POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Katedra kriminologie

Mládež a kyberkriminalita

Diplomová práce

Youth and Cybercrime

Master thesis

VEDOUCÍ PRÁCE

PhDr. Alena Marešová, Ph.D.

AUTOR PRÁCE

Bc. Nikola Šafránová

PRAHA

2022

Čestné prohlášení

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

V Jílovém, dne

Bc. Nikola Šafránová

Poděkování

Na tomto místě bych ráda poděkovala PhDr. Alena Marešová, Ph.D. za cenné připomínky, rady a informace, které mi pomohli v hledání informací pro tuto práci. Také jí děkuji za její čas a ochotu.

ANOTACE

Diplomová práce se zabývá kyberkriminalitou mládeže. Kyberkriminalita obecně je stále aktuálním problémem. V teoretické části jsou charakterizovány základní pojmy, které se vztahují k této problematice. Dále jsou zde definovány jednotlivé druhy kyberkriminality, fenomenologie, etiologie a kontrola kriminality mládeže a kyberkriminality. Praktická část obsahuje dotazníkové šetření, jeho popis, cíle, výzkumné předpoklady a jeho závěrečné vyhodnocení. Tématem dotazníku je Mládež a kyberkriminalita a snaží se zjistit rozsah páchání kyberkriminality mládeží. Ten podle výsledků dotazníkového šetření není příliš velký a je tedy možné, že kyberkriminalita se ve větší míře začíná páchat až ve vyšším věku, než je mládež.

KLÍČOVÁ SLOVA

mládež, kyberprostor, sociální sítě, kyberkriminalita, kontrola kriminality, prevence kyberkriminality mládeže

ANNOTATION

The master thesis deals with juvenile cybercrime. Cybercrime in general is still a current problem. The theoretical part characterizes the basic concepts that relate to this issue. Furthermore, individual types of cybercrime, phenomenology, etiology and control of juvenile delinquency and cybercrime are defined here. The practical part contains a questionnaire survey, its description, objectives, research assumptions and its final evaluation. The topic of the questionnaire is Youth and Cybercrime and seeks to determine the extent of cybercrime. According to the results of the questionnaire survey, the extent of cybercrime is not very large and it is therefore possible that cybercrime does not begin to be committed to a greater extent than at the age of young people.

KEYWORDS

youth, cyberspace, social networks, cybercrime, crime control, youth cybercrime prevention

Obsah

Úvod

Žijeme v digitální době. Komunikační a informační technologie se neustále rozvíjí a tím se rozvíjí i hrozby ve virtuální realitě neboli kyberprostoru. Dnešní doba je spojena s rostoucím využíváním internetu, a především pak sociálních sítích. Zejména mladí lidé tyto možnosti stále více využívají, a to k práci, kvůli škole, k zábavě nebo na zahnání nudy. Většina lidí si už bez těchto technologií nedokáže život ani představit. Kyberprostor má ale i svou stinnou stránku a tou je páchání kyberkriminality. Ta je taky tématem této práce. Konkrétněji pojednává o kyberkriminalitě mládeže.

Práce se primárně zaměřuje na populaci lidí ve věku 12-24 let tedy na mládež. Kyberkriminalita mládeže může být často opomíjená s důvody, že děti zase tolik ještě komunikačním a informačním technologiím nerozumějí nebo že se obecně předpokládá, že kyberkriminalita se začíná páchat až v pozdějším věku. Tato obecná domněnka je také jedním z cílů této práce. Autorka se ji pokusí dokázat nebo naopak vyvrátit. Druhým hlavním cílem práce je zjistit rozsah kyberkriminality mládeže.

Práce je rozdělena na dvě části – teoretickou a praktickou. Cílem teoretické části je charakterizovat základní pojmy, a to mládež, kyberprostor, sociální sítě a kyberkriminalita. Dále seznámit se s fenomenologií a etiologií kriminality mládeže a kyberkriminality. Následují jednotlivé druhy projevů kyberkriminality a vývoj kriminality mládeže a kyberkriminality v České republice. V závěru teoretické části je charakterizována kontrola kriminality, která postupně přechází k prevenci kyberkriminality mládeže. K tomuto autorka využila obsahovou analýzu odborné literatury a internetových zdrojů.

V praktické části, která má jako hlavní cíl zjistit rozsah kyberkriminality mládeže, bylo využito kvantitativní metody formou dotazníkového šetření. V úvodu této části práce jsou stanoveny i čtyři výzkumné předpoklady, které byly vytyčeny předem. V závěru jsou jednotlivě vyhodnoceny. Podle odpovědí v dotazníku se dozvíme, zda byly správné, odlišné nebo zcela nesprávné. Sám dotazník se skládá z 31 otázek a respondentům byl předkládán elektronicky. Závěry vzešly z 219 vyplněných dotazníků.

Teoretická část

1. Charakteristika základních pojmů

Pro porozumění problematiky je nejprve nutné si definovat základní pojmy. Těmi pro tuto práci jsou mládež, kyberprostor, sociální sítě a kybernetická kriminalita.

1.1 Mládež

Kriminologie pro pojem mládeže nejčastěji používá definici ze sociologie. Jedná se o *„osoby, které z pohledu společnosti nelze označit jako osoby sociálně zralé, samostatné, zpravidla ve věkovém rozmezí 12–24 let.“* Je nutné podotknout, že tam kde se dokládají statistická data o kriminalitě mládeže se užívají trestněprávní vymezení a členění. Do pojmu mládež tedy lze zahrnout děti, mladistvé, osoby blízké věku mladistvých a mladé dospělé pachatele.[1]

Dítětem je osoba do věku 15 let. Z pohledu českého trestního práva není dítě trestně odpovědné. Protiprávní čin spáchaný dítětem se nazývá čin jinak trestný. Mladistvým je osoba ve věkovém rozmezí 15-18 let. Podle zákona č. 218/2003 Sb., o soudnictví ve věcech mládeže mají relativní trestní odpovědnost. Jimi spáchaný protiprávní čin se nazývá provinění. Do skupiny osob blízkých věku mladistvých spadají osoby ve věku 19-20 let, výjimečně i 21 let. V českém trestním právu tato skupina není přesně definována. Mladí dospělí pachatelé se věkově kryjí s předchozí skupinou. Dle sociologie je to věková skupina v rozmezí 18-24 let.[2]

Každý vědní obor (vývojová psychologie, pedagogika, psychiatrie, penologie atd.) na mládež nahlíží trochu jinak. V této práci se ale autorka bude držet hlavně vymezení podle sociologie a trestního práva.

---

[1] MAREŠOVÁ, Alena. *Kriminalita mládeže v podmínkách současné české společnosti: pro studenty magisterského studijního programu*. Praha: Policejní akademie České republiky v Praze, 2018. 15 s. ISBN 978-80-7251-483-0

[2] MAREŠOVÁ, Alena. *Kriminalita mládeže v podmínkách současné české společnosti: pro studenty magisterského studijního programu*. Praha: Policejní akademie České republiky v Praze, 2018. 16, 17, 30 s. ISBN 978-80-7251-483-0

1.2 Kyberprostor

Obecně je kyberprostor virtuální realita interaktivního počítačového světa. Lze tedy říct, že je to veškerý internet jako takový. Nemá konec ani začátek. Hlavní funkcí kyberprostoru je rychlé a snadné komunikování, posílání si souborů navzájem nebo nakupování a placení za ně. Nejdůležitější vlastností kyberprostoru je anonymita. Ta samotná hraje ve prospěch kybernetické kriminalitě.[3]

Kyberprostor je také možné definovat jako: *„prostor kybernetických aktivit či jako prostor vytvořený informačními a komunikačními technologiemi, který vytváří virtuální svět (či prostor) jako paralelu k prostoru reálnému.“* Je však zcela závislý na materiální podstatě, nacházející se ve světě reálném.[4]

V zákoně č. 181/2014 Sb., o kybernetické bezpečnosti je pojem kyberprostor vymezen takto: *„digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“*[5]

1.3 Sociální sítě

Vzhledem k tématu práce je nutné do základních pojmů zahrnout i sociální sítě. Většina dnešní mládeže tráví více času ve virtuálním světě na sociálních sítích než ve světě reálném.

Sociální sítě můžeme vymezit jako internetovou službu, která na základě registrace umožní vytvořit profil uživatele, pod kterým lze tuto službu využívat především ke komunikaci, sdílení informací, fotografií, videí atd. s dalšími registrovanými uživateli.[6] Sociální sítě jsou nejčastějším prostředím, ve kterém se kybernetická kriminalita odehrává.

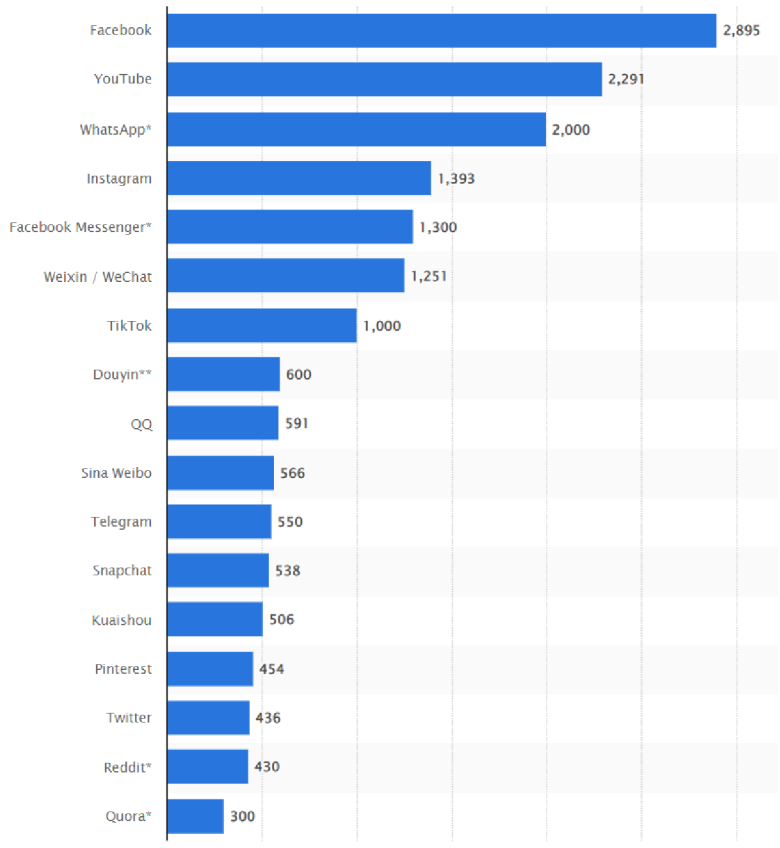
---

[3] Kyberprostor [online]. [cit. 25.12.2021] Dostupné z: https://www.sprava-site.eu/kyberprostor/
[4] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. 43 s. ISBN 978-80-88168-15-7
[5] Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), § 2
[6] Sociální sítě [online]. [cit. 25.12.2021]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/

Sociální sítě mohou mít sociální účel, obchodní účel nebo obojí prostřednictvím webů jako Facebook, Twitter, LinkedIn a Instagram. Sociální sítě jsou také významnou základnou pro obchodníky, kteří chtějí zaujmout zákazníky (např. zvýšení povědomí o značce nebo podpora loajality ke značce). Sociální sítě jsou důležité, protože umožňují lidem rozvíjet vztahy s ostatními, se kterými by se jinak nemohli spojit. Pomáhá také zvýšit produktivitu podnikání při použití pro účely PR, marketingu a reklamy.[7]

Sociální sítě mají také své nevýhody. Těmi jsou např. rychlé šíření dezinformací nebo vysoké náklady na používání a udržování profilů (platí pro firmy, ne pro běžného uživatele).[8]

Graf 1: Nejpoužívanější soc. sítě za říjen 2021 ve světě (v milionech)



Zdroj: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

[7] What is social networks [online]. [cit. 14.2.2022]. Dostupné z: https://www.investopedia.com/terms/s/social-networking.asp
[8] Tamtéž

1.4 Kybernetická kriminalita

Pro tento pojem dodnes neexistuje jednotná definice.

Nejobecněji lze kybernetickou kriminalitu (dále jen „kyberkriminalita“) definovat jako: *„jednání namířené proti počítači, případně počítačové síti, nebo jako jednání, při němž je počítač použit jako nástroj pro spáchání trestného činu.“* Aby bylo možné uplatnit definici kyberkriminality, je nutné, aby se taková činnost odehrávala v kyberprostoru.[9]

U Policie České republiky (dále jen „PČR“) je tento pojen definován jako: *„trestná činnost, která je páchána v prostředí informačních a komunikačních technologií včetně počítačových sítí. Samotná oblast informačních a komunikačních technologií je buď předmětem útoku, nebo je páchána trestná činnost za výrazného využití informačních a komunikačních technologií jakožto významného prostředku k jejímu páchání.“*[10]

Zákon č. 40/2009 Sb. v souvislosti s kyberkriminalitou uvádí tyto trestné činy: § 230 Neoprávněný přístup k počítačovému systému a nosiči informací, § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat, § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

Kyberkriminalitu mohou provádět jednotlivci nebo skupiny s relativně malými technickými dovednostmi nebo vysoce organizované globální zločinecké skupiny, které mohou zahrnovat zkušené vývojáře a další osoby s příslušnými odbornými znalostmi. Aby se ještě více snížily šance na odhalení a stíhání, kyberzločinci se často rozhodnou působit v zemích se slabými nebo neexistujícími zákony o počítačové kriminalitě.[11]

---

[9] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. 34 s. ISBN 978-80-88168-15-7

[10] Kybernetická kriminalita [online]. [cit. 25.12.2021]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[11] What is cybercrime [online]. [cit. 14.2.2022]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/cybercrime

2. Fenomenologie kriminality mládeže

Prvním typickým rysem kriminality mládeže je její vysoká míra latence. Toto tvrzení platí zejména u méně závažných forem kriminality. Společnost více toleruje pachatele méně závažných forem kriminality z řad mládeže, protože si myslí, že je to normální, vývojově podmíněný, jev.[12]

Dalším rysem kriminality mládeže je, že se na ní podílejí výrazně více chlapci než dívky. Potvrzují to zahraniční i české výzkumy. Dle statistických údajů PČR převládají méně závažné majetkové trestné činy (popřípadě činy jinak trestné), hlavně krádeže. Velmi závažné formy násilné kriminality jsou tedy výjimečné. Čím dál častěji je upozorňováno na zapojení mládeže do kyberkriminality hlavně v souvislosti se sextingem a kyberšikanou.[13]

Mládež trestnou činnost páchá většinou ve skupinách nebo formou spolupachatelství, a to zpravidla s vrstevníky. Toto tvrzení platí zpravidla pro chlapce.[14]

Typickým rysem je také nedostatečná plánovitost přípravy trestného činu. Své skutky páchají impulzivně. Nasvědčuje o tom náhodnost místa trestného činu, použití nevhodných nástrojů nebo potřeb pro získání či ukrytí lupu, nevhodný čas pro provedení skutku anebo špatné „zametení“ svých stop. Dalším rysem kriminality mládeže je neadekvátnost jejich jednání a neschopnost odložit uspokojení potřeb na pozdější dobu nebo se některých potřeb vzdát. V neposlední řadě mezi zmiňované rysy patří také násilí. To se může vztahovat k osobě nebo k věci. Pachatel se neadekvátním násilím snaží stvrdit své schopnosti, prosadit se, chce zažít dobrodružství, přinutit někoho, aby jej poslouchal a také chce získat uznání od své vrstevnické skupiny.[15]

---

[12] VÁLKOVÁ, Helena, KUCHTA Josef, HULMÁKOVÁ Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. V Praze: C.H. Beck, 2019. 284 s. ISBN 978-80-7400-732-3.
[13] VÁLKOVÁ, Helena, KUCHTA Josef, HULMÁKOVÁ Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. V Praze: C.H. Beck, 2019. 285, 286 s. ISBN 978-80-7400-732-3.
[14] VÁLKOVÁ, Helena, KUCHTA Josef, HULMÁKOVÁ Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. V Praze: C.H. Beck, 2019. 288 s. ISBN 978-80-7400-732-3.
[15] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 489-491 s. ISBN 978-80-7598-554-5

