POČÍTAČOVÁ KRIMINALITA

Katarína Kampová[1], Lenka Siváková[2], Miroslav Brvnišťan[3], Tomáš Loveček[2], Andrej Veľas[1]

ABSTRAKT
Vývoj informačných, komunikačných technológií a súčasne celosvetovo rozšíreného internetu ako komunikačného a mediálneho priestoru je bezpochyby jednou z najdynamickejších oblastí globálnej spoločnosti. Táto rýchlo rozvíjajúca sa oblasť so sebou prináša okrem veľkého množstva pozitív i mnoho negatív. Ako hlavné negatíva je možné označiť vznik nových druhov trestnej činnosti a taktiež postupný presun súčasných druhov trestnej činnosti z oblasti reálneho (fyzického) sveta do sveta virtuálneho, resp. kyberpriestoru. Cieľom tohto článku je poukázať na fenomén „počítačovej kriminality“, na úskalia, ktoré kyberprietor v súčasnosti prináša a taktiež poukázať na súčasný prístup k riešeniu tejto problematiky v rámci SR.

Kľúčové slová:
Kybernetická bezpečnosť, počítačová kriminalita, kybernetický zločin, SR právne predpisy

ABSTRACT
The current developments in the field of the Information Technology and as well as the widespread Internet as a communication and media space are undoubtedly one of the most dynamic areas of global society. This rapidly evolving area brings a lot of positives as well as many negatives. As a major negative, the emergence of new types of crime, as well as the gradual transfer of current types of crime from the real (physical) world

[1] Katedra bezpečnostného manažmentu, Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline, Univerzitná 8215/1, 01026 Žilina, Katarina.Kampova@fbi.uniza.sk, Andrej.Velas@fbi.uniza.sk +421 41 513 6668.

[2] Pracovisko výskumu bezpečnosti, Fakulta bezpečnostného inžinierstva, Žilinská univerzita v Žiline, Univerzitná 8215/1, 01026 Žilina, Lenka.Sivakova@fbi.uniza.sk, Tomas.lovecek@fbi.uniza.sk +421 41 513 6864.

[3] JUDr. Miroslav Brvnišťan, PhD, Katedra krízového manažmentu a verejnej správy, Akadémia PZ Bratislava, Sklabinská 1, 835 17 Bratislava, brvnistan@bmsec.sk.

into the virtual world, cyberspace. The aim of this article is to point out the phenomenon of "cybercrime", the difficulties that the cyberspace is presenting and also address the current approach to solving this problem within the Slovak Republic.

Key words:
Cyber security, computer security, cybercrime, SR legislation

1. AKTUÁLNOSŤ PROBLEMATIKY POČÍTAČOVEJ KRIMINALITY

ARPANET ako základ kyberpriestoru vznikol v roku 1968 a to prepojením štyroch univerzitných počítačov. Následne došlo k masívnemu rozšíreniu tohto virtuálneho priestoru a to v súvislosti s príchodom internetu. Najnovší prieskum Eurostatu ukázal, že iba 14 percent Európanov ešte nikdy nepoužilo internet. Na Slovensku je to 15 percent. Najviac, tretina obyvateľov, doteraz nepoužila internet v Bulharsku [1]. Pôvodne nebol internet určený pre takéto masívne využívanie a i preto nebol na úplnom počiatku jeho existencie kladený dôraz na bezpečnostné prvky, ktorý by obmedzovali či zabraňovali zneužívaniu internetu k páchaniu trestného činu. Môžeme konštatovať, že v dnešnej dobe je kyberpriestor omnoho viac využívaný ako v minulosti a životy jednotlivcov, ale i skupín v spoločnosti sa stále viac odohrávajú v tomto virtuálnom priestore. V tejto dobe si zrejme málo kto vie predstaviť, akým smerom a akou rýchlosťou sa tento virtuálny svet bude vyvíjať a rozširovať.

