© Wydawnictwo UR 2016 „Edukacja – Technika – Informatyka" nr 1/15/2016
ISSN 2080-9069 www.eti.rzeszow.pl
ISSN 2450-9221 online DOI: 10.15584/eti.2016.1.18

PETER LOŠONCZI[1], **MARIÁN MESÁROŠ**[2]

Východiská pre bezpečnosť detí v prostredí internetu

Background for child safety in the Internet environment

[1] Ing., PhD. MBA, Vysoká škola bezpečnostného manažérstva v Košiciach, Ústav občianskej bezpečnosti, Katedra kybernetickej bezpečnosti, Slovenska republika
[2] Dr.h.c. prof. Ing., DrSc. MBA, Vysoká škola bezpečnostného manažérstva v Košiciach, Ústav občianskej bezpečnosti, Katedra práva a prevencie criminality, Slovenska republika

Abstrakt

Štúdia pojednáva o teoretických, legislatívnych a sociologických východiskách pre riešenie problematiky ochrany detí v prostredí internetu. Nástroje štátu a EÚ sú základným východiskom pre riešenie tejto problematiky, ktorá prerastá hranice štátov a regiónov. Vhodná štandardizácia tohto prostredia je nevyhnutnosťou pre ochranu detí a boja proti kriminalite na nich páchanej.

Kľúčové slová: internet, deti, informačná bezpečnosť, kriminalita, prevencia.

Abstract

The study discusses the theoretical, legislative and sociological approaches for addressing the issue of child protection in the Internet environment. The tools of the State and the EU are an essential starting point for the solution of this problem, which goes beyond the borders of the States and regions. Appropriate standardisation of this environment is a necessity for the protection of children and the fight against crime committed against them.

Key words: Internet, children, information security, crime, prevention.

Úvod do informačnej bezpečnosti

Informačná bezpečnosť je celosvetový problém.Ľahký prístup k internetu spôsobuje, že sa deti dostávajú k informáciám a tie ich môžu negatívne ovplyvniť. Zväčšuje sa narušovaniesúkromia, zneužívanie identity, duševného vlastníctva a javy, ktoré súvisia so svetom informačných technológií. Na negatívny vplyv médií upozorňujú rodičia a učitelia, psychológovia a odborníci na informačné technológie. Problematika informačnej bezpečnosti je veľmi obsiahla a zahŕňa technologickú bezpečnosť, ochranu osobných, firemných a štátnych informácií a možné negatívne dopady na populáciu. Európske hospodárske spoločenstvo podporuje iniciatívu Európskej komisie *Bezpečný*

internet a siete INSAFE a INHOPE na podporu bezpečného používania internetu deťmi. Vznikajú nové pravidlá smerujúce k zvyšovaniuinformačnej bezpečnosti. V roku 2009 boli vypracované *Bezpečnejšie zásady využívania sociálnych sietí v EÚ a* v roku 2010 súpis usmernení vzťahujúcich sa na výrobu a poskytovanie on-line obsahu pre deti a mladých ľudí. V roku 2011 vstúpila do platnosti smernica o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii, ktorá kriminalizuje zločiny ako je detská pornografia, *grooming*detí (nadviazanie priateľstva s deťmi za účelom ich sexuálneho zneužitia), sexuálne zneužívanie prostredníctvom webovej kamery, alebo pozeranie detskej pornografie na internete. Na problematiku reagujú v niektorých krajinách vytvorením tiesňových liniek, poskytovaním bezplatného softvéru na rodičovskú kontrolu, vytváraním mechanizmov na oznamovanie škodlivého a nezákonného obsahu. Európska komisia zaradila boj proti počítačovej kriminalite za prioritu v rámci stratégie vnútornej bezpečnosti a za dôležitú sa považuje prevencia.

Deti používajú internet už pred začiatkom školskej dochádzky a sú v tomto virtuálnom svete zraniteľné. Preto je potrebné ich chrániť. Vplyv na bezpečnosť detí nie je možné vopred predvídať, kvôli rozvíjajúcim sa možnostiam internetu. Základom stratégie sú štyri piliere, ktoré sa navzájom dopĺňajú [Bobot, Jakubeková 2013]:

1. Podpora kvality on-line obsahu pre mladých ľudí.
2. Zvyšovanie informovanosti a zlepšovanie možností.
3. Vytváranie bezpečného on-line prostredia pre deti.
4. Boj proti pohlavnému zneužívaniu a sexuálnemu vykorisťovaniu detí.