Motivace mládeže k páchání trestné činnosti se nedá přímo odůvodnit. Mládež má v dnešní době velkou paletu možností, velmi málo se na ně kladou požadavky, které často nedokážou kladně vstřebat a tím pádem si svůj hněv vybíjí páchaním trestné činnosti. K jejich motivaci může také přispět vidina mnoha předmětů vysoké ceny nebo prožitků, které dnešní svět nabízí a které si peněžně nemohou dovolit. Rozhodnou se jich tedy zmocnit nelegální cestou. Delikventní mládež často také odmítá převzít odpovědnost za své chování a mají nepřetržitý sklon zasahovat do práv jiných osob. Je značně těžké je k něčemu donutit. Docílíme toho jen způsobem, když z toho něco „kápne“ i jim. Nabídka pro ně musí být jistým způsobem výhodná.[16]

3. Etiologie kriminality mládeže

Příčin kriminality mládeže je mnoho, některé ovlivňují delikventní chování více, jiné méně nebo se vzájemně ovlivňují. Hlavním faktorem pro určení příčin protiprávního jednání je zejména soubor subjektivních vlastností osobnosti, které mají na vývoj jedince značný vliv. Dalším ovlivňujícím faktorem je pak společnost, ve které se jedinec pohybuje. Vyjdeme-li z multifaktorového přístupu, je přijatelné zmínit zejména následující faktory, které se mohou podílet na vzniku nebo rozvoji nežádoucího chování u mládeže. Jedná se o tyto faktory:

a) *„individuální zvláštnosti jedince podmíněné geneticky, chorobou, duševní poruchou, osobnostními dispozicemi (např. ADHD, jiné abnormality mozku, impulzivita, nízká sebekontrola)*
b) *nepříznivé rodinné charakteristiky a zkušenosti (např. nízký socioekonomický status, kriminální infekce v rámci rodiny, duševní onemocnění v rámci rodiny, chybějící či nedostatečné citové vazby na rodiče, psychická deprivace, problematické výchovné styly)*
c) *nedostatečné či dokonce rizikové působení školního prostředí, jako významné socializační instituce (např. nepřipravenost na děti ze sociálně vyloučených skupin obyvatel či s jinými znevýhodněními, což přispívá k jejich selhávání v rámci vzdělávání, klima na škole,*

[16] Fenomenologie kriminality mládeže [online]. [cit. 22.2. 2022]. Dostupné z: https://is.ambis.cz/th/ewcdm/Kriminalita_mladeze_a_jeji_prevence_-_David_Novy.pdf

podporující šikanu, selektivní či někdy stigmatizující přístupy učitelů apod.)

d) *negativní vliv prostředí (život v sociálně vyloučené komunitě, nízký socioekonomický status, vliv vrstevnických skupin a subkultur, vliv médií a hraní počítačových her zejména v souvislosti s násilnou kriminalitou)*
e) *dostatek příležitostí*
f) *sociálně patologické jevy menší závažnosti jako např. alkoholismus, drogová závislost, záškoláctví, agresivní chování aj. (ty jsou však zpravidla chápány jako sekundární rizikové faktory, neboť jejich příčiny často odpovídají výše uvedeným příčinám kriminality mládeže)*
g) *neadekvátní užití formálních sociálních intervencí – nadužívání zejména institucionálních forem opatření či sankcí, neodpovídajících riziku dalšího kriminálního selhání*
h) *společenské a demografické změny a posuny hodnotových orientací jak celé společnosti, tak subkultury mládeže“*[17]

Mezi další příčiny kriminality mládeže můžeme zařadit špatně prožívaný volný čas a pocit nudy. Ten se mládež snaží zahnat okamžitým nápadem, který nebude vyžadovat delší snažení, nebyl rozumově příliš náročný a aby bylo součástí dobrodružství nebo soutěž.[18]

4. Fenomenologie kyberkriminality

Mezi základní charakteristiku kyberkriminality patří jednoznačně rychlost výměny dat. V jednom momentě jsou dosažitelná na tisících místech a během okamžiku můžou být naopak smazány. Dále je pro kyberprostor charakteristické, že stačí jen malé náklady pro získání velkého vlivu nebo způsobení značné škody. Pachateli stačí získat jen přístup k internetu a mít jistou uživatelskou schopnost. Dalším rysem kyberkriminality je její vysoká latence. Oběť často ani

[17] VÁLKOVÁ, Helena, KUCHTA Josef, HULMÁKOVÁ Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. V Praze: C.H. Beck, 2019. 291-293 s. ISBN 978-80-7400-732-3.
[18] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 505 s. ISBN 978-80-7598-554-5

netuší, že se stala cílem útoku. Jindy poškozený naopak nechce oznámit orgánům činným v trestním řízení napadení svých zařízení. K vysoké latenci dále také přispívá bezprostřední neviditelnost způsobených následků, a v nějakých případech i zpochybňovaná společenská škodlivost.[19]

Co se týče charakteristiky pachatele vždy záleží na druhu trestné činnosti, které se dopustil. Proto tedy neexistuje typický pachatel kyberkriminality. Podmínkou je pouze základní uživatelská znalost kyberprostoru. V tomto případě by se jednalo o pachatele amatéra. O profesionála by se jednalo, pokud by k základní uživatelské znalosti disponoval i hlubšími znalostmi o práci s moderními komunikačními zařízeními (např. DOS nebo malware).[20]

Stejně tak není typická ani oběť kyberkriminality. Také její charakteristiky souvisejí s druhem a typem trestné činnosti. Viktimnost nápadně zvyšuje její neopatrnost.[21]

5. Kriminogenní faktory kyberkriminality

Kriminogenní faktory jsou rizikoví činitelé, kteří motivují, vyvolávají, usnadňují nebo podporují páchání trestných činů. Působí v rámci společenského systému a jejich kombinací lze dospět k odhalení obecných příčin kriminality. Mohou se dělit na obecné, zvláštní a konkrétní; subjektivní nebo objektivní; a nakonec podle místa, času a doby trvání.[22]

Obecnými kriminogenními faktory jsou spáchání trestného činu za účelem zisku, nízká úroveň právního vědomí, absence morálních hodnot, deformace životních cílů a hodnot, mylné chápání porevoluční svobody a demokracie, tolerance veřejnosti.[23]

---

[19] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 390,391 s. ISBN 978-80-7598-554-5
[20] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 392 s. ISBN 978-80-7598-554-5
[21] Tamtéž
[22] VÁLKOVÁ, Helena, KUCHTA Josef, HULMÁKOVÁ Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. V Praze: C.H. Beck, 2019. 547 s. ISBN 978-80-7400-732-3.
[23] Tamtéž

Specifickými kriminogenními faktory na úseku kyberkriminality jsou:

- *„vysoká míra latence*
- *pocit převahy nad zaměstnavatelem, policií, veřejností*
- *pocit beztrestnosti a neodhalitelnosti*
- *vysoká dostupnost počítačových zařízení*
- *možnost dálkového přístupu prostřednictvím počítačových sítí*
- *možnost anonymizace uživatele nebo podvržení nepravdivých identifikačních údajů a metadat*
- *rozpor mezi teritorialitou práva a globalitou internetu*
- *složitost kyberprostoru a jeho součástí*
- *obtížně definovatelné skutkové podstaty*
- *extrémně rychlá proměnlivost kyberprostoru a jeho částí v čase*
- *kriminální subkultura sociálních sítí, která má charakter toho, co známe z „fyzického světa“ jako tzv. závadové party (sem patří velké skupiny působící v určitém kybernetickém světě, ale i skupiny střední a malé spojené určitým cílem, ideologií apod.)“*[24]

6. Úmluva o kybernetické kriminalitě

Tato úmluva je známá též jako Budapešťská úmluva. Je první mezinárodní smlouvou, která usiluje o řešení internetové a počítačové kriminality harmonizací vnitrostátních zákonů, zlepšením vyšetřovacích technik a zvýšením spolupráce mezi národy. Vypracovala jej Rada Evropy ve francouzském Štrasburku za aktivní účasti pozorovatelských států Rady Evropy Kanady, Japonska, Filipín, Jižní Afriky a Spojených států amerických. Úmluvu a její vysvětlující zprávu přijal Výbor ministrů Rady Evropy dne 8. listopadu 2001. V platnost vstoupila dne 1. července 2004. K prosinci 2020 úmluvu ratifikovalo 65 států. Dne 1. března 2006 vstoupil v platnost Dodatkový protokol k Úmluvě o

[24] VÁLKOVÁ, Helena, KUCHTA Josef, HULMÁKOVÁ Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. V Praze: C.H. Beck, 2019. 548 s. ISBN 978-80-7400-732-3.

kybernetické kriminalitě. Od států, které dodatkový protokol ratifikovaly, se požaduje, aby kriminalizovaly šíření rasistických a xenofobních materiálů prostřednictvím počítačových systémů, stejně jako hrozby a urážky motivované rasismem nebo xenofobií.[25]

Úmluva o kybernetické kriminalitě se zabývá zejména porušováním autorských práv, počítačovými podvody, dětskou pornografií, zločiny z nenávisti a porušováním bezpečnosti sítí. Obsahuje také řadu pravomocí a postupů, jako je prohledávání počítačových sítí a zákonné odposlechy. Jejím hlavním cílem, stanoveným v preambuli, je provádění společné trestní politiky zaměřené na ochranu společnosti před kyberkriminalitou, zejména přijímáním vhodných právních předpisů a podporou mezinárodní spolupráce. Cílem úmluvy je především:

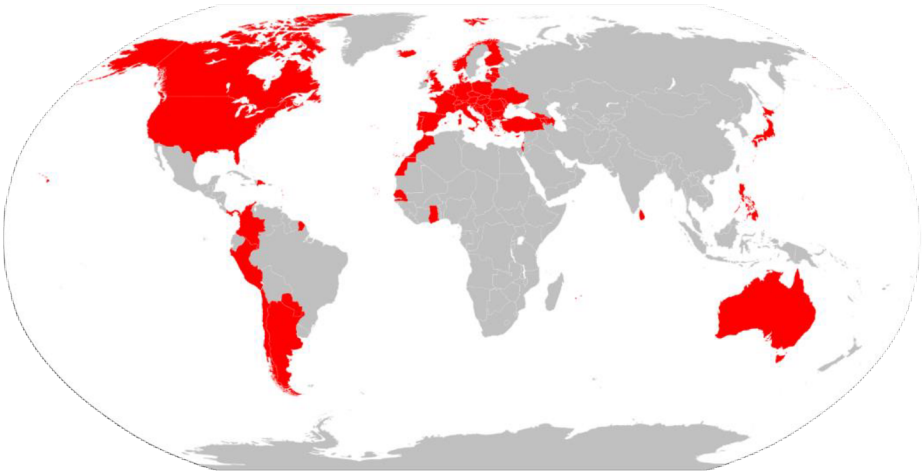
a) harmonizace vnitrostátních trestních hmotněprávních znaků trestných činů a souvisejících ustanovení v oblasti kyberkriminality
b) poskytování vnitrostátních pravomocí v oblasti trestního práva procesního nezbytné pro vyšetřování a stíhání takových trestných činů, jakož i jiných trestných činů spáchaných prostřednictvím počítačového systému nebo důkazů, které jsou v elektronické podobě
c) nastavení rychlého a efektivního režimu mezinárodní spolupráce[26]

Úmluva definuje tyto trestné činy: nezákonný přístup, nezákonné odposlechy, zásahy do dat, zásahy do systému, zneužití zařízení, počítačové padělání, počítačové podvody, trestné činy související s dětskou pornografií a trestné činy související s autorským právem a právy s ním souvisejícími. Stanoví také takové procesněprávní otázky, jako je urychlené uchování uložených údajů, urychlené uchování a částečné zpřístupnění provozních údajů, výrobní zakázka, vyhledávání a zabavení počítačových dat, sběr provozních údajů v reálném čase a zachycování obsahových údajů. [27]

---

[25] The Convention on Cybercrime [online]. [cit. 10.1.2022]. Dostupné z: https://en.wikipedia.org/wiki/Convention_on_Cybercrime
[26] The Convention on Cybercrime [online]. [cit. 10.1.2022]. Dostupné z: https://en.wikipedia.org/wiki/Convention_on_Cybercrime
[27] The Convention on Cybercrime [online]. [cit. 10.1.2022]. Dostupné z: https://en.wikipedia.org/wiki/Convention_on_Cybercrime

Obrázek 1: Země, které Úmluvu ratifikovaly



Zdroj: https://en.wikipedia.org/wiki/Convention_on_Cybercrime

7. Projevy kyberkriminality

Kybernetických útoků je mnoho. Je tedy nezbytné si je rozdělit do několika kategorií. Nejčastěji se rozlišují podle Úmluvy o kybernetické kriminalitě na:

a) *„útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů*
b) *útoky spočívající ve vytváření a šíření škodlivého (nelegálního nebo nežádoucího) obsahu*
c) *útoky spočívající v porušování práv duševního vlastnictví*
d) *tradiční kriminalita v novém kabátě (širší pojetí, než zastává Úmluva o kybernetické kriminalitě, hovořící pouze o podvodu a padělání)“*[28]

7.1 Útoky proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů

Většina kyberkriminality se zakládá na malwaru a sociálním inženýrství. Malware je škodlivý software a soudní inženýrství znamená manipulace uživatele za účelem provedení určité akce nebo získání informace. Nejčastějším postupem je průnik do systému, oklamání uživatele a následné použití získaných

[28] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 393 s. ISBN 978-80-7598-554-5

dat.[29] Pro prolomení hesel nebo průnik do počítačových systémů se nečastěji používá phishing, pharming, keylogger nebo IP spoofing.

7.1.1 Phishing a pharming

Phishing je snaha počítačových podvodníků získat citlivé osobní informace, jako jsou hesla, údaje o platebních kartách, rodná čísla nebo čísla bankovních účtů. Šíří se podvodnými e-maily nebo přesměrováním na falešné webové stránky. E-maily jsou nejčastěji od vaší banky nebo například od České pošty. Jsou gramaticky nesprávné a většinou navádějí na kliknutí na neznámou internetovou adresu. V dnešní době je ale čím dál těžší takové podvodné zprávy rozeznat, protože podvodníci si již dávají pozor na gramatiku a jsou zkušenější. Nicméně stále platí, že banka po svých klientech nikdy nebude chtít zadávat citlivé informace do e-mailu.[30]

Pharming využívá speciální počítačové programy pro napodobování určité důvěryhodné webové stránky. K tomu používá svoji webovou stránku, která se však v URL adrese drobně liší (vynecháním či přidáním jednoho písmenka). Podvodná webová stránka pak zpravidla vyzve uživatele k zadání jeho přihlašovacích údajů (nejčastěji k internetovému bankovnictví) nebo k jiné akci. Pokud tak uživatel učiní, podvodníci se poté mohou přihlásit do internetového bankovnictví pod uživatelovým jménem. Jestliže na účtu není nastaveno další zabezpečení, mohou také z účtu nepozorovaně převádět peníze.[31]

7.1.2 Malware

Dále se k zásahům do počítačů a jiných zařízeních značně využívá malware. Jak již bylo zmíněno jedná se o škodlivý software s různými funkcemi. Podmínkou je nainstalování softwaru do konečného zařízení, což učiní většinou sám uživatel obvykle nevědomky. Instalace malwaru se zpravidla spustí při otevření souboru, který je přiložený v e-mailu nebo stažením programu

---

[29]GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 393 s. ISBN 978-80-7598-554-5

[30] Co je to phishing [online]. [cit. 7.1. 2022]. Dostupné z: https://www.avast.com/cs-cz/c-phishing#gref https://www.eset.com/cz/phishing/

[31]GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 394 s. ISBN 978-80-7598-554-5

z pochybné internetové stránky anebo někdy stačí pouhé kliknutí na odkaz na internetu. Výsledkem malwaru jsou poté počítačové viry nebo počítačoví červi.[32]

Viry se v napadeném zařízení šíří samy, kdežto počítačoví červi rozesílají své kopie na další zařízení. Malware po instalaci za pomoci počítačových virů začne vyvíjet vlastní činnost spočívající v poškozování zařízení napadáním systémových souborů. Může soubory přepsat, smazat nebo znepřístupnit.[33]

Malware má dva poddruhy, a to ransomware a spyware. Ransomware je škodlivý kód, který se používá pro vydírání uživatelů. Po úspěšném infikování zařízení blokuje přístup k zařízení nebo šifruje definovaná data na disku. Po uživateli požaduje výpalné s příslibem (negarantovaným), že po zaplacení dojde ke zpřístupnění zařízení nebo odšifrování dat. Spyware je velice obtížné odhalit. Skrytě sbírá informace o uživatelově chování na internetu, historii prohlížených stránek nebo jiné osobní údaje. Často také posílá bez uživatelova vědomí tyto informace přes internet třetím stranám.[34]

7.1.3 DoS útok

Denial of service (dále jen „DoS“) neboli odepření služby je útok, jehož cílem je vyřadit počítač nebo síť a učinit je nepřístupnými pro zamýšlené uživatele. Útoky DoS obvykle fungují tak, že zahlcují cílový počítač obrovským množstvím požadavků, což má za následek odmítnutí služby dalším uživatelům.[35]

7.2 Útoky spočívající v šíření škodlivého (nelegálního nebo nebezpečného) obsahu

Pod tuto kapitolu můžeme zařadit dětskou pornografii, sexting, kyberšikanu, kyberstalking nebo kybergrooming.

