro spuštění programu je nutný administrátorský přístup a příkaz vypadá následovně:
   - *sudo dd if=/dev/sda of=/out/disk.img status=progress conv=sync,noerror*
   - pozn.: volba *„status=progress“* v příkazu slouží k zobrazení aktuálního postupu

   Posledním krokem je vytvoření hashe získané bitové kopie. To se provede příkazem:
   - *sha512sum /out/disk.img > /out/disk.sha512*

   Pokud bylo použito šifrování, je nutné předat i klíče pro obnovu dat.

PŘÍKLAD ZAJIŠTĚNÍ DAT Z VYPNUTÉHO POČÍTAČE[58]

Pro získání dat z vypnutého počítače je možné přeskočit bod, kdy se získávají data z paměti RAM, jelikož se jedná o dočasnou paměť, která se po vypnutí sama vymaže. Proto z prostředí OS Microsoft Windows stačí použít nástroj FTK Imager nebo obdobný, a z prostředí OS Linux využít program „dd“ nebo jeho obdoby (např. „dc3dd“ nebo „cfldd“).

[58] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST*: Návody. Návod na zajištění dat pro forenzní analýzu - Linux* [online]. Brno: NÚKIB, 2019, 21. 8. 2019 [cit. 2022-05-07]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/navody/

PŘÍKLAD ZAJIŠTĚNÍ DAT Z VIRTUÁLNÍHO STROJE[59]

Z prostředí VMWARE se paměť RAM získá z běžícího virtuálního stroje ze souboru VMEM, který je obrazem paměti RAM. Tento soubor postačí zkopírovat.

VMwre pro interní uložiště používá obvykle formát VMDK a pro většinu analýz postačí tento soubor poskytnout znalci. Jen si musíme uvědomit, že pokud je interní disk rozdělen, je nutné dodat všechny soubory, ze kterých se interní uložiště skládá.

PŘÍKLAD ZAJIŠTĚNÍ DAT Z MOBILNÍHO ZAŘÍZENÍ[60]

Mezi mobilní zařízení se může řadit např. chytrý telefon (tzv. smartphone) nebo tablet různých značek. Většinou se jedná o zařízení s OS Android, jehož vývoj vede firma Google, či OS IOS od společnosti Apple. Hardware těchto zařízení je velmi různorodý a není jednoduché vytvořit bitovou kopii uložiště dat bez přímého připojení k tomuto zařízení. Proto jsou níže uvedeny jen doporučení pro bezpečné zajištění zařízení pro transport k znalci v oboru ICT, který následně provede forenzní analýzu.

Pro bezpečný transport musí být provedeny tyto základní úkony:

- sepsat, jaké předcházející akce vedly k tomuto incidentu;
- uvést zařízení do režimu "letadlo" a zkontrolovat, že je Wi-Fi vypnutá;
- zkontrolovat, zda je baterie zařízení dobita alespoň na 50% (v opačném případě dobijte zařízení jedině připojením do zásuvky, nikoli přes USB připojené k PC, či jinému zařízení!);
- přelepte neprůsvitnou páskou všechny kamery a mikrofony;
- pokud je k dispozici, vložte zařízení navíc do stíněného nepropustného pouzdra.

---

[59] Taktéž.

[60] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST: *Návody. Návod na zajištění dat pro forenzní analýzu - Linux* [online]. Brno: NÚKIB, 2019, 21. 8. 2019 [cit. 2022-05-07]. Dostupné z: https://nukib.cz/cs/infoservis/dokumenty-a-publikace/navody/

PŘÍLOHA P II: ROZHODOVACÍ POMŮCKA PRO VYŠETŘOVATELE KYBERNETICKÉHO TR. ČINU