Potrebné je deti nielen chrániť ale aj posilniť digitálnu gramotnosť detí a ich rodičov, aby sa mohli sami chrániť. Školy sa musia zamerať na zvyšovanie gramotnosti detí v oblasti informačného prostredia, na rozvoj sociálnych schopností a povedomia. V súčasnosti sa Európsky parlament zaoberá nariadením na ochranu osobných údajov a smernicou na ochranu údajov na účely súdneho vyšetrovania. Európska komisia zavádza pravidlá pre lepšiu kontrolu nad používaním osobných údajov. Dôležitou novinkou je „právo byť zabudnutý“. To umožňuje občanom žiadať o odstránenie svojich osobných údajov z rôznych databáz, ktoré nie sú na to oprávnené. Dôraz sa kladiena potrebu súhlasu na využívanie a prenos osobných údajov a na pokuty a sankcie za porušenie práv na ochranu súkromia. Slovensko sa zapája domedzinárodných aktivít, ako je napríklad deň bezpečnejšieho internetu, ktorý začiatkom februára od roku 2004 organizuje európska organizácia INSAFE vo viac ako 65 krajinách sveta [Bobot, Jakubeková 2013].

V Slovenskej republike sa na základe Stratégie pre informačnú bezpečnosť z roku 2008 a akčného plánu mapujú možnosti školského a iného vzdelávania. Pre jednotlivých používateľov informačných a komunikačných technológií sa vytvoria v oblasti informačnej bezpečnosti štandardy znalostí. Informačná

bezpečnosť bude súčasťou všetkých predmetov nielen predmetu informatika. Bude sa podporovať publikovanie odbornej literatúry a metodických dokumentov zameraných na riešenie informačnej bezpečnosti. Na základe strategických materiálov Slovenskej republiky a Európskej únie je stratégia vypracovaná na obdobie piatich rokov. V praxi sa jej uplatnenie žiada aj v oblasti vzdelávania v regionálnom školstve [Národná stratégia 2008]. Hoci sa začlenenie mediálnej gramotnosti do školského vzdelávania na základnom stupni hodnotí pozitívne, naliehavou výzvou je aj zapojenie všetkých pedagogických pracovníkov, mládeže a rodičov, a nevyhnutný je takisto aj proces harmonizácie medzi školami [Kováčová, Klimo 2013].

Charakteristika informačnej bezpečnosti

Súčasná doba Internetu, počítačov a iných informačných technológií prinieslaokrem svojich nesporných výhod aj množstvo hrozieb, ktoré ohrozujú deti a dáta nakaždom kroku virtuálneho internetového sveta. Preto je nutné a potrebné urobiťopatrenia, ktoré minimalizujú pôsobenie týchto hrozieb. Dôležitým sa stáva budovanie informačnej bezpečnosti a bezpečnostného povedomia celej spoločnosti.

Informačná bezpečnosť je podľa medzinárodného štandardu ISO/IEC 270011, ochrana informácie pred množstvom hrozieb. *Informácia je* obsahom údajov avyskytuje sa v rozličných formách: písomnej, ústnej, obrazovej, elektronickej. Na jejspracovávanie sa používajú rozličné prostriedky. Ohrozenie informácie je problém, ktorý treba rýchle a účinne riešiť. Ochrana informácie vychádza z toho, na aký účel sainformácia používa a čo ju a akým spôsobom ohrozuje. Základné bezpečnostnépožiadavky na ochranu informácie *sú dostupnosť, dôvernosť, autentickosť aintegrita*. *Dostupnosť* informácie znamená, že informácia je k dispozícii oprávnenýmosobám vždy, keď ju potrebujú. *Dôvernosť* informácie znamená, že sa informácianedostane do rúk neoprávneným osobám. Integrita údajov vylučuje možnosť zmenyúdajov. *Autentickosť* informácie znamená zaistenie integrity a zároveň pôvodudokumentu [Národná stratégia 2008].