---

[32] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 395 s. ISBN 978-80-7598-554-5

[33] Tamtéž

[34] Co je to ransomware a spyware [online]. [cit. 10.1. 2022]. Dostupné z: https://www.eset.com/cz/ransomware/ https://www.avast.com/cs-cz/c-spyware#gref

[35] What is DoS attack [online]. [cit. 10.1. 2022]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/ https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

7.2.1 Dětská pornografie

Jedná se o určitou formu ztvárnění (v podobě fotografie či videozáznamu) sexuálních motivů nebo aktivit, ve kterém je zobrazeno jako sexuální aktér nebo objekt dítě. Vše je vytvořeno za účelem vyvolání pohlavního vzrušení. Může se jednat například o snímky obnažených dětí zachycující polohy skutečného či předstíraného sexuálního styku nebo snímky obnažených dětí v polohách vyzývavě předvádějících pohlavní orgány. Šiřiteli dětské pornografie mohou být nejen dospělé osoby ale i sami děti.[36]

„Dětská pornografie je spojena i s dětskou prostitucí, často dobrovolnou v podobě tzv. sextingu – zasílání vlastních sexuálně laděných portrétů a videí, typicky zveřejňování tzv. selfie, a to za úplatu, výměnou za jiné fotografie i bez dalšího.“[37] Pojmem sexting tedy označujeme vědomé a dobrovolné elektronické rozesílání a sdílení zpráv, fotografií a videí se sexuálním obsahem. Fotografie a videa nejčastěji zobrazují samotného odesílatele. Sexting podporuje šíření pornografie mladistvých a dětí.[38]

V souvislosti s dětskou pornografií zákon č. 40/2009 Sb. zná tyto trestné činy: § 191 Šíření pornografie, § 192 Výroba a jiné nakládání s dětskou pornografií, § 193 Zneužití dítěte k výrobě pornografie, § 194 Účast na pornografickém představení.

7.2.2 Kyberšikana

Kyberšikana je druh šikany využívající informační a komunikační technologie (počítače, tablety, mobilní telefony, sociální sítě, emaily apod.) k ublížení druhému. Subjekty kyberšikany jsou obdobně jako u klasické šikany útočník → oběť → přihlížející (není pravidlem).[39]

---

[36] Dětská pornografie definice [online]. [cit. 10.1. 2022]. Dostupné z: https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx
[37] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 397 s. ISBN 978-80-7598-554-5
[38] Dětská pornografie definice [online]. [cit. 11.1. 2022]. Dostupné z: https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx
[39] Kyberšikana [online]. [cit. 11.1. 2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/

Útočník zpravidla vystupuje anonymně, pod falešnými přezdívkami, vytváří jednoúčelové e-mailové schránky nebo falešné profily na sociálních sítích. Díky tomuto pocitu anonymity je posílena jeho odvaha v použití agresivnější formy útoku. U klasické šikany lze předpokládat, kdy a kde přijde další útok. Kyberšikana ale tento znak vylučuje. Útok může přijít kdykoliv a kdekoliv. Možnost sdílení nebo následné přeposílání útočících příspěvků zvyšuje intenzitu vedeného útoku. Útočníkovi tedy postačí příspěvek publikovat pouze jednou, o jeho opakování a šíření se často postarají přihlížející. Jejich jednání nepřímo, ale velice důrazně zvyšuje negativní psychický dopad na oběť. Vzhledem k tomu, že dopady kyberšikany jsou spíše v rovině psychické, je velmi obtížné je na oběti rozeznat nebo poznat oběť samotnou. Posledním znakem klasické i kybernetické šikany je dlouhodobost. Útok při klasické šikaně má vždycky svůj konec, to ale neplatí v případě kyberšikany. V kyberprostoru útok nemusí skončit nikdy.[40]

Nejčastějšími projevy kyberšikany jsou:

- zasílání urážlivých a zastrašujících zpráv nebo pomluv
- pořizování zvukových záznamů, videí či fotografií, jejich upravování a následné zveřejňování s cílem poškodit vybranou osobu
- vytváření internetových stránek, které urážejí, pomlouvají nebo ponižují konkrétní osobu
- zneužívání cizího účtu – krádež identity
- provokování a napadání uživatelů v diskusních fórech
- odhalování cizích tajemství
- vydírání pomocí mobilního telefonu nebo internetu
- obtěžování a pronásledování voláním, psaním zpráv nebo prozváněním[41]

Kyberšikana může přejít v kyberstalking. Tento termín lze jednoduše popsat jako nebezpečné pronásledování za pomoci komunikačních a

[40] Kyberšikana [online]. [cit. 11.1. 2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/
[41] Kyberšikana [online]. [cit. 11.1. 2022]. Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

informačních technologií. Mezi jeho znaky patří dlouhodobost, opakovanost a stupňování kontaktů. Agresor chce u své oběti vyvolat pocit strachu o jeho soukromí, zdraví a život. Dále může chtít demonstrovat svou sílu, poškodit oběť před společností nebo chce navázat kontakt po opětovném odmítnutí. Kyberstalking lze zařadit pod trestný čin Nebezpečné pronásledování podle § 354 zákona č. 40/2009 Sb.[42]

7.2.3 Kybergrooming

Jedná se o psychickou manipulaci oběti prostřednictvím internetu s cílem jejího sexuálního využití. Kybergroomer (často se vydávající za jinou osobu, než kterou je) kontaktuje vybranou osobu s níž zpravidla i dlouhodobě udržuje a prohlubuje vztah. Snaží se izolovat oběť od svého blízkého okolí a zahrnuje ji drobnými dárky. Postupně si začne říkat o pornografické materiály, vybízet ji ke striptýzu přes webkameru a tak podobně. Poté, co se na něm oběť stane emočně závislou, žádá osobní setkání, při kterém ji obvykle dál sexuálně využije (k výrobě pornografie, sexuální zneužití, znásilnění).[43]

Kybergrooming se nejčastěji vyskytuje v různých chatovacích aplikacích, sociálních sítích nebo na internetových seznamkách. Obětí se může stát téměř kdokoliv, většinou se ale jedná o dívky ve věku 11–17 let, které často využívají informační a komunikační technologie. Tyto dívky mnohdy trpí nedostatkem sebedůvěry nebo pocitem osamění. Jsou lehce zmanipulovatelné a neznalé rizik internetové komunikace.[44]

Toto jednání by se dalo potrestat podle § 193b Navazování nedovolených kontaktů s dítětem zákona č. 40/2009 Sb.

---

[42] Kyberstalking [online]. [cit. 12.1. 2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/

[43] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 397, 398 s. ISBN 978-80-7598-554-5

[44] Kybergrooming [online]. [cit. 12.1. 2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

Tabulka 1: Počet pravomocně vyřízených pachatelů podle § 193b TZ

	2015	2016	2017	2018	2019
	3 odsouzení	6 odsouzených 1x zastaveno[218]	16 odsouzených	18 odsouzených	45 odsouzených
Počet prvopachatelů	2	2	10	11	31
Mladistvý pachatel (ve věku 15-17 let)	-	1	-	1	3
Pachatel ve věku 18-19 let	-	-	1	1	3
Pachatel ve věku 20-24 let	1	2	1	3	8
Pachatel ve věku 25-29 let	2	3[219]	5	8	12
Pachatel ve věku 30-39 let	-	1	7	3	6
Pachatel ve věku 40-49 let	-	-	2	2	10
Pachatel ve věku 50 a více let	-	-	-	-	3
Nepodmíněný trest odnětí svobody	-	1 (věznice s dozorem)	4 (3x věznice s dozorem, 1x s ostrahou)	2 (věznice s ostrahou)	1 (věznice s ostrahou)
Podmíněné odložení trestu odnětí svobody	3 (1 x s dohledem)	5	11 (4x s dohledem)	14 (4x s dohledem)	33 (9x s dohledem)
Upuštěno od potrestání a uloženo ochranné léčení (§ 47 TZ)	-	-	1	-	1
Uloženo ochranné léčení sexuologické	2	4	8	4	11

Zdroj: http://www.ok.cz/iksp/docs/463.pdf

Pachatelů bylo nejprve málo, ale postupem času se jejich počet rozrostl. Lze očekávat, že v budoucnu číslo bude dál vzrůstat. Všichni existující jsou muži převažující ve věkovém rozmezí 20-29 let. Postupně se ale přidávají i starší věkové skupiny.[45]

7.3 Útoky spočívající v porušování práv duševního vlastnictví

Na internetu nejen že lze cokoliv sdílet se širokým okruhem uživatelů, ale také nabízí prostor pro porušování práv duševního vlastnictví. Díky elektronickému obchodování lze snadno elektronickou podobu děl zneužít. K tomu dochází nejčastěji umístěním díla na veřejně přístupné úložiště, kde ho může získat pomocí stažení v podstatě každý.[46]

[45] Fenomenologie kyberkriminality [online]. [cit. 25.2.2022]. Dostupné z: http://www.ok.cz/iksp/docs/463.pdf

[46] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 400 s. ISBN 978-80-7598-554-5

Nejčastějšími útoky jsou obcházení ochrany proti kopírování (například u počítačových her), zpřístupňování (nejčastěji hudby a filmů), úprava (zvláště operačních programů a specializovaných softwarů v hodnotě desítek tisíc korun) autorských děl. Motivací takto jednajících lidí je zisk, ukázka jejich schopností a posilování myšlenky internetu jako prostoru svobodného sdílení idejí všech.[47]

7.4 Tradiční kyberkriminalita v novém kabátě

Nejčastější formou je podvod ve spojení s internetovým obchodováním. Nejvíce se tak děje při platbě předem. Při tomto záměru jsou zakládány krátkodobě i celé weby, které nabízejí zboží s cílem prodat co nejvíce zboží, které je zdánlivě za velmi výhodnou cenu. Poté co zákazník zaplatí mu buď zboží nepřijde vůbec nebo dorazí zcela jiné, anebo dorazí ale je v horší kvalitě než té slibované nebo v menším množství.[48] Takovéto jednání lze zařadit pod trestný čin Podvod podle §209 zákona č. 40/2009 Sb.

Dalším druhem jsou různé formy zneužívání platebních debetních i kreditních karet. V prvé řadě se jedná o takzvaný carding, což znamená neoprávněné hrazení zboží a služeb umožněné platbami online bez fyzické přítomnosti samotné karty. V tomto případě postačí znát číslo karty, datum platnosti a trojčíslí za zadní straně karty. Druhou formou zneužívání platebních karet je srážení jiné než uvedené částky poskytovatelem zboží nebo služby.[49]

Termínem skimming se nazývá kopírování údajů z magnetického proužku platební karty bez vědomí pravomocného držitele karty a jejich následné nahrání na novou zfalšovanou platební kartu.[50]

Jako poslední podobu tradiční kyberkriminality v novém kabátě by si autorka dovolila uvést krádež identity. Útočník podvodným jednáním získá citlivá data oběti, aby se později za oběť mohl vydávat. Krádež identity úzce souvisí s technikami soudního inženýrství používající se pro zisk citlivých údajů o oběti.

---

[47] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 400 s. ISBN 978-80-7598-554-5
[48] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 401 s. ISBN 978-80-7598-554-5
[49] Tamtéž
[50] Tamtéž

Za velmi úrodné zdroje citlivých informací se dají označit profily na sociálních sítích. Motivací je rozhodně finanční zisk, protože útočník si může jménem oběti vzít půjčku, nakupovat zboží na e-shopech nebo vybírat peníze z bankomatu.[51]

8. Hlavní vlivy na vznik delikvence mládeže v oblasti kyberkriminality

Jak se kybernetické dovednosti s každou generací zlepšují, někteří z mládeže zjišťují, že disponují souborem dovedností, kterým autority v jejich životech plně nerozumějí. Bez řádného vedení může být talent pro určité aspekty informačních technologií využit k negativním prostředkům, místo aby byl směrován pozitivně, což má za následek chybný vstup do světa kyberkriminality. Internet umožňuje mladým lidem omezit svou sociální angažovanost výlučně na konkrétní sdružení nebo sítě. Pro mládež je internet jako svůdná bažina, velmi lákavá pro vstup, ale velmi lepkavá a lze se z ní těžko vymanit.[52]

Autorka práce vidí hlavní vlivy na vznik delikvence mládeže v oblasti kyberkriminality v těchto podnětech:

- finanční zisk
- uspokojení pocitu zvědavosti a vzrušení
- nástroj pro zahnání nudy
- dotyčný to má jako koníček
- pocit anonymity
- úkoly od vrstevníků, ke kterým chce dotyčný zapadnout
- získání výhod v počítačových hrách
- pocit moci

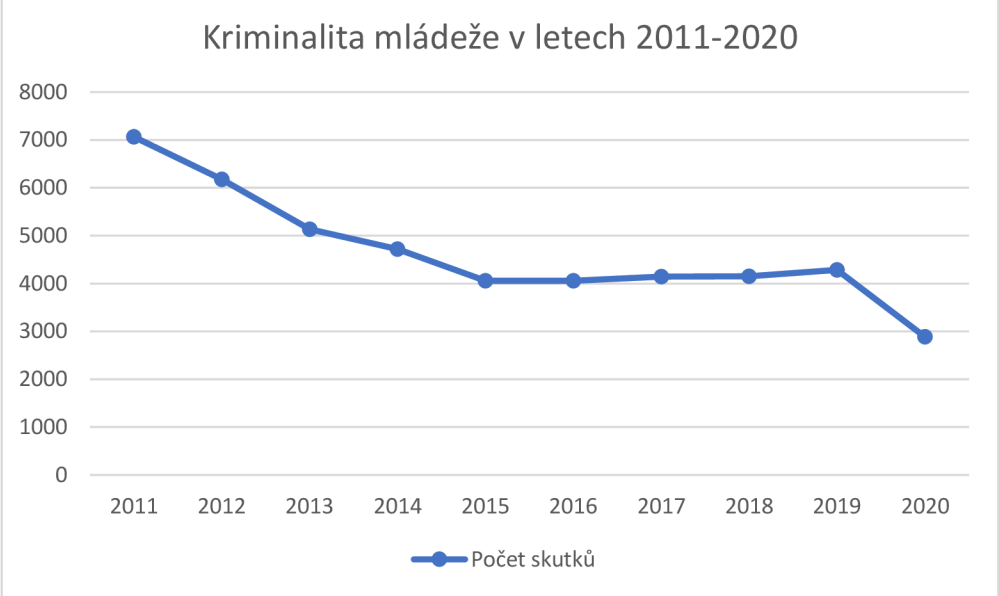
[51] Krádež identity [online]. [cit. 12.1. 2022]. Dostupné z: https://www.eset.com/cz/kradez-identity/
[52] Why young people commit cybercrime [online]. [cit. 20.1. 2022]. Dostupné z: https://www.beaming.co.uk/insights/young-people-get-cybercrime/ http://www.xinhuanet.com/english/2020-01/22/c_138725790.htm

Klíčem k zabránění mládeži v páchání kyberkriminality za účelem dosažení finančního zisku je dát jim možnost využít své dovednosti k dobru a dát jim vědět, že to může být stále lukrativní, ale bez rizika vězení.[53]

9. Vývoj kriminality mládeže a kyberkriminality v České republice

Současný trend kriminality mládeže je pozvolna sestupný, jak dokazuje následný graf. V číslech získaných ze Zpráv o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky z let 2011-2020 jsou brány jako mládež pouze nezletilí a mladiství. Nejsou zde tedy zahrnuta čísla mladých dospělých. Nejčastějšími provině ními/činy jinak trestných jsou v oblasti majetkové trestné činnosti, ostatní kriminality (sprejerství, výtržnictví) a násilné kriminality. Kriminalita mládeže v roce 2020 zaznamenala oproti roku 2019 znatelný pokles. Jednou z možností, jak si tento úkaz vysvětlit je pandemie covid-19. Dále se v roce 2020 žádné výrazné nové trendy nebo formy kriminality mládeže neobjevily.[54]