Informačný systém sa skladá z prvkov, akými sú dáta, hardvér, softvér, ľudskézdroje alebo stavebné priestory. Proces, ktorým sa rozumie ochrana informačných systémov je navrhovanie, schvaľovanie a implementácia softvérových, hardvérových, technických a sociálno-personálnych ochranných opatrení, spojených s minimalizácioustrát, vzniknutých v dôsledku poškodenia, zničenia alebo zneužitia týchto systémov. *„Stav, ktorý je snaha dosiahnuť pomocou tohto komplexu opatrení, sa nazývainformačná bezpečnosť (INFOSEC), bezpečnosť informačných a komunikačnýchtechnológií (IT/CT), bezpečnosť informačných systémov (BIS)“* [Loveček 2007].

Informačná bezpečnosť nezáleží len od hardvéru a softvéru, ale aj od ľudí a ich riadení. Najväčšou hrozbou informačného systému je jeho užívateľ.

Informačný systém sa neustále vyvíja a jeho bezpečnosť je dynamická záležitosť, pretoje potrebné ochranné opatrenia neustále prispôsobovať. Tak ako v každej bezpečnosti, neexistuje 100% pokrytie všetkých hrozieb. V očiach užívateľov, bezpečnosťv mnohých prípadoch predstavuje nadbytočnosť a skomplikovanie práce.

Internetová kriminalita páchaná na deťoch

Internetová kriminalita zahrňuje takú trestnú činnosť, kde sieťové pripojenie môže byť nástrojom, cieľom alebo miestom páchania trestného činu. Internetová trestná činnosť zahrňuje široké spektrum aktivít, ktoré môžu viesť ku krádežiam, podvodom, vydieraniam, sexuálnym deliktom a iným činom [Krauz 2011]. Do internetovej kriminality páchanej na deťoch môžeme zaradiť kyberšikanu, kybergrooming aonlinedetskú pornografiu.

1) *Kyberšikana* je špecifický druh šikanovania, ktorý využíva internet, mobilné telefóny a ďalšie nástroje moderných komunikačných technológií za účelom ublíženiu alebo zosmiešneniu inej osoby. Môže mať rôznu podobu. Agresor môže obeti zasielať výhražné, kruté e-maily a SMS správy, obeť môže dostávať výhražné telefonáty alebo môže byť obťažovaná cez chat. Agresor môže vytvárať webové stránky, kde môže obeť urážať a zosmiešňovať. Patrí sem aj rozosielanie obrázkov, fotografií, videonahrávok ľuďom z okolia obete, kde je obeť zosmiešňovaná, alebo tiež vyvesenie pornografických fotografií s tvárou obete. Existujú prípady, kedy agresor získal hesláa identifikačné údaje obete a pod jej menom zasielal ostatým na internete vulgárne a obťažujúce správy, fotografie a videa.
2) *Kybergrooming* označuje chovanie užívateľa internetu, ktorý má v dieťati vyvolať falošnú dôveru, pripraviť ho na schôdzku a obeť pohlavne zneužiť. Deje sa to cez verejný chat, zoznamky, ICQ a emaily. Grooming označuje v širšom slova zmysle manipulatívne chovanie. Agresor je trpezlivý, hovorí o význame lásky, do konverzácie vkladá témy sexuálnej povahy, žiada po obeti intímne fotografie a kybersex prostredníctvom webkamery. Páchatelia týchto trestných činov sú dospelí ale aj mladiství a ich počet stále rastie. Mnohokrát nemajú žiadne záznamy o trestných činoch.
3) *Detská pornografia* dávno pred vznikom a vývojom počítačov a internetu, ale dnes sa stáva hlavným médiom jej šírenia. Internet slúži k výrobe, skladovaniu, prezeraniu detskej pornografie, ale tiež ako komunikáciamedzi páchateľom a obeťou. Detská pornografia je vizuálne zobrazenie sexuálneho chovania detí a mladistvých do 18 rokov. Patrí sem aj sexting (zasielanie fotografií, videí so sexuálnym obsahom, ktorý urobili partneri a začalo sa šíriť internetom). Neexistuje jeden typ páchateľa a užívateľa internetu so záujmom o detskú pornografiu a zároveň je to ťažké poznať. Užívatelia pochádzajú z rôznych socioekonomických vrstiev a prostredí [Hulanová 2013].

Policajný zbor Slovenskej republiky vykazuje štatistiku páchanú na deťoch, poškodené osoby do 18 rokov vrátane. V nej nevykazuje kriminalitu na deťoch páchanú pomocou internetu. Podľa štatistiky kriminalita páchaná na deťoch v Slovenskej republike klesá. Prevažuje násilná a mravnostná kriminalita. Z násilnej kriminality prevažuje úmyselné ublíženie na zdraví a vydieranie. Z mravnostnej kriminality prevažuje sexuálne zneužívanie ostatných osôb. Z krádeží prevažujú vreckové krádeže [PZ SR 2014].

Opatrenia zamerané na bezpečnosť detí na internete

Podľa Stratégie prevencie kriminality a inej protispoločenskej činnosti v Slovenskej republike na roky 2012–2015, *„prevencia kriminality a inej protispoločenskej činnosti predstavuje cieľavedomé pôsobenie štátu, vládnych organizácií, cirkví, občianskych združení, podnikateľských subjektov a vzdelávacích inštitúcií pri zvyšovaní povedomia obyvateľstva, ktoré má prispieť k tomu, aby sa obyvatelia nestali páchateľmi alebo obeťami trestných a iných protispoločenských činov"* [Stratégia prevencie 2012].

Stratégia predstavuje východisko pre preventívne programy a projekty na národnej, regionálnej a miestnej úrovni. Úlohy prevencie kriminality majú byť začlenené do všetkých príslušných politík a programov. Zvláštna pozornosť sa má venovať pozitívnemu ovplyvňovaniu najmä detí a mládeže a ako obete kriminality si vyžadujú cielenú ochranu. V oblasti viktimačnej prevencie kriminality sa odporúča realizovať aktivityzamerané na: propagáciu aktivít prostredníctvom médií, miestnych informačných prostriedkov, letákov, realizáciu programov bezpečného správania sa rizikových skupín, zverejňovanie kriminogénnych situácií s návrhmi na ich predchádzanie, zriaďovanie a prevádzku telefonických liniek, realizácii psychologického, právneho a sociálneho poradenstva pre obete trestnej činnosti, výcviky osôb, ktoré dochádzajú profesijne do kontaktu s obeťami trestnej činnosti; poskytovanie krízových konzultácií a poradenstva [Stratégia prevencie 2012].

Podľa Pedagogicko-organizačných pokynov MŠ SR v zmysle úloh vyplývajúcich zo Stratégie prevencie kriminality pre rezort školstva saodporúča realizovať projekty a aktivity prevencie a eliminácie rizikového správania, delikvencie a kriminality, záškoláctva, šikanovania, bezpečného používania internetu, ako aj na podporu právneho vedomia detí a žiakov [Pedagogické pokyny 2013]. Z Akčného plánu rozvoja s mládežou košického samosprávneho kraja na roky 2012–2014 vyplýva organizovanie aktivít zameraných na predchádzanie kriminalitypáchanej mládežou a na mládeži, alebo na ich eliminovanie a realizovanie besedy sožiakmi stredných škôl o prevencii rizikového správania. Spolupracovať so zástupcamipolicajného zboru SR a s Mestskou políciou Košice. Na stredných školách v rámcitriednických hodín, na rodičovských združeniach a predmetoch, kde sa využíva internet, spolupracovať s regionálnou

televíziou na diskusii na tému „etika na internete“ apodporiť tak bezpečné využívanie internetu [Akčný plán 2012].

Stábová [2007] uvádza, že využívanie internetu znamená okrem výhod ajriziká hlavne pre deti a mládež. To neznamená, že treba obmedziť používanie internetu, ale treba zvýšiť počítačové kompetencie rodičov aj detí. Nie je to len záležitosť vlády, musí sa zapojiť celá spoločnosť, polícia, justícia, rodičia, školy aposkytovatelia služieb internetu. Dôležitá je výmena skúseností medzi odborníkmi z oblasti medicíny, psychológie, sociológie, kriminológie, polície a justície. Taktiež medzi jednotlivými krajinami, keďže ide o médium s cezhraničnou pôsobnosťou. Veľmi dôležitý voblastiprevencie je výskum v oblasti nebezpečenstva internetu.