Graf 2: Kriminalita mládeže v letech 2011-2020



Zdroj: Data získaná ze Zpráv o situaci v oblasti bezpečnosti a veřejného pořádku na území České republiky z let 2011-2020 a z Analýzy trendů kriminality v České republice v roce 2019

[53] Why young people commit cybercrime [online]. [cit. 20.1. 2022]. Dostupné z: https://www.beaming.co.uk/insights/young-people-get-cybercrime/
[54] Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky 2020 [online]. [cit. 24.1. 2022]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

Mládež je velmi aktivní v kyberprostoru. Pomohla tomu i pandemie covid-19. Převážná část mládeže z důvodů online výuky a nemožnosti se osobně scházet a z dostatku volného času, který není kontrolován ze strany rodičů a škol, tráví tento čas v kyberprostoru. V prognóze vývoje trestné činnosti mládeže lze tedy předpokládat, že se bude častěji přesouvat do kyberprostoru.[55]

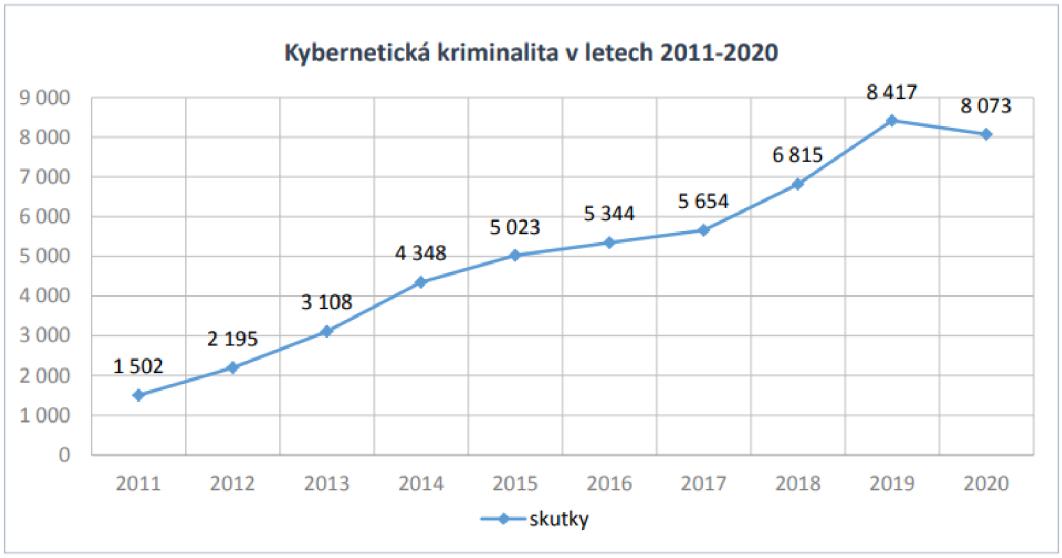
Naopak kybernetická kriminalita má dlouhodobě vzestupný trend. Nejčastějšími trestnými činy v oblasti kyberkriminality jsou podvody mezi soukromými osobami, poškození a zneužití záznamu na nosiči informací, úvěrové podvody a také ostatní mravnostní trestné činy. Lze říci, že například DDoS útoky na počítačové systémy stagnují, více jsou používány phishingové a spear-phishingové útoky s cílem zamoření pomocí napadené přílohy počítačového systému oběti. Vývoj kyberkriminality v České republice se v roce 2020 výrazně nelišil od vývoje ve vyspělých státech Evropy a světa.[56]

S rozvojem současných a vývojem nových informačních a komunikačních technologií lze předpokládat, že kybernetická trestná činnost bude i nadále prostupovat všemi kriminálními problematikami, jelikož řada činností je realizována ve virtuálním prostředí. V dalších letech, stejně jako v minulých rocích, lze očekávat kybernetické útoky s jednoznačným cílem majetkového prospěchu, které budou mít vzrůstající tendenci.[57]

V následujícím grafu je zobrazen vývoj kyberkriminality v České republice za období 2011-2020. Uvedená data v grafu se týkají všech pachatelů. Zahrnují tedy nezletilce, mladistvé i dospělé pachatele.

[55] Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky 2020 [online]. [cit. 24.1. 2022]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx
[56] Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky 2020 [online]. [cit. 24.1. 2022]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx
[57] Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky 2020 [online]. [cit. 24.1. 2022]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

Graf 3: Kybernetická kriminalita v letech 2011-2020



Zdroj: Data získaná ze Zpráv o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky z let 2011-2020

Tabulka 2: Přehled statistických údajů o skutcích dle § 230-232 TZ

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

Zdroj: http://www.ok.cz/iksp/docs/463.pdf

„Z tabulky je zřejmé, že v letech 2000 až 2015 docházelo k postupnému zvyšování počtu zjištěných skutků, přičemž od roku 2010 vykazuje tento růst o poznání větší dynamiku. Nevětší meziroční nárůst v tomto období činící 122 % (tj. o 368 skutků více) byl zaznamenán mezi roky 2013 a 2014. Mezi lety 2015 a 2016 byl zaznamenán největší meziroční pokles ve sledovaném období (o 69 skutků méně). V následujících letech však již počet zjištěných skutků opět začal vykazovat vzrůstající tendenci.“[58]

Data ke kyberkriminalitě mládeže autorka práce nesehnala. V policejních statistikách jsou sice uvedeny počty skutků nezletilých a mladistvých, avšak není u konkrétních trestných činů uvedeno, zda byly spáchány s využitím informačních a komunikačních technologií. Nemá se tedy jak dostat k takovým datům.

10. Kontrola kriminality

Pojem kontrola kriminality se často vyskytuje v rovině trestněprávní, sociologické a i kriminologické. Lze ho definovat jako snahu státu a společnosti o to, aby byla kriminalita udržena v určitých mezích. Kontrola kriminality je uskutečňována dvěma strategiemi. První je strategie represivní, která má trestnou činnost potlačovat. Druhou strategií je prevence. Ta má kriminalitě předcházet.[59]

10.1 Struktura prevence kriminality

Prevence kriminality probíhá na třech úrovních. Jedná se o prevenci sociální, situační a prevenci viktimnosti a pomoci obětem trestných činů.

Sociální prevence představuje aktivity ovlivňující proces socializace a sociální integrace. Dále aktivity orientované na změnu škodlivých společenských a ekonomických podmínek, které jsou považovány za klíčové příčiny páchání trestné činnosti. Sociální prevence je součástí sociální politiky. Účinnost sociální prevence je obtížně statisticky či ekonomicky měřitelná, lze na ni jen usuzovat, a

[58] Fenomenologie kyberkriminality [online]. [cit. 25.2.2022]. Dostupné z: http://www.ok.cz/iksp/docs/463.pdf
[59] Kontrola kriminality [online]. [cit. 27.1. 2022]. Dostupné z: https://www.fsps.muni.cz/inovace-SEBS-ASEBS/elearning/kriminologie/kontrola

to z hlediska odhadů sociálních perspektiv jedinců – objektů preventivního působení.[60]

Situační prevence těží ze zkušeností, že určité druhy kriminality se objevují v určité době, na určitých místech a za určitých okolností. Pomocí opatření režimové, fyzické a technické ochrany se snaží kriminogenní podmínky minimalizovat. Nejúčinněji působí při omezování majetkové trestné činnosti. Úspěšnost situační prevence je vysoká, je však podmíněna odpovídající volbou opatření a finančními a personálními prostředky do ní vložených. Hlavní odpovědnost za opatření situační prevence nesou především občané a obce a v rámci vymezených kompetencí i Ministerstvo vnitra, respektive PČR.[61]

Prevence viktimnosti a pomoc obětem trestných činů je založena na pojetích bezpečného chování, rozdílného s ohledem na různé kriminální situace a psychickou připravenost ohrožených osob. V praxi se jedná o skupinové i individuální zdravotní, psychologické a právní poradenství, trénink v obranných strategiích a propagaci technických možností ochrany před trestnou činností. Užívá metody sociální i situační prevence.[62]

10.2 Úrovně preventivních aktivit

Sociální a situační prevence se vzájemně doplňují v rámci primární, sekundární a terciální prevence.

Primární prevence zahrnuje hlavně výchovné, vzdělávací, volnočasové, osvětové a poradenské aktivity, které jsou zaměřené především na nejširší veřejnost. Specifická pozornost je zaměřena na pozitivní ovlivňování hlavně dětí a mládeže (využívání volného času, možnosti sportovního vyžití). Primární prevence spočívá zejména v rodinách, ve školách a v místních společenstvích.[63]

---

[60] Struktura prevence kriminality [online]. [cit. 8.2. 2022]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/
[61] Struktura prevence kriminality [online]. [cit. 8.2. 2022]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/
[62] Tamtéž
[63] Prevence kriminality [online]. [cit. 9.2. 2022]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/

Sekundární prevence se zaobírá rizikovými jedinci a skupinami osob, u kterých je zvýšená pravděpodobnost, že se stanou pachateli nebo oběťmi trestné činnosti. Dále se zabývá sociálně patologickými jevy (např. drogové a alkoholové závislosti, záškoláctví, gamblerství, povalečství, vandalismus, dlouhodobá nezaměstnanost) a příčinami kriminogenních situací.[64]

Terciární prevence se zakládá v resocializaci kriminálně narušených osob (např. pracovní uplatnění vč. rekvalifikace, sociální a rodinné poradenství, pomoc při získávání bydlení). Jejím záměrem je udržet dosažené účinky předchozích intervencí a rekonstrukce nefunkčního sociálního prostředí.[65]

„Odpovědnost za oblast primární a sociální prevence spadá do působnosti rodiny, obce a Ministerstva školství, mládeže a tělovýchovy. Sekundární a terciární prevence je s ohledem na odbornou náročnost jednotlivých aktivit záležitostí resortu Ministerstva práce a sociálních věcí a v některých souvislostech i Ministerstva spravedlnosti a Ministerstva zdravotnictví. Ve specifické části populace působí i Ministerstvo obrany.“[66]

10.3 Systém prevence kriminality v České republice

V České republice probíhá prevence kriminality na třech základních úrovních. Na meziresortní úrovni působí celostátní koordinační centrum prevence s názvem Republikový výbor pro prevenci kriminality. V jeho čele stojí ministr vnitra a je složený ze zástupců jednotlivých ministerstev a dalších orgánů působících v této oblasti. Tento orgán vytváří pojetí preventivní vládní politiky a pomáhá městům metodickou a konzultační činností. Na resortní úrovni jsou potom stanovovány programy prevence na základě věcné působnosti jednotlivých ministerstev a na místní úrovni je do preventivních programů zapojena také policie, nevládní organizace, orgány veřejné správy a další

[64] Prevence kriminality [online]. [cit. 9.2. 2022]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/
[65] Tamtéž
[66] Tamtéž

instituce působící v obcích. Snaží se podle potřeb a možností dané obce účelným způsobem rozložit působnost prevence sociální a situační.[67]

10.4 Kontrola kriminality mládeže

V trestněprávní rovině se problému kriminality mládeže věnuje zákon č. 218/2003 Sb., o soudnictví ve věcech mládeže, zákon č. 89/2012 Sb., občanský zákoník a zákon č. 359/1999 Sb., o sociálně-právní ochraně dětí.[68]

Pracovníci sociálně-právní ochrany dětí plní důležité úkoly v péči o predelikventní a delikventní děti. Působí v rámci krajských úřadů a obecních úřadů s rozšířenou působností. Snaží se výchovně působit na mládež, poskytují mladým lidem poradenské služby, vedou výchovné pohovory, účastní se trestního řízení proti mladistvým a podávají o klientech orgánům činným v trestním řízení kvalifikované zprávy. Dalším subjektem sociálně-právní ochrany děti jsou sociální asistenti, kteří vykonávají specializovanou činnost. Jedná se o sociální terénní aktivitu, kdy se má za to, že ohrožené jedince je třeba z řad mládeže aktivně vyhledávat z prostředí, kde se vyskytují přirozeně. Jedinci z řad mládeže je možné skutečně pomoci až když si vytvoří pozitivní vztah k sociálnímu pracovníku.[69]

V prevenci lze vystopovat velmi důležité činitele, které nás obklopují v každodenním životě, jako je rodina, škola nebo komunita. Vše musí vytvářet vzájemný soulad, aby dítě nebylo náchylné k trestné činnosti. Pokud tyto činitelé fungují, mohou se stát základním předpokladem pro úspěch v prevenci kriminality mládeže.[70]

Rodina je základ, ze kterého vyrůstáme a utváříme si díky ní názory, zvyky nebo také svou morální kvalitu. Je to první „organizace“, která děti vede ve výchově, ukazuje správnost či neúspěchy rodičovských činů. Formuje děti v

---

[67] Prevence kriminality [online]. [cit. 8.2. 2022]. Dostupné z: https://www.mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09NA%3d%3d

[68] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 506, 507 s. ISBN 978-80-7598-554-5

[69] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 506, 507 s. ISBN 978-80-7598-554-5

[70] Prevence kriminality mládeže [online]. [cit. 15.2. 2022]. Dostupné z: https://is.ambis.cz/th/x9pl6/Benesova_Hana_BP_2017.pdf

plnohodnotného člověka, který se z nich stane v dospělosti. Škola by měla mít kvalitní výuku zajištěnou proškolenými pedagogy, zájmové kroužky vedené v takovém duchu, aby školáky zaujaly a směrovaly k nalezení jejich skutečných individuálních zájmů a potřeb, které by je obohatily v jejich dalším vývoji. Ve škole si děti také tvoří nové přátele. Postupem času si nachází svoji komunitu, která bude mít výrazný vliv na jeho chování. Tento vliv může být kladný anebo záporný.[71]

10.4.1 Cíle pro předcházení kriminality mládeže

Pro úspěšné vedení prevence kriminality mládeže by mohlo pomoci naplnění těchto cílů:

- *„zvyšovat pocit bezpečnosti občanů*
- *začlenit prevenci kriminality do politik obcí, krajů i státu*
- *více spolupracovat mezi orgány státní správy, samosprávy, PČR, občany a nevládními organizacemi, včetně racionálního využívání personálních i finančních zdrojů obohacovat práci PČR o situační přístupy a sociálně preventivní prvky, včetně poradenských a informačních služeb občanům*
- *prohlubovat povědomí veřejnosti o legálních možnostech ochrany před trestnou činností*
- *poskytovat vědecky podloženou péči a služby malým dětem s problematickým chováním i jejich rodinám*
- *najmout místní dobrovolníky a zapojit je v komunitě do práce s vysoce rizikovou a delikventní mládeží*
- *zavést účinné preventivní programy ve školách*
- *zapojit celou komunitu do plánování a zavádění komplexních strategií na prevenci trestné činnosti mládeže, na kterých by se podílely rodiny, školy a celé čtvrti*
- *nasadit větší počet policistů do ulic, více kamerových systémů a osvětlených ulic*

[71] Prevence kriminality mládeže [online]. [cit. 15.2. 2022]. Dostupné z: https://is.ambis.cz/th/x9pl6/Benesova_Hana_BP_2017.pdf

- *budovat pouliční sportoviště pro mládež“*[72]

10.5 Kontrola kyberkriminality

Co se týče represe, jednoznačně na kyberkriminalitu reaguje trestní zákoník prostřednictvím již zmiňovaných počítačových trestních činů a řadou dalších skutkových podstat. Spáchání trestného činu pomocí kyberprostoru je u některých skutkových podstat navíc zvlášť přitěžující okolnost. Kybernetickou bezpečností se dále zabývá především zákon č. 480/2004 Sb., o některých službách informační společnosti, zákon č. 127/2005 Sb., o elektronických komunikacích, zákon č. 110/2019 Sb., o zpracování osobních údajů a zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Poslední zmiňovaný zákon stanovuje pravidla pro vyhodnocování kybernetických rizik a přijímání příslušných opatření, zajišťuje bezpečnost informací v informačních systémech a dostupnost a spolehlivost služeb a sítí elektronických komunikací. Dále stanovuje Národní úřad pro kybernetickou a informační bezpečnost jako ústřední správní orgán pro kybernetickou bezpečnost (dále jen „NÚKIB“) a Národní centrum kybernetické bezpečnosti (dále jen „NCKB“) jako jeho výkonnou sekci, která také provozuje vládní CERT (Computer Emergency Response Team), vyhodnocuje bezpečnostní rizika a činí nezbytná opatření.[73]

„NÚKIB vznikl 1. srpna 2017 a je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo. Do gesce NÚKIB patří také organizace a příprava kybernetických cvičení. Cvičení hrají nezastupitelnou roli při zajišťování kybernetické bezpečnosti České republiky. Umožňují věrně simulovat rozličné typy krizových situací a slouží jak technickému publiku, tak pracovníkům na nejvyšší úrovni s rozhodovacími pravomocemi. Při jejich tvorbě a provedení je zásadní úzká

[72] Prevence kriminality mládeže [online]. [cit. 15.2. 2022]. Dostupné z: https://is.ambis.cz/th/x9pl6/Benesova_Hana_BP_2017.pdf
[73] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 405, 406 s. ISBN 978-80-7598-554-5

kooperace s dalšími partnery v rámci tzv. whole-of-government přístupu. Vedle edukativního prvku cvičení pomáhají budovat důvěru a utužovat vzájemné vztahy.“[74]

„NCKB zajišťuje zejména:

- *činnost Vládního CERT České republiky*
- *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*
- *pořádání a účast na kybernetických cvičeních na národní a mezinárodní úrovni*
- *výzkum a vývoj v oblasti kybernetické bezpečnosti*
- *ve spolupráci s kabinetem ředitele zastupování České republiky 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 České republiky v NATO a členství v EU a členství v jiných mezinárodních organizacích*

[74] Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 22.2. 2022]. Dostupné z: https://www.nukib.cz/cs/o-nukib/ https://www.nukib.cz/cs/kyberneticka-bezpecnost/cviceni/

- *stanovuje komunikační strategii Úřadu v oblasti kybernetické bezpečnosti ve spolupráci s ostatními organizačními celky Úřadu"*[75]

Pro prevenci se rozvíjí obor informatiky zaměřený na ochranu dat, a to počítačová bezpečnost. Každé zařízení využívající kyberprostor by mělo mít ochranný software (antivir). Důležitá je ale také obezřetnost jednotlivých uživatelů při používání hesel, stahování obsahu, nakupování zboží nebo služeb nebo být střídmý při sdělování osobních údajů. Účelné je pravidelné zálohování svých dat. Na závěr je nutné zmínit fyzickou ochranu jednotlivých zařízení a osvětu a vzdělávání v oblasti kyberkriminality.[76]

10.6 Prevence kyberkriminality mládeže

Prevence kriminality je vedle represe součástí trestní politiky. Preventivní politika představuje ofenzivní strategii kontroly kriminality, jež spoléhá hlavně na nerepresivní prostředky. Zabývá se odstraňováním sociálně patologických jevů, snižováním motivů a příležitostí k páchání trestných činů.

Do prevence kyberkriminality mládeže je nutné zapojit na prvním místě rodiče mládeže. Rodiče jako první mohou vidět varovné signály, že se s jejich dětmi něco děje. Mohou si s dětmi promluvit a vést je správným směrem. Mezi varovné signály pro rodiče by mohly patřit tyto body:

- dítě tráví veškerý svůj volný čas na počítači/mobilu/tabletu
- jeví zvláštní zájem o kódování a má učební materiál o práci na počítači, který nepotřebuje do školy
- má nepravidelný spánkový režim
- má finanční příjem ze svých online aktivit
- nechtějí odpovídat na otázky co dělají na počítači/mobilu/tabletu

[75] Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 22.2. 2022]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/
[76] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 406, 407 s. ISBN 978-80-7598-554-5

- stávají se více sociálně izolovanými[77]

Je potřeba svým dětem říct, jak se na internetu chovat, na co si dát pozor a co se nesmí dělat. Rodiče mají taky možnost tzv. rodičovské kontroly nad zařízeními, které jejich děti používají. Jedná se třeba o znemožnění spuštění aplikace nebo omezení času požívání zařízení. Další pomocí je filtrování obsahu internetu, které slouží k ochraně před nevhodným obsahem.[78]

Dalším subjektem prevence kyberkriminality mládeže je škola. Ta by se svými žáky také toto téma měla probírat. Může pořádat různé besedy a zvát si externí pracovníky z této oblasti. Dále může organizovat počítačový kroužek, kde se můžou děti učit, jak s počítačem legálně pracovat. Zde by mohli děti uplatnit i svůj talent pro informační a komunikační technologie. Nemusely by tudíž experimentovat bez dozoru doma a případně se zaplést do něčeho nelegálního.[79]

Jiným subjektem jsou různé neziskové sdružení. Tvoří kampaně, které jsou vidět na internetu, v televizi ale i na ulici. Za zmínku stojí Národní centrum bezpečnějšího internetu (dále jen „NCBI"). *„Jeho posláním je přispívat ke zvýšení bezpečnosti užívání internetu, moderních informačních a komunikačních technologií, zvyšovat povědomí uživatelů o jejich kladech a možných nebezpečích, přispívat k osvojování etických norem v online prostředí, napomáhat předcházení a snižování možných sociálních rizik spojených s jejich užíváním."* NCBI je členem celoevropské sítě národních osvětových center bezpečnějšího internetu INSAFE. NCBI provádí řadu projektů, z nichž nejdůležitější je Saferinternet.cz, ten je zaměřený na zvyšování povědomí o bezpečnějším užívání internetu, pomoc uživatelům internetu v potížích, a na boj proti šíření ilegálního obsahu online. K jejich dalším významným projektům patří Bezpečně online, Proti nenávisti online, Mladí proti

---

[77]Prevention of juvenile cybercrime [online]. [cit. 25.1. 2022]. Dostupné z: https://www.getsafeonline.org/personal/blog-item/cybercrime-preventing-young-people-from-getting-involved/

[78] GŘIVNA, Tomáš, SCHEINOST, Miroslav, ZOUBKOVÁ Ivana a kol. *Kriminologie*. 5., aktualizované vydání. Praha: Wolters Kluwer, 2019. 407 s. ISBN 978-80-7598-554-5

[79] Prevention of juvenile cybercrime [online]. [cit. 25.1. 2022]. Dostupné z: https://www.getsafeonline.org/personal/blog-item/cybercrime-preventing-young-people-from-getting-involved/

nenávisti online. Ve spolupráci se svými partnery pořádá konference, semináře, přednášky a školení zaměřené na oblast bezpečnějšího užívání internetu a prevenci internetové kriminality.[80]

Projekt Bezpečně online je zaměřený na mládež s cílem napomáhat u nich k bezpečnému a sebejistému používání internetu a nových komunikačních technologií. Tematickým těžištěm je hlavně bezpečné používání finančních online služeb, aktivní ochrana soukromých informací před zneužitím a efektivní využívání možností informačních technologií a internetu. Kromě osvěty mezi mládeží mají jejich webové stránky za cíl také poskytnout základní metodickou pomoc učitelům a rodičům.[81]

Kampaň Mladí proti nenávisti online je zaměřená v prvé řadě na potlačení projevů nenávisti v prostředí online, a to ať už jde o projevy extremismu, rasové úzkoprsosti, nebo utlačování menšin, ale zajisté i podporu etického a slušného chování při online komunikaci. Cílovým subjektem této kampaně je mládež, která v současnosti tráví mnoho svého volného času komunikací především v prostředí sociálních sítí. Druhým subjektem jsou dospělí – hlavně učitelé a knihovníci, kteří s oslovenou skupinou přímo pracují.[82]

Dalším sdružením v oblasti kyberkriminality je CZ.NIC. Jedná se o správce české domény nejvyšší úrovně. Cílem jejich akademie je vzdělávání a osvěta v oblasti internetových technologií. Své služby poskytuje nejenom počítačovým profesionálům, ale i laické veřejnosti, studentům a učitelům od základní až po vysokou školu. Provozují kurzy o konkrétních tématech. Přednášenou látku si lze vyzkoušet i v praxi.[83] Tyto kurzy mohou být ideální pro mládež, která touží s internetem nebo technologiemi experimentovat. Zde tak mohou činit pod dozorem a nemusí se dopustit něčeho nelegálního, jak se často může stát u nich doma bez dozoru.

---

[80] Prevence kyberkriminality mládeže [online]. [cit. 25.1. 2022]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/rozcestnik-kyberkriminality/
[81] Bezpečně online [online]. [cit. 24.2. 2022]. Dostupné z: https://bezpecne-online.ncbi.cz/uvod/o-projektu
[82] Mladí proti nenávisti online [online]. [cit. 24.2. 2022]. Dostupné z: https://www.ncbi.cz/projekty/ukoncene-projekty/mladi-proti-nenavisti-online.html
[83] CZ.NIC akademie [online]. [cit. 24.2. 2022]. Dostupné z: https://akademie.nic.cz/

Na tomto místě by autorka také ráda zmínila Bílý kruh bezpečí a Linku bezpečí. Bílý kruh bezpečí poskytuje přímou pomoc obětem a svědkům trestných činů, podílí se na prevenci kriminality a usiluje o zlepšení práv a postavení poškozených v trestním řízení. Jejich služba je odborná, bezplatná, diskrétní, nestranná a nezávislá. Osobní kontakt zajišťuje pokaždé dvojice poradců, právník a psycholog. Od kontaktu s Bílým kruhem bezpečí lze očekávat:

- *„bezpečný prostor a podporu při ventilaci svých oprávněných emocí (stud, ponížení, lítost, hněv, zármutek, pocit viny aj.)*
- *znovuobnovení pocitu bezpečí*
- *prověření základních potřeb (zdraví, bydlení, finance, zaměstnání, vztahy aj.) a hledání potřebných zdrojů*
- *pomoc při zhodnocení aktuální situace, utřídění individuálních cílů*
- *srozumitelné informace o právech obětí trestných činů a rady, jak na tato práva dosáhnout*
- *stanovení priorit, první nezbytné kroky k nápravě škod, poradenství při hledání strategií (krátkodobých i dlouhodobých)*
- *informování o navazujících službách, event. doporučení nebo zprostředkování takové služby*
- *v mimořádně závažných případech nabídku doplňkových služeb Bílého kruhu bezpečí“*[84]

Na Bílý kruh bezpečí se mohou obrátit nejen oběti ale i mládež, která ví, že dělá něco, co se nemá, už si sama neví rady, jak z toho ven a rodičům se bojí svěřit.

Úkolem Linky bezpečí je poskytování kvalitní a snadno dostupné pomoci dětem, studentům a všem, kteří jednají v jejich zájmu. Pomáhá s řešením náročných životních situací i každodenních starostí a problémů. Zároveň provozuje Rodičovskou linku, která je určená nejen rodičům, ale i všem

[84] Bílý kruh bezpečí [online]. [cit. 24.2. 2022]. Dostupné z: https://www.bkb.cz/o-nas/poslani-a-cinnost/

dospělým se starostí o dítě. Linka bezpečí je stejně jako Bílý kruh bezpečí bezplatná a anonymní pomoc.[85]

Prevence kyberkriminality mládeže by se tedy dala shrnout do těchto bodů:

- zvyšování povědomí s cílem informovat mládež a rodiče
- vzdělávání mládeže o kybernetické bezpečnosti, kybernetické kriminalitě a zákonech ve školách
- identifikování nejvíce ohrožených skupin mládeže a pracovat s nimi
- šíření národní reklamní kampaně v oblasti kyberkriminality[86]

[85] Linka bezpečí [online]. [cit. 24.2. 2022]. Dostupné z: https://spolek.linkabezpeci.cz/o-nas/
[86] Prevention of juvenile cybercrime [online]. [cit. 25.1. 2022]. Dostupné z: https://www.paladincapgroup.com/wp-content/uploads/2016/11/Pathways-White-Paper-US-final-1.pdf

Praktická část

1. Dotazníkové šetření

K uskutečnění zkoumání rozšířenosti kyberkriminality mládeže byla využita kvantitativní metoda formou dotazníkového šetření. Technika dotazníku byla zvolena z důvodu možnosti oslovení velkého počtu mládeže a možnosti následné celkové analýzy výsledků.

1.1 Cíle dotazníkového šetření

Hlavním cílem dotazníkového šetření je zjistit rozsah kyberkriminality mládeže. Dalším cílem je potvrdit domněnku, že kyberkriminalita se ve větším rozsahu páchá až v dospělém věku. V dotazníkovém šetření by tedy měly být skoro všechny odpovědi na otázky páchání jakéhokoliv druhu kyberkriminality negativní.

1.2 Výzkumné předpoklady

1) Většina dotazované mládeže nepáchá kyberkriminalitu.
2) Alespoň polovina respondentů zná někoho, kdo kyberkriminalitu páchá.
3) Nejmladší věková kategorie respondentů (12-14 let) páchá kyberkriminalitu nejméně ze všech tří dotazovaných věkových kategorií.
4) Většině respondentů není kontrolován čas strávený na počítači/mobilu/tabletu ze strany rodičů.

1.3 Charakteristika dotazníkového šetření

Dotazník je tvořen 31 otázkami. Ze začátku respondenti odpovídají na obecné otázky týkající se pohlaví, věku, vzdělání a v jak velkém městě žijí. Následují konkrétní otázky zaměřené na páchání kyberkriminality. Všechny otázky (kromě jedné, která je otevřená) jsou uzavřené. Dotazník je přílohou č. 1 této práce.

Dotazník byl respondentům podaný elektronicky. Dělo se tak v lednu 2022 a dotazník byl k dispozici 9 dní. Byla k tomu využita internetová stránka Survio[87]. Dotazníkové šetření probíhalo anonymně a v úvodu byl kladen důraz na podmínku dotazníku, že je pouze pro osoby ve věkové kategorii 12-24 let. Dotazník vyplnilo celkem 219 respondentů. Jejich výběr byl nahodilý na základě dobrovolnosti.

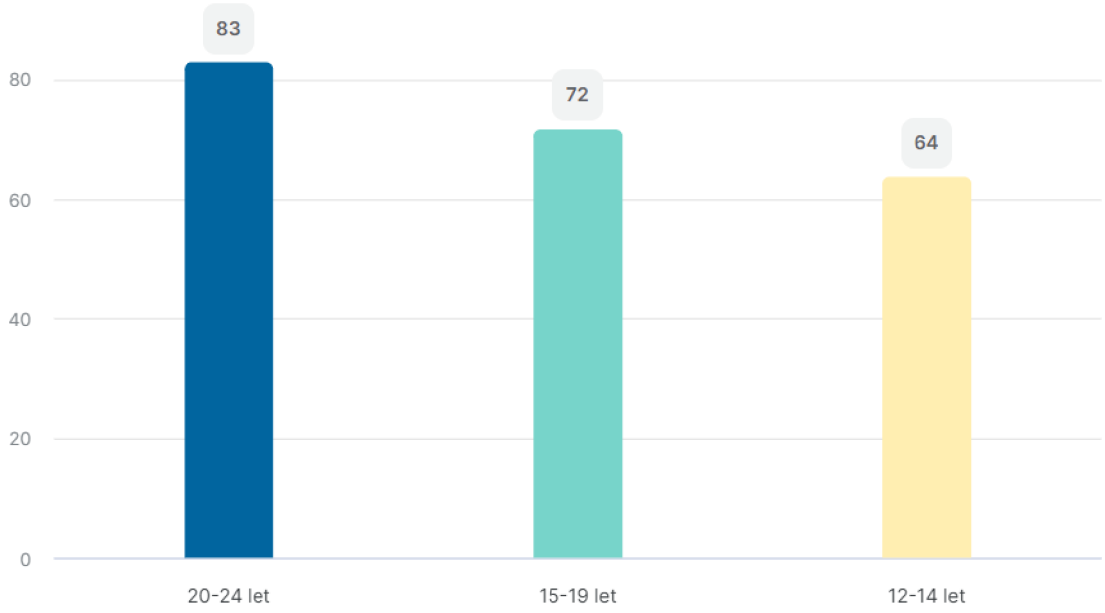
1.4 Výsledky dotazníkového šetření

V této části budou postupně reprezentovány otázky dotazníku a odpovědi na ně. Na povinné otázky odpovědělo již zmiňovaných 219 respondentů. Na poslední otázku (jediná otevřená a nepovinná), která byla určena jen pro ty, kteří v předchozí otázce odpověděli kladně odpovědělo 35 respondentů.

Otázka č. 1: Jaké je vaše pohlaví:

Z výsledků vyplývá, že dotazníkového šetření se zúčastnilo 118 žen (53,9 %) a 101 mužů (46,1 %).