V roku 2011 bola do nášho systému výchovy a vzdelávania v štátnom vzdelávacom programe zavedená prierezová téma: „Mediálna výchova“. Cieľom prierezovej tematiky je, aby žiaci: lepšie porozumeli pravidlám fungovania mediálnehosveta a primerane veku sa v ňom orientovali, dokázali posudzovať mediálne šírené posolstvá, objavovať v nich to hodnotné, pozitívne formujúce ich osobnostný aprofesionálny rast, dokázali si uvedomiť negatívne mediálne vplyvy na svoju osobnosťa snažiť sa ich zodpovedným prístupom eliminovať a vedeli tvoriť mediálne produkty [Mediálna výchova 2011].

Preventívne aktivity zamerané na bezpečnosť detí na Internete

Policajný zbor SR realizuje projekt „Správaj sa normálne“, ktorého cieľom je budovanie dôvery medzi políciou, školou, dieťaťom, rodinou a verejnosťou. Veľmi aktuálnou je téma „Bezpečne vo virtuálnom svete!“, ktorá má deťom vysvetliť význam dodržiavania zásad bezpečného používania a správania sa na internete [PZ SR 2014]. V rámci prevencie kriminality Policajný zbor SR v časti Preventívne rady pre občanov na stránke MV SR, upozorňuje na riziká s používaním internetu a komunikáciou na sociálnych sieťach. V roku 2012 KR PZ v Košiciach zorganizovalo okrem iných projektov projekt „Zodpovedne.sk“, cieľom bolo upozorniť na riziká spojené s používaním internetu a výchova k zodpovednému správaniu sa na internete a zvýšenie právneho vedomia detí a „Kyberšikana- hrozba virtuálneho priestoru“, cieľom ktorého bolo vysvetliť pojem kyberšikana a poukázať na riziká vo virtuálnom priestore a počítačová kriminalita [Projekty 2012].

Počítačovej prevencii sa venuje aj mestská polícia. Mestská polícia Nitra už niekoľko rokov na základných školách realizuje projekt: „Stop počítačovej kriminalite“. Cieľovou skupinou projektu sú žiaci V. až VII. ročníka vybraných základných škôl v meste Nitra vo veku 10–13 rokov, ohrozených anonymným virtuálnym priestorom – možným zdrojom nevhodnej zábavy a porušovania zákona na úrovni počítačovej kriminality. Problematikou a základnými informáciami o počítačovej kriminalite boli oboznámení aj rodičia, pedagogickí

pracovníci a verejnosť, prostredníctvom rozdistribuovaných edukačných letákov, plagátu a vytvorených edukačných panelov [MsP Nitra 2014].

Mestská polícia v Košiciach sa tiež venuje kriminálnej prevencii na základných školách a to besedami s použitím prezentácie „Kriminálna prevencia pre deti a mládež“, v ktorej je časť venovaná bezpečnému využívaniu internetu. Metodicko-pedagogické centrum realizuje v rámci kontinuálneho vzdelávania učiteľov vzdelávanie na tému: „Informačná bezpečnosť v škole“ a vydalo aj publikáciu s rovnakým názvom. Žiaci stredných škôl v spolupráci s nadáciami už sami realizujú rôzne projekty zamerané na bezpečnosť na internete. Napríklad žiaci SOŠ automobilovej v Košiciach, II. F trieda v školskom roku 2012/2013 bola realizátorom projektu: „Realizovať školenie o bezpečnosti na internete pre rodinných príslušníkov“. V rámci projektu Zodpovedne.sk bola vydaná publikácia „Deti v sieti“. Projekt je zameraný na bezpečné a zodpovedné používanie internetu, mobilných telefónov a iných nových technológií. Je podporovaný Európskou úniou v rámci komunitárneho programu Safer Internet plus. Zameriava sa na šírenie osvety o bezpečnom používaní internetu a mobilov, o rizikách virtuálneho priestoru a možnostiach získania poradenstva a pomoci. Mnoho podnetných a užitočných informácií je možné nájsť na portáloch, ktoré sú vytvorené na tento účel[1], alebo v rôznych médiách, ktoré sa problematike sporadicky na rôznej odbornej úrovni venujú.