Otázka č. 2: Jaký je váš věk:



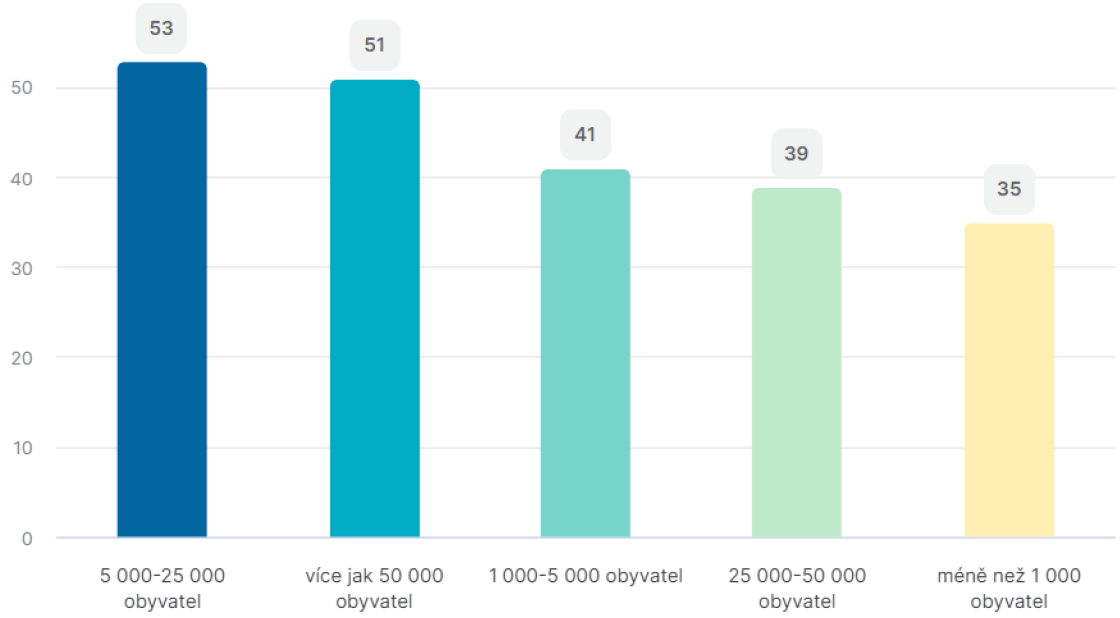
Graf 4: Otázka č. 2: Jaký je váš věk

[87] https://www.survio.com/cs/

U této otázky respondenti vybírali ze tří možností a to 12-14 let, 15-19 let, 20-24 let. Z grafu vyplývá, že věkové rozdělení dopadlo takto:

- 12-14 let → 64 respondentů (29,2 %)
- 15-19 let → 72 respondentů (32,9 %)
- 20-24 let → 83 respondentů (37,9 %)

Otázka č. 3: V jak velkém městě (vesnici žijete):



Graf 5: Otázka č. 3: V jak velkém městě (vesnici) žijete

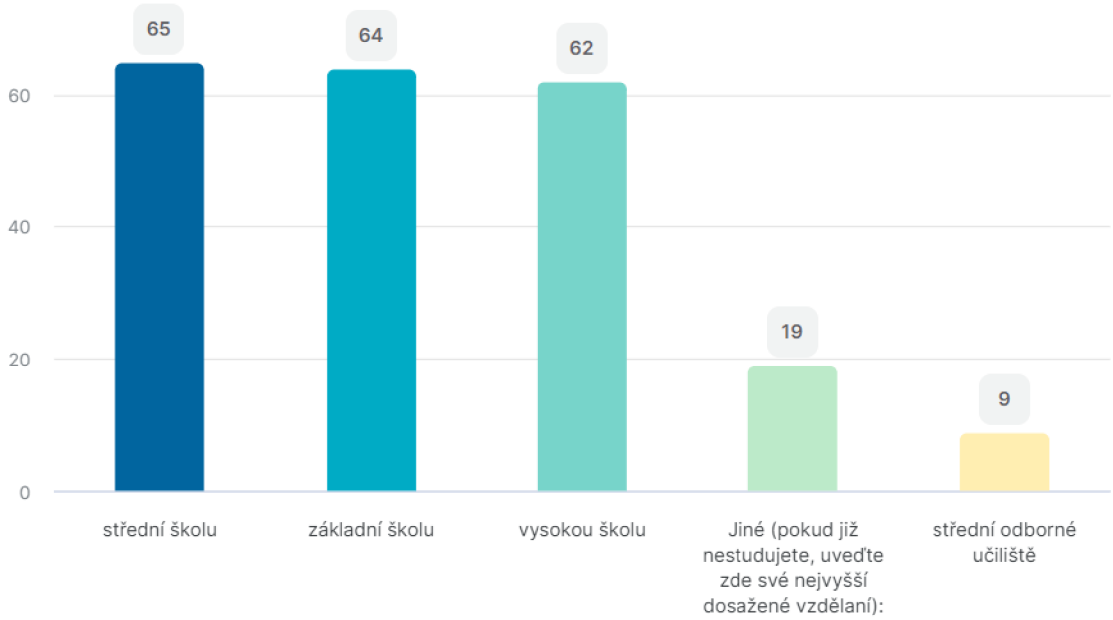
Z grafu plynou následující údaje:

- méně než 1 000 obyvatel → 35 respondentů (16 %)
- 1 000 – 5 000 obyvatel → 41 respondentů (18,7 %)
- 5 000 – 25 000 obyvatel → 53 respondentů (24,2 %)
- 25 000 – 50 000 obyvatel → 39 respondentů (17,8 %)
- více jak 50 000 obyvatel → 51 respondentů (23,3 %)

Otázka č. 4: Jakou školu studujete:

Z následujícího grafu lze vyčíst, že největší zastoupení má střední škola (65 respondentů → 29,7 %), následuje základní škola (64 respondentů → 29,2 %), vysoká škola (62 respondentů → 28,3 %). V odpovědi jiné (pokud, již

nestudujete, uveďte nejvyšší dosažené vzdělání), na kterou odpovědělo 19 respondentů (8,7 %), se vyskytuje základní škola, střední škola a vysoká škola nejčastěji uvedená jako „Bc.“. Nejméně zastoupená odpověď je střední odborné učiliště (9 respondentů → 4,1 %).



Graf 6: Otázka č. 4: Jakou školu studujete

Otázka č. 5: Používáte sociální sítě:

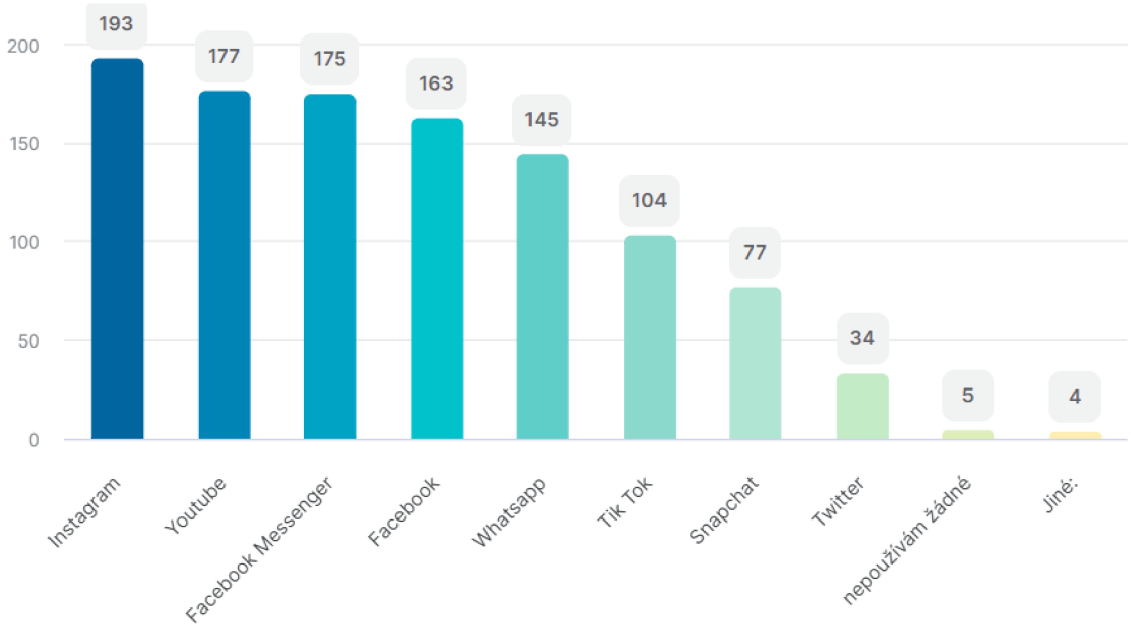
Odpovědi byly zcela jednoznačné. Kladně odpovědělo 212 respondentů (96,8 %). Záporně odpovědělo pouze 7 respondentů (3,2 %).

Otázka č. 6: Jaké sociální sítě používáte:

U této otázky šlo vybrat několik odpovědí. Z následujícího grafu vyplývají tyto údaje:

- Facebook používá 163 respondentů (74,4 %)
- Facebook Messenger používá 175 respondentů (79,9 %)
- Instagram používá 193 respondentů (88,1 %)
- Whatsapp používá 145 respondentů (66,2 %)
- Tik Tok používá 104 respondentů (47,5 %)

- Snapchat používá 77 respondentů (35,2 %)
- Youtube používá 177 respondentů (80,8 %)
- Twitter používá 34 respondentů (15,5 %)
- pro odpověď nepoužívám žádné se rozhodlo 5 respondentů (2,3 %)
- odpověď jiné označili 4 respondenti (1,8 %) – figurovali zde odpovědi: Discord, Reddit, LinkedIn, 4chan, Telegram

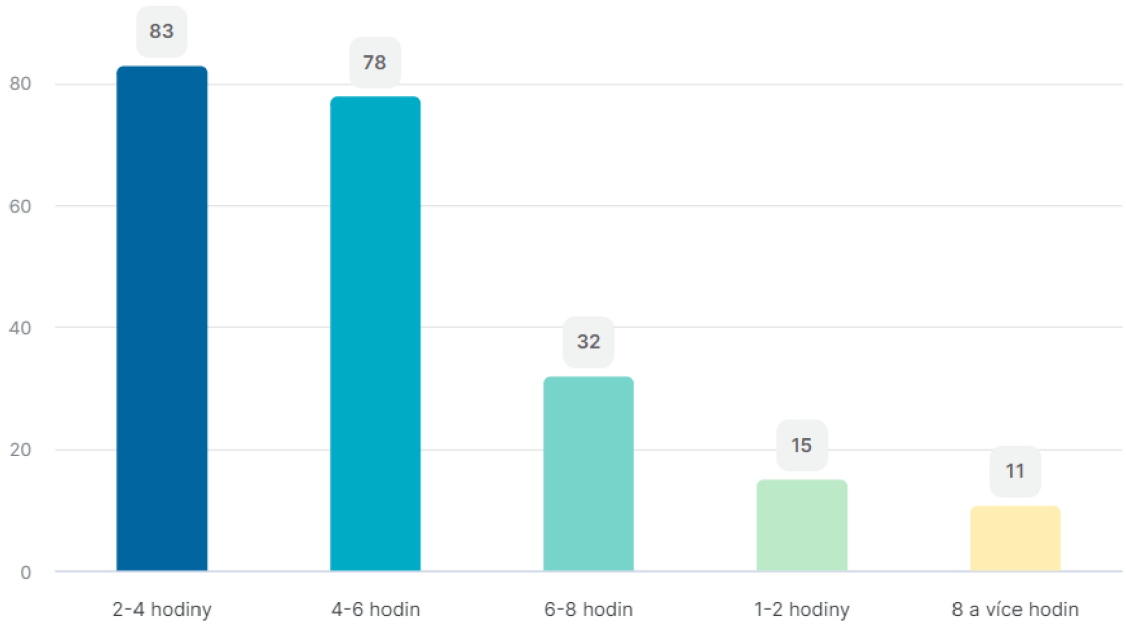


Graf 7: Otázka č. 6: Jaké sociální sítě používáte

Otázka č. 7: Kolik hodin denně trávíte na počítači/mobilu/tabletu:

Z následujícího grafu vyplývají tyto údaje:

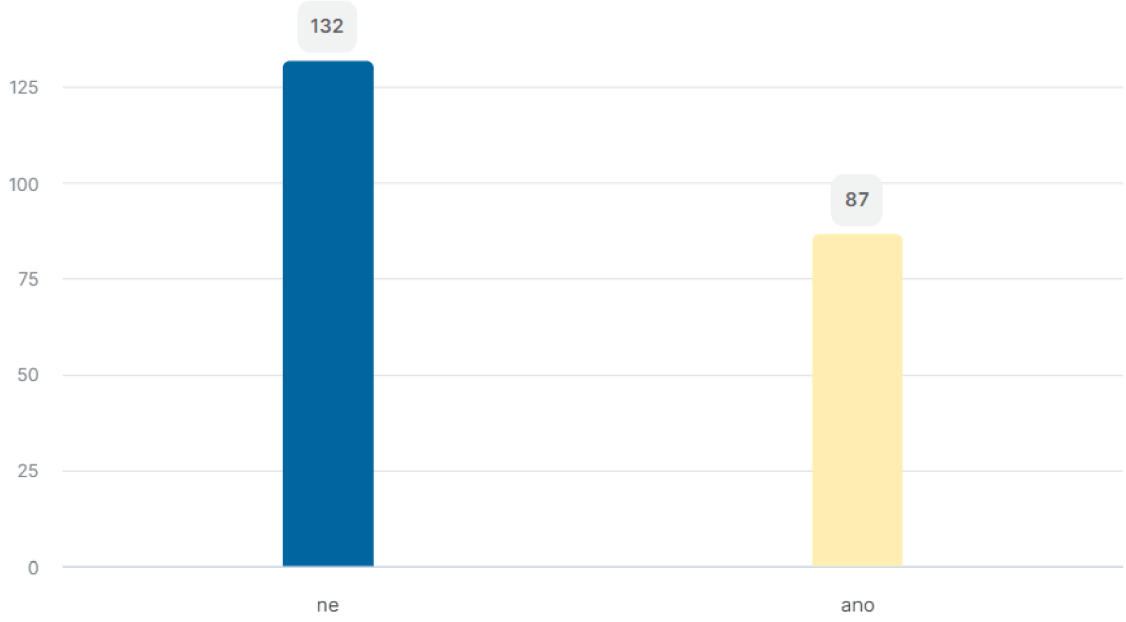
- 1–2 hodiny → 15 respondentů (6,8 %)
- 2–4 hodiny → 83 respondentů (37,9 %)
- 4–6 hodin → 78 respondentů (35,6 %)
- 6–8 hodin → 32 respondentů (14,6 %)
- 8 a více hodin → 11 respondentů (5,1 %)



Graf 8: Otázka č. 7: Kolik hodin denně trávíte na počítači/mobilu/tabletu

Otázka č. 8: Víte, co je to phishing a pharming:

Tyto pojmy znalo 87 respondentů (39,7 %). Naopak je neznalo 132 respondentů (60,3 %).



Graf 9: Otázka č. 8: Víte, co je to phishing a pharming

Otázka č. 9: Pokud ano, uměli byste ho vytvořit:

Zde odpovědělo kladně 19 respondentů (8,7 %). Negativně odpovědělo 81 respondentů (37 %). Odpověď „na předchozí otázku jsem odpověděl/a záporně“ si vybralo 119 respondentů (54,3 %).

Otázka č. 10: Pokud ano, používáte ho pravidelně ve svůj prospěch:

Na tuto otázku respondenti odpověděli takto:

- ano → 3 respondenti (1,4 %)
- jen občas → 1 respondent (0,5 %)
- ne → 43 respondentů (19,6 %)
- na předchozí otázku jsem odpověděl/a záporně → 172 respondentů (78,5 %)

Otázka č. 11: Znáte někoho, kdo to dělá:

U této otázky jsou odpovědi opět zcela jednoznačné. Kladně odpovědělo 10 respondentů (4,6 %). Záporně odpovědělo 209 respondentů (95,4 %).

Otázka č. 12: Víte, co je to počítačový vir:

Odpovědi jsou znovu zcela jednoznačné. Počítačový vir zná 216 respondentů (98,6 %) a neznají ho pouze 3 respondenti (1,4 %).

Otázka č. 13: Pokud ano, umíte ho vytvořit:

Na tuto otázku kladně odpovědělo 10 respondentů (4,6 %). Negativně odpovědělo 206 respondentů (94,1 %). Pro odpověď „na předchozí otázku jsem odpověděl/a záporně“ se rozhodli 3 respondenti (1,3 %).

Otázka č. 14: Pokud ano, využíváte ho pravidelně ve svůj prospěch:

Odpovědi zde vyšly takto:

- ano → 3 respondenti (1,4 %)
- jen občas → 1 respondent (0,5 %)

- ne → 84 respondentů (38,4 %)
- na předchozí otázku jsem odpověděl/a záporně → 131 respondentů (59,7 %)

Otázka č. 15: Znáte někoho, kdo to dělá:

Zde kladně odpovědělo 22 respondentů (10 %) a záporně 197 respondentů (90 %).

Otázka č. 16: Víte, co je to krádež identity:

Tato otázka byla zodpovězena skoro všemi respondenty kladně → 207 respondentů (94,5 %). Záporně odpovědělo pouze 12 respondentů (5,5 %).

Otázka č. 17: Dokázal/a byste někomu ukrást identitu prostřednictvím počítače/mobilu/tabletu:

Zde kladně odpovědělo 56 respondentů (25,6 %). Negativně odpovědělo 151 respondentů (68,9 %). Odpověď „na předchozí otázku jsem odpověděl/a záporně“ si vybralo 12 respondentů (5,5 %).

Otázka č. 18: Už jste to někdy udělal/a:

Kladně odpovědělo 11 respondentů (5 %). Záporně se vyjádřilo 124 respondentů (56,6 %). Pro odpověď „na předchozí otázku jsem odpověděl/a záporně“ se rozhodlo 84 respondentů (38,4 %).

Otázka č. 19: Znáte někoho, kdo to udělal:

Výsledky ukázaly, že 62 respondentů (28,3 %) zná někoho, kdo jinému identitu ukradl, a 157 respondentů (71,7 %) nikoho takového nezná.

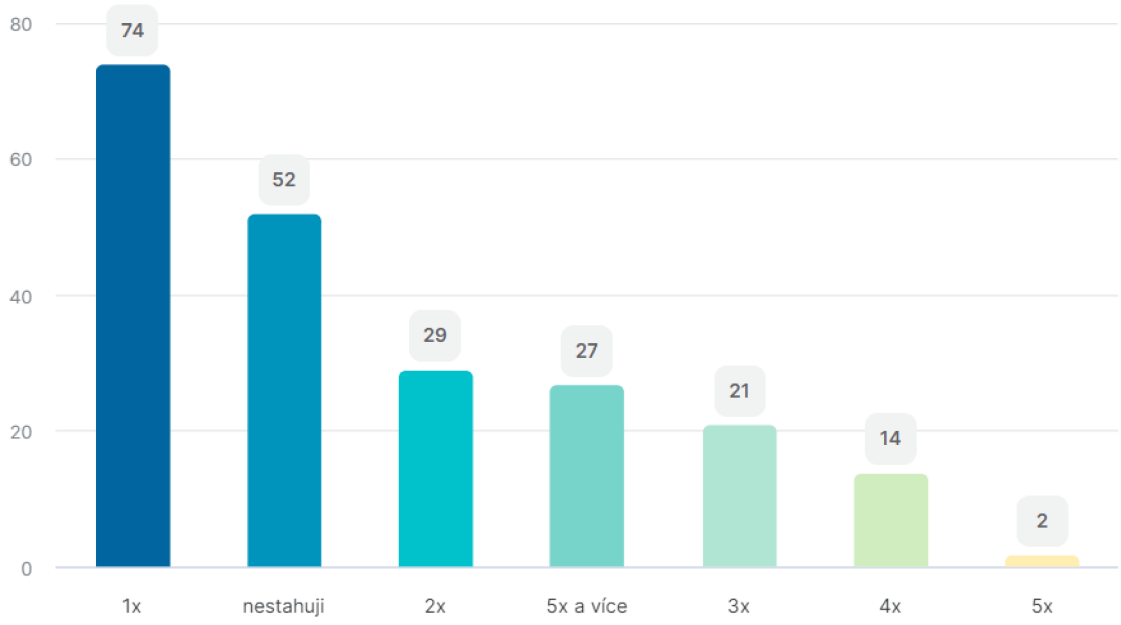
Otázka č. 20: Stáhli jste někdy z neoficiálních internetových stránek muziku nebo film:

Na tuto otázku kladně odpovědělo 186 respondentů (84,9 %). Záporně se vyjádřilo 33 respondentů (15,1 %).

Otázka č. 21: Pokud ano, kolikrát měsíčně se tak děje:

Z následujícího grafu lze vyčíst tyto údaje:

- 1x měsíčně stahuje 74 respondentů (33,8 %)
- 2x měsíčně stahuje 29 respondentů (13,2 %)
- 3x měsíčně stahuje 21 respondentů (9,6 %)
- 4x měsíčně stahuje 14 respondentů (6,4 %)
- 5x měsíčně stahují 2 respondenti (0,9 %)
- 5x a více měsíčně stahuje 27 respondentů (12,3 %)
- odpověď nestahuji si vybralo 52 respondentů (23,8 %)



Graf 10: Otázka č. 21: Pokud ano, kolikrát měsíčně se tak děje

Otázka č. 22: Znáte někoho, kdo pravidelně stahuje muziku nebo filmy z neoficiálních internetových stránek:

Zde odpovědělo kladně 164 respondentů (74,9 %). Záporně odpovědělo 55 respondentů (25,1 %).

Otázka č. 23: Požadovali jste po někom někdy nahé fotografie prostřednictvím počítače/mobilu/tabletu:

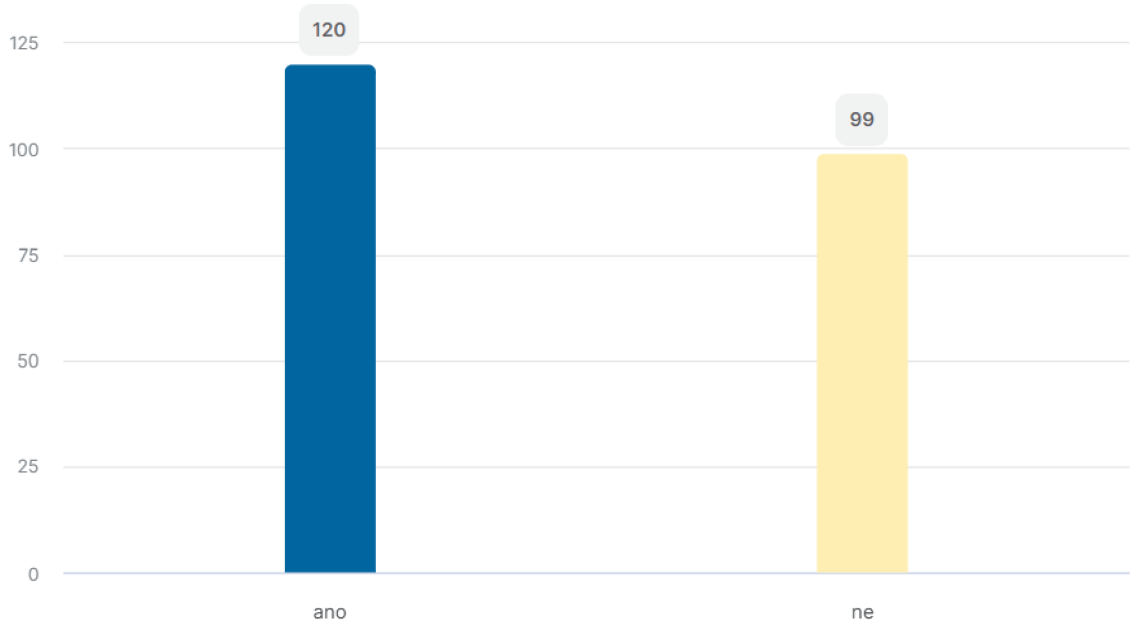
Výsledky ukázaly, že 31 respondentů (14,2 %) v minulosti požadovalo nahé fotografie a 188 (85,8 %) respondentů je nepožadovalo.

Otázka č. 24: Vydírali jste později těmito fotografiemi dotyčného:

Na tuto otázku odpovědělo kladně 6 respondentů (2,7 %). Negativně se vyjádřilo 83 respondentů (37,9 %). Odpověď „na předchozí otázku jsem odpověděl/a záporně“ si vybralo 130 respondentů (59,4 %).

Otázka č. 25: Znáte někoho, kdo by odpověděl kladně na otázku č. 23:

Výsledky ukázaly, že 120 respondentů (54,8 %) zná někoho, kdo požadoval nahé fotografie, a 99 respondentů (45,2 %) nikoho takového nezná.



Graf 11: Otázka č. 25: Znáte někoho, kdo by odpověděl kladně na otázku č. 23

Otázka č. 26: Znáte někoho, kdo by odpověděl kladně na otázku č. 24:

Zde výsledky ukázaly, že 63 respondentů (28,8 %) zná někoho, kdo nahými fotografiemi dotyčného vydíral, a 156 respondentů (71,2 %) nikoho takového nezná.

Otázka č. 27: Šikanujete někoho opakovaně prostřednictvím počítače/mobilu/tabletu:

Zde odpověděli kladně 4 respondenti (1,8 %). Negativně odpovědělo 210 respondentů (95,9 %). Pro odpověď „v minulosti ano" se rozhodlo 5 respondentů (2,3 %).

Otázka č. 28: Využíváte k tomu svůj vlastní nebo falešný profil na sociálních sítích/e-mailu/seznamce:

Výsledky ukázaly tyto údaje:

- vlastní profil → 8 respondentů (3,7 %)
- falešný profil → 9 respondentů (4,1 %)
- na předchozí otázky jsem odpověděl/a záporně → 202 respondentů (92,2 %)

Otázka č. 29: Znáte někoho, kdo šikanuje prostřednictvím počítače/mobilu/tabletu:

Na tuto otázku odpovědělo kladně 47 respondentů (21,5 %) a záporně 172 respondentů (78,5 %).

Otázka č. 30: Kontrolují vám rodiče, co děláte na počítači/mobilu/tabletu:

Zde respondenti odpověděli takto:

- ano → 10 respondentů (4,6 %)
- dříve ano, teď vzhledem k věku už ne → 65 respondentů (29,7 %)
- ne → 144 respondentů (65,7 %)

Otázka č. 31: Pokud ano, jakým způsobem:

Tato otázka byla jako jediná otevřená a nepovinná, vzhledem k tomu, že ne každému dítěti rodiče kontrolují počítač/mobil/ tablet. Odpovědi, které se zde vyskytly, zněly takto:

- *„časové omezení a omezení vyhledávání*
- *Dám jim mobil, ať se do něho kouknou.*
- *Dívali se bez mého vědomí do mých zařízení.*
- *Jen prohledali konverzace.*
- *Kdysi mi kontrolovali hry, jaké jsem mohl hrát a obecně co bylo nainstalované na počítači (jenom taťka tam mohl instalovat nové věci). Dále moc nekontrolovali další obsah, jelikož v té době neexistovalo tolik "hrozeb", jelikož jsem měl přísný zákaz sociálních sítí, které se v tu dobu pouze rozjížděly.*
- *kontrola Osobní orientace*
- *Kontrolovali historii prohlížeče.*
- *Kontrolovali, s kým si píšu.*
- *Koukají do historie a taťka vidí na co koukám.*
- *Musela jsem jim ukázat telefon, co dávám na soc. sítě a s kým si píšu.*
- *na aplikaci u sebe v mobilu*
- *náhodně kontrolují stránky*
- *Za čas se mě zeptali, co dělám na mobilu a chtěli něco ukázat, např. na co koukám na YouTube.*
- *Sama od sebe jí občas ukážu, co tam mám, ale jinak mi to nekontroluje.*
- *rodičovská aplikace*
- *přístup k heslům různých aplikací a samotnému telefonu*
- *Rodiče mají u sebe v mobilu aplikaci a tam vidí, co dělám na mobilu.*
- *omezením času stráveného na počítači*
- *Občas se kouknou, co na tom telefonu dělám a píšu za zprávy.*

- *Občas mi mamka řekne abych ji ukázal svůj instagramový profil, aby viděla, jestli tam nedávám nějaké nevhodné fotky vzhledem k mému věku.“*

Vyskytly se zde i odpovědi typu *„nevím, normálně, už si přesně nepamatuji, nechci odpovídat, nekontrolují“.*

1.5 Vyhodnocení výzkumných předpokladů

V této části autorka práce vyhodnotí, zda výsledky dotazníkové šetření potvrzují výzkumné předpoklady nebo jestli se od nich liší či je naprosto vyvrací. Postupně bude zhodnocen každý výzkumný předpoklad.

1) Většina dotazované mládeže nepáchá kyberkriminalitu.

Z vyhodnocení autorčina dotazníkového šetření vyplývá, že phishing a pharming pravidelně používá 1,4 % respondentů a jen občas ho používá pouze 0,5 % respondentů. Phishing a pharming navíc víc jak půlka respondentů ani nezná (60,3 %). Počítačový vir pravidelně používá 1,4 % respondentů a jen občas ho používá pouze 0,5 % respondentů. V minulosti 5 % respondentů ukradlo někomu identitu prostřednictvím počítače/mobilu/tabletu, 84,9 % respondentů stáhlo muziku nebo filmy z neoficiálních internetových stránek, 14,2 % respondentů po někom požadovalo nahé fotografie a 2,7 % těmito fotografiemi dotyčného později i vydíralo. Prostřednictvím počítače/mobilu/tabletu šikanuje pouze 1,8 % respondentů.

Jak vidíme, pouze u nelegálního stahování jsou tři čtvrtiny kladných odpovědí. U ostatní kyberkriminality je takových odpovědí méně než 20 %. Ve výsledku lze tedy říci, že první výzkumný předpoklad byl správný.

2) Alespoň polovina respondentů zná někoho, kdo kyberkriminalitu páchá.

U phishingu a pharmingu zná 4,6 % respondentů někoho, kdo ho používá. U počítačového viru je to 10 % respondentů. Dále 28,3 % respondentů zná někoho, kdo jinému ukradl identitu prostřednictvím počítače/mobilu/tabletu, 74,9 % respondentů zná někoho, kdo stahuje muziku nebo filmy z neoficiálních

internetových stránek. U 54,8 % respondentů je někdo v okolí, kdo požaduje nahé fotografie od ostatních a 28,8 % respondentů zná i někoho, kdo jimi později vydírá. Na konec 21,5 % respondentů zná někoho, kdo šikanuje prostřednictvím počítače/mobilu/tabletu.

Podle uvedených dat se druhý výzkumný předpoklad nepotvrdil. Pouze u dvou druhů kyberkriminality (nelegální stahování a sexting) alespoň polovina respondentů zná někoho, kdo ji páchá. U dalších druhů kyberkriminality jsou procenta hluboko pod polovinou. Tento výzkumný předpoklad autorka tedy označuje za ne zcela pravdivý.

3) Nejmladší věková kategorie respondentů (12-14 let) páchá kyberkriminalitu nejméně ze všech tří dotazovaných věkových kategorií.

Podle výsledků jednotlivých odpovědí autorka práce vytvořila tabulku pro přehlednější uvedení dat k tomuto výzkumnému předpokladu.

č. otázky / věk	**otázka č. 10**	**otázka č. 14**	**otázka č. 18**	**otázka č. 20**	**otázka č. 23**	**otázka č. 24**	**otázka č. 27**
12-14	1	1	2	50	9	4	1
15-19	2	2	3	62	5	1	2
20-24	0	0	9	77	17	1	1

Tabulka 3: Páchání kyberkriminality podle věku

Dle dat v tabulce lze říci, že páchání kyberkriminality podle věkové kategorie se tak razantně neliší. Nejmladší kategorie má nejmenší počet odpovědí u dvou otázek. Prostřední věková kategorie má nejmenší počet u jedné otázky a nejstarší věková kategorie u dvou otázek. Stejný počet odpovědí se objevil u dvou otázek.

V souhrnu lze tedy uvést, že tento předpoklad se nepodařilo dokázat.

4) Většině respondentů není kontrolován čas strávený na počítači/mobilu/tabletu ze strany rodičů.

Výsledky dotazníku ukázaly, že pouze 4,6 % respondentům rodiče kontrolují čas a aktivitu na počítači/mobilu/tabletu. V minulosti se tak dělo 29,7 % respondentům. Pokud se tyto dva údaje sečtou, kladně odpovědělo pouze

34,3 % respondentů. Naopak 65,7 % respondentům rodiče strávený čas a aktivitu na počítači/mobilu/tabletu nekontrolují.