Záver

Deti si neuvedomujú, akou emocionálnou silou na nich médiá vplývajú, preto je nutné zamerať sa na šírenie osvety o bezpečnom používaní internetu a mobilov, o rizikách virtuálneho priestoru a možnostiach získania poradenstva a pomoci. Dôležitá je prevencia, aby sa deti nestali obeťou, alebo páchateľom trestných činov. Deti je potrebné nielen chrániť, ale aj posilniť ich digitálnu gramotnosť. Týka sa to aj ich rodičov, školy a celej spoločnosti.

Poďakovanie

Táto štúdia bola spracovaná v rámci riešenia inštitucionálneho projektu VŠBM v Košiciach IP/42/ VŠBM/2014: Informačná bezpečnosť občana.

Literatúra

Akčný plán (2012), *Akčný plán rozvoja práce s mládežou Košického samosprávnehokraja na roky 2012–2014*., Úrad KSK, http://www.gymmoldava.sk/dokumenty/20122013/akcny_plan_rozvoja_prace_s_mladezou.pdf.

[1] www.zodpovedne.sk, www.bezpecnenainternete.sk, www.bezpecnesvedkom, webnode.sk/rady-pre-rodicov, www.bezpecnyinternet.sk, www.bezpecnynakup.sk, www.itpravo.sk, www.pomoc.sk, http://internet.rodinka.sk/oprojekte.html, http:// pomoc online.cz/, www.bezpecneonline.cz, www.stop-line.sk, www.ovce.sk, www.kry-sa.sk a veľa ďalších portálov.

Bobot V., Jakubeková M. (2013), *Informačná bezpečnosť v škole*, Bratislava, http://www.mpc-edu.sk/library/files/publik_ciainfbezp_web.pdf.

Kováčová L., Klimo V. (2013), *Fundamentals ofsecurityeducation in theprocessofglobalization*, „Odes´kyiPolitechnichnyiUniversytet PRATSI", iss. 2 (41).

Krauz A. (2011), *Niewolnictwo dzieci na e-globie w XXI wieku zamiast edukacji*, [w:] M. Duris, *Technicke vzdelavanie ako sucast vseobecneho vzdelavania*, 27 medzinarodna vedecko-odborna konferencia, Banska Bystricia.

Legislatíva (2011). *Legislatíva pre zriaďovanie škôl a školských zariadení*, Školský portál, http://www.skolskyportal.sk/clanky/legislativa-pre-zriadovanie-skol-skolskych-zariadeni.

Loveček T. (2007), *Bezpečnosť informačných systémov*, Žilina.

MsP Nitra (2014), *Stop počítačovej kriminalite*, http://www.mspnitra.sk/stranky/prevencia/podporeneprojekty/stop-pocitacovej-kriminalite.php.

Národná stratégia (2008), *Národná stratégia pre informačnú bezpečnosť v SR*, Bratislava, http://www.informatizacia.sk/narodna-strategia-pre-ib/6783s.

Návrh zabezpečenia (2009), *Návrh zabezpečenia CSIRT.SK*, Bratislava, http://www.informatizacia.sk/informacna bezpecnost/2999s.

Pedagogické pokyny (2013), *Pedagogicko-organizačné pokyny na školský rok 2013/2014*, Bratislava, http://www.minedu.sk/data/att/4966.pdf.

Projekty (2012), *Projekty KR PZ v Košiciach v roku 2012*, http://www.minv.sk/?rok_2012.

Stábová D. (2007), *Počítačová kriminalita a nebezpečenstvo internetu pre deti a mládež*, „Sociálna prevencia – Prevencia kriminality" no. 1, http://www.infodrogy.sk/drogyUserFiles/File/IVB_Kmiminalita_1_2007_zelene.pdf.

Stratégia prevencie (2012), *Stratégia prevencie kriminality a inej protispoločenskejčinnosti v Slovenskej republike na roky 2012–2015*, https://lt.justice.gov.sk/Attachment/vlastnymat.rtf?instEID=1&attEID=41082&docEID=217608&matEID=4630&langEID=1&tStamp=20111108083408430.

Zámer zákona (2010), *Zámer zákona o informačnej bezpečnosti*, Bratislava, http://www.informatizacia.sk/informacna-bezpecnost/2999s.