Kladných odpovědí, vzhledem k tomu, jak je kyberprostor nebezpečný, bylo opravdu málo. Tím pádem byl ale čtvrtý výzkumný předpoklad správný a podařilo se ho potvrdit.

1.6 Závěrečné zhodnocení dotazníkového šetření

V této kapitole autorka práce zhodnotí hlavní cíle, které byly stanoveny. Jednalo se o zjištění rozsahu kyberkriminality mládeže a o domněnku, že kybekriminalita se ve větším rozsahu páchá až v dospělém věku.

Jak již bylo poukázáno u vyhodnocení prvního výzkumného předpokladu, phishing a pharming pravidelně používá 1,4 % respondentů a jen občas ho používá pouze 0,5 % respondentů. Počítačový vir pravidelně používá 1,4 % respondentů a jen občas ho používá pouze 0,5 % respondentů. V minulosti 5 % respondentů ukradlo někomu identitu prostřednictvím počítače/mobilu/tabletu, 84,9 % respondentů stáhlo muziku nebo filmy z neoficiálních internetových stránek, 14,2 % respondentů po někom požadovalo nahé fotografie a 2,7 % těmito fotografiemi dotyčného později i vydíralo. Prostřednictvím počítače/mobilu/tabletu šikanuje pouze 1,8 % respondentů.

V souhrnu z těchto dat tedy vyplývá, že rozsah kyberkriminality mládeže je velmi malý. Tomuto tvrzení se vymyká pouze nelegální stahování. Dále by chtěla autorka upozornit také na to, že toto tvrzení se týká pouze těch druhů kyberkriminality, na které byl dotazník zaměřený.

Domněnka o tom, že kybekriminalita se ve větším množství páchá až v dospělém věku, svým způsobem souvisí s předešlým cílem, a to zjistit rozsah kyberkriminality mládeže. Jak již bylo několikrát ukázáno, dotazovaná mládež páchá kyberkriminalitu jen zřídka. Za rok 2020 bylo spácháno 8 073 skutků v oblasti kyberkriminality. Je tedy možné se domnívat, že kyberkriminalita se opravdu ve větší míře páchá až ve vyšším věku než 14-24 let. Samozřejmě všechna mládež nemusí být tak vzorová a nepáchající kyberkriminalitu, jako tomu tak bylo u respondentů dotazníkového šetření.

V úvodu praktické části byly stanoveny čtyři výzkumné předpoklady. Jednalo se o autorčiny domněnky, které chtěla dokázat pomocí odpovědí z dotazníku. Dva předpoklady byly správné a díky odpovědím se je dokázalo prokázat. Jeden předpoklad byl nesprávný a další se nedokázalo zcela prokázat. Dat bylo zřejmě málo k prokázání tohoto jevu.

Celkově považuje autorka provedený dotazník za úspěšný, i když se některé výzkumné předpoklady neprokázaly. Hlavní cíle se však prokázat dokázalo.

Závěr

Kyberkriminalita je v současné době nejvíce se rozrůstající typ trestné činnosti nejenom na území České republiky. Mládež stále více tráví čas na počítačích/mobilech/tabletech, a to je způsobené nejen dobou „covidovou“. Ve výsledku to bude znamenat, že v budoucnosti poroste i kyberkriminalita mládeže. Cílem této práce bylo shrnout problematiku tématu do jednoho souboru a v praktické části zjistit rozsah kyberkriminality mládeže a potvrdit nebo vyvrátit domněnku, že se kybekriminalita začíná ve větší míře páchat až v pozdějším věku. Všechny tyto cíle považuje autorka za splněné.

V teoretické části byly vysvětleny základní pojmy, fenomenologie, etiologie a kontrola kriminality mládeže a kyberkriminality. Byly podrobně rozebrány druhy kyberkriminality a také nastíněn vývoj kriminality mládeže a kyberkriminality v České republice. Autorka se zamyslela i nad možnými hlavními vlivy vzniku kyberkriminality mládeže.

V praktické části bylo pomocí dotazníkového šetření prokázáno, že dotazovaní respondenti kyberkriminalitu v zásadě moc nepáchají. V souhrnu bylo kladných odpovědí méně jak polovina. Tím pádem, můžeme předpokládat, že domněnka pro začátek páchání kyberkriminality až v pozdějším věku může být správná. Všechny cíle, které byly stanoveny v úvodu, byly splněny.

Bylo by zajímavé dotazník ohledně kyberkriminality mládeže vpravit do všech základních škol, středních odborných učilišť, středních škol a bakalářských studií v České republice. Výsledky by byly jednoznačně komplexnější a lépe vypovídající. Příslušné orgány by měly přehled o velikosti tohoto problému a mohly by začít konat příslušné kroky.

V dnešní době více než v dřívější je nutné, aby rodiče dávali na své děti pozor. Měli by se zajímat, co jejich děti dělají celou dobu online, vysvětlit jim, že tam na ně může čekat nebezpečí a také to, co by na internetu rozhodně dělat neměly. Vysvětlovat a varovat by měli i učitelé ve školách a pro příklad třeba i reklamy v televizi nebo na internetu.

Seznam literatury

Monografie

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

VÁLKOVÁ, Helena, KUCHTA Josef, HULMÁKOVÁ Jana a kol. *Základy kriminologie a trestní politiky*. 3. vydání. V Praze: C.H. Beck, 2019. ISBN 978-80-7400-732-3.

MAREŠOVÁ, Alena. *Kriminalita mládeže v podmínkách současné české společnosti: pro studenty magisterského studijního programu*. Praha: Policejní akademie České republiky v Praze, 2018. ISBN 978-80-7251-483-0

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

Zákonná úprava

Zákon č. 40/2009 Sb., trestní zákoník

Zákon č. 218/2003 Sb., o soudnictví ve věcech mládeže

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Webové stránky a elektronické zdroje

Kyberprostor [online]. [cit. 25.12.2021] Dostupné z: https://www.sprava-site.eu/kyberprostor/

Sociální sítě [online]. [cit. 25.12.2021]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/socialni-media/socialni-site/

What is social networks [online]. [cit. 14.2.2022]. Dostupné z: https://www.investopedia.com/terms/s/social-networking.asp

Kybernetická kriminalita [online]. [cit. 25.12.2021]. Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

What is cybercrime [online]. [cit. 14.2.2022]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/cybercrime

Fenomenologie kriminality mládeže [online]. [cit. 22.2. 2022]. Dostupné z: https://is.ambis.cz/th/ewcdm/Kriminalita_mladeze_a_jeji_prevence_-_David_Novy.pdf

The Convention on Cybercrime [online]. [cit. 10.1.2022]. Dostupné z: https://en.wikipedia.org/wiki/Convention_on_Cybercrime

Co je to phishing [online]. [cit. 7.1. 2022]. Dostupné z: https://www.avast.com/cs-cz/c-phishing#gref https://www.eset.com/cz/phishing/

Co je to ransomware a spyware [online]. [cit. 10.1. 2022]. Dostupné z: https://www.eset.com/cz/ransomware/ https://www.avast.com/cs-cz/c-spyware#gref

What is DoS attack [online]. [cit. 10.1. 2022]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/ https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

Dětská pornografie definice [online]. [cit. 11.1. 2022]. Dostupné z: https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx

Kyberšikana [online]. [cit. 11.1. 2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/

Kyberšikana [online]. [cit. 11.1. 2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/

Kyberšikana [online]. [cit. 11.1. 2022]. Dostupné z: https://www.policie.cz/clanek/vite-co-je-kybersikana.aspx

Kyberstalking [online]. [cit. 12.1. 2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kyberstalking/

Kybergrooming [online]. [cit. 12.1. 2022]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybergrooming/

Krádež identity [online]. [cit. 12.1. 2022]. Dostupné z: https://www.eset.com/cz/kradez-identity/

Why young people commit cybercrime [online]. [cit. 20.1. 2022]. Dostupné z: https://www.beaming.co.uk/insights/young-people-get-cybercrime/ http://www.xinhuanet.com/english/2020-01/22/c_138725790.htm

Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území České republiky 2020 [online]. [cit. 24.1. 2022]. Dostupné z: https://www.mvcr.cz/clanek/statistiky-kriminality-dokumenty.aspx

Fenomenologie kyberkriminality [online]. [cit. 14.2.2022]. Dostupné z: http://www.ok.cz/iksp/docs/463.pdf

Kontrola kriminality [online]. [cit. 27.1. 2022]. Dostupné z: https://www.fsps.muni.cz/inovace-SEBS-ASEBS/elearning/kriminologie/kontrola

Struktura prevence kriminality [online]. [cit. 8.2. 2022]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/

Prevence kriminality [online]. [cit. 9.2. 2022]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/

Prevence kriminality [online]. [cit. 8.2. 2022]. Dostupné z: https://www.mvcr.cz/clanek/web-o-nas-prevence-prevence-kriminality.aspx?q=Y2hudW09NA%3d%3d

Prevence kriminality mládeže [online]. [cit. 15.2. 2022]. Dostupné z: https://is.ambis.cz/th/x9pl6/Benesova_Hana_BP_2017.pdf

Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 22.2. 2022]. Dostupné z: https://www.nukib.cz/cs/o-nukib/ https://www.nukib.cz/cs/kyberneticka-bezpecnost/cviceni/

Národní úřad pro kybernetickou a informační bezpečnost [online]. [cit. 22.2. 2022]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/

Prevention of juvenile cybercrime [online]. [cit. 25.1. 2022]. Dostupné z: https://www.getsafeonline.org/personal/blog-item/cybercrime-preventing-young-people-from-getting-involved/

Prevence kyberkriminality mládeže [online]. [cit. 25.1. 2022]. Dostupné z: https://prevencekriminality.cz/prevence-kriminality/kyberkriminalita/rozcestnik-kyberkriminality/

Bezpečně online [online]. [cit. 24.2. 2022]. Dostupné z: https://bezpecne-online.ncbi.cz/uvod/o-projektu

Mladí proti nenávisti online [online]. [cit. 24.2. 2022]. Dostupné z: https://www.ncbi.cz/projekty/ukoncene-projekty/mladi-proti-nenavisti-online.html

CZ.NIC akademie [online]. [cit. 24.2. 2022]. Dostupné z: https://akademie.nic.cz

Bílý kruh bezpečí [online]. [cit. 24.2. 2022]. Dostupné z: https://www.bkb.cz/o-nas/poslani-a-cinnost/

Linka bezpečí [online]. [cit. 24.2. 2022]. Dostupné z: https://spolek.linkabezpeci.cz/o-nas/

Prevention of juvenile cybercrime [online]. [cit. 25.1. 2022]. Dostupné z: https://www.paladincapgroup.com/wp-content/uploads/2016/11/Pathways-White-Paper-US-final-1.pdf

Seznam obrázků

Seznam grafů a tabulek

Seznam příloh

Příloha č. 1

Dobrý den,

věnujte prosím několik minut svého času vyplnění následujícího dotazníku. Respektuje, prosím, že dotazník je určený pouze pro osoby ve věku 12-24 let. Dotazník je ANONYMNÍ. Vyplňujte ho, prosím, pravdivě. Veškeré získané informace budou využity jednorázově pouze jako materiál pro diplomovou práci. Děkuji!

1. Jaké je vaše pohlaví: (vyberte jednu odpověď)
    - muž
    - žena
2. Jaký je váš věk: (vyberte jednu odpověď)
    - 12–14 let
    - 15–19 let
    - 20–24 let
3. V jak velkém městě (vesnici) žijete: (vyberte jednu odpověď)
    - Méně než 1 000 obyvatel
    - 1 000 – 5 000 obyvatel
    - 5 000 – 25 000 obyvatel
    - 25 000 – 50 000 obyvatel
    - více jak 50 000 obyvatel
4. Jakou školu studujete: (vyberte jednu odpověď)
    - základní školu
    - střední odborné učiliště
    - střední školu
    - vysokou školu
    - jiné (pokud již nestudujete, uveďte zde své nejvyšší dosažené vzdělaní): _____
5. Používáte sociální sítě: (vyberte jednu odpověď)
    - ano
    - ne

6. Jaké sociální sítě používáte: (vyberte jednu nebo více odpovědí)
    - Facebook
    - Facebook Messenger
    - Instagram
    - Whatsapp
    - Tik Tok
    - Snapchat
    - Youtube
    - Twitter
    - nepoužívám žádné
    - Jiné: _____
7. Kolik hodin denně trávíte na počítači/mobilu/tabletu: (vyberte jednu odpověď)
    - 1–2 hodiny
    - 2–4 hodiny
    - 4–6 hodin
    - 6–8 hodin
    - 8 a více hodin
8. Víte, co je phishing a pharming: (vyberte jednu odpověď)
    - ano
    - ne
9. Pokud ano, uměli byste ho vytvořit: (vyberte jednu odpověď)
    - ano
    - ne
    - na předchozí otázku jsem odpověděl/a záporně
10. Pokud ano, používáte ho ve svůj prospěch pravidelně: (vyberte jednu odpověď)
    - ano
    - jen občas
    - ne
    - na předchozí otázku jsem odpověděl/a záporně

11. Znáte někoho, kdo to dělá: (vyberte jednu odpověď)
    - ano
    - ne
12. Víte, co je počítačový vir: (vyberte jednu odpověď)
    - ano
    - ne
13. Pokud ano, umíte ho vytvořit: (vyberte jednu odpověď)
    - ano
    - ne
    - na předchozí otázku jsem odpověděl/a záporně
14. Pokud ano, požíváte ho ve svůj prospěch pravidelně: (vyberte jednu odpověď)
    - ano
    - jen občas
    - ne
    - na předchozí otázku jsem odpověděl/a záporně
15. Znáte někoho, kdo to dělá: (vyberte jednu odpověď)
    - ano
    - ne
16. Víte, co je to krádež identity: (vyberte jednu odpověď)
    - ano
    - ne
17. Dokázal/a byste někomu ukrást identitu za pomoci počítače/mobilu/tabletu: (vyberte jednu odpověď)
    - ano
    - ne
    - na předchozí otázku jsem odpověděl/a záporně
18. Už jste to někdy udělal/a: (vyberte jednu odpověď)
    - ano
    - ne
    - na předchozí otázku jsem odpověděl/a záporně

19. Znáte někoho, kdo to udělal: (vyberte jednu odpověď)
    - ano
    - ne
20. Stáhli jste někdy z neoficiálních internetových stránek muziku nebo film: (vyberte jednu odpověď)
    - ano
    - ne
21. Pokud ano, kolikrát měsíčně se tak děje: (vyberte jednu odpověď)
    - 1x
    - 2x
    - 3x
    - 4x
    - 5x
    - 5x a více
    - nestahuji
22. Znáte někoho, kdo pravidelně stahuje muziku nebo filmy z neoficiálních internetových stránek: (vyberte jednu odpověď)
    - ano
    - ne
23. Požadovali jste po někom někdy nahé fotografie za pomoci využití počítače/mobilu/tabletu: (vyberte jednu odpověď)
    - ano
    - ne
24. Vydírali jste později těmito fotografiemi dotyčného: (vyberte jednu odpověď)
    - ano
    - ne
    - na předchozí otázku jsem odpověděl/a záporně
25. Znáte někoho, kdo by odpověděl kladně na otázku číslo 23: (vyberte jednu odpověď)
    - ano
    - ne

26. Znáte někoho, kdo by odpověděl kladně na otázku číslo 24: (vyberte jednu odpověď)
    - ano
    - ne
27. Šikanujete někoho opakovaně prostřednictvím počítače/mobilu/tabletu: (vyberte jednu odpověď)
    - ano
    - ne
    - v minulosti ano
28. Využíváte k tomu svůj vlastní nebo falešný profil na sociálních sítích/e-mailu/seznamce: (vyberte jednu odpověď)
    - vlastní
    - falešný
    - na předchozí otázku jsem odpověděl/a záporně
29. Znáte někoho, kdo šikanuje prostřednictvím počítače/mobilu/tabletu: (vyberte jednu odpověď)
    - ano
    - ne
30. Kontrolují vám rodiče, co děláte na počítači/mobilu/tabletu: (vyberte jednu odpověď)
    - ano
    - dříve ano, teď vzhledem k věku už ne
    - ne
31. Pokud ano jakým způsobem: (napište jedno nebo více slov)

    _____