Bezpečnosť a ochrana jednotlivca, skupín ale aj celej spoločnosti pred kriminalitou súvisiacou s využívaním moderných informačných a komunikačných systémov a technológií sa stáva nie len pre SR, EU ale aj ostatné štátu sveta čoraz väčšiu výzvu. Tento výrok je možné potvrdiť i výsledkami nedávnych prieskumov, z ktorých vyplýva, že digitálne hrozby sa vyvíjajú rýchlo a že verejnosť vníma počítačovú kriminalitu ako významnú hrozbu. Ransomwarové útoky od roku 2015 narástli o 300 % a hospodársky vplyv počítačovej kriminality sa medzi rokmi 2013 a 2017 zvýšil päťnásobne. Do roku 2019 by sa podľa štúdií mohli ešte štvornásobiť. Až 87 % respondentov považuje počítačovú kriminalitu za dôležitú výzvu pre vnútornú bezpečnosť EÚ [2]. Zraniteľnosti, ktoré vyplývajú z tohto otvoreného virtuálneho sveta, ktorý prepája jednotlivé krajiny medzi sebou, bez jednoznačných obmedzení vytvárajú predpoklad na pôsobenie rôznych hrozieb. Vzhľadom na charakter týchto hrozieb v mnohých prípadoch nie je možné uplatnenie trestnoprávnych noriem danej krajiny, pretože ich pôsobnosť je obmedzená, dochádza k prekrývaniu jurisdikcie jednotlivých štátov.

2. POČÍTAČOVÁ KRIMINALITA

Počítačová kriminalita je v súčasnosti najrýchlejšie sa rozvíjajúca forma kriminality. V celosvetovom meradle je počet obetí počítačovej kriminality viac ako milión ľudí denne. Ide o výnosnejší druh kriminality ako celosvetový obchod s marihuanou, kokaínom a heroínom dohromady [3]. Je mimoriadne široká, zahŕňa napríklad hacking, cracking, warez, phishing, sniffing či skimming. V mnohých prípadoch je veľmi sofistikovaná a jej objasnenosť hraničí s nulou [3].

Samotný termín počítačová kriminalita nie je explicitne definovaný v Trestnom zákone alebo v obdobnom normatívnom právnom akte. Pre účely slovenských trestnoprávnych predpisov sa vychádzalo z definície obsiahnutej v Dohovore rady Európy o počítačovej kriminalite, ktorý dňa 1. augusta 2007 ratifikovala slovenská vláda. Touto normatívnou zmluvou, ktorá je pre Slovenskú republiku záväzná z hľadiska medzinárodného práva a európskeho práva, je počítačová kriminalita vymedzená nasledovne: „Počítačová kriminalita je akékoľvek nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu. S termínom počítačová kriminalita sa v rámci Slovenskej republiky môžeme stretnúť v rôznych alternatívach, napríklad kybernetická kriminalita alebo kyberkrimalita. V anglickom jazyku nachádzame oveľa viac alternatív, napríklad computer crime, cyber crime, cybercrime, cyber-crime, high-tech-crime, virtual crime, e-crime či internet crime.

Podľa [4] je kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi. Podľa [5] internetová kriminalita je trestná činnosť, kedy sú služby alebo aplikácie na internete použité na trestný čin, sú cieľom trestného činu alebo internet je zdrojom, nástrojom, cieľom alebo miesto trestného činu.

Počítače v podstate neumožňujú páchať nový typ trestnej činnosti, iba poskytujú novú technológiu a nové spôsoby na páchanie už známych trestných činov ako je sabotáž, krádež, zneužitie, neoprávnené užívanie cudzej veci, vydieranie alebo špionáž. I keď Trestný zákon priamo nedefinuje počítačovú kriminalitu pozná a definuje skutkové podstaty jednotlivých trestných činov, ktoré spolu tvoria právny rámec pre počítačovú kriminalitu na Slovensku. Pri riešení počítačovej kriminality sa teda polícia opiera hlavne o tieto zákony: č. 91/2016 Z.z., č. 300/2005 Z.z., č. 301/2005 Z.z., č. 185/2015 Z.z., č. 351/2011 Z.z., č. 211/2000 Z.z., č. 18/2018 Z.z., č. 171/1993 Z.z., ZZ 275/2006 Z.z., Výnos MF SR 55/2014 Z.z., vyhláška NBÚ č.337/2004 Z.z. a smernice, resp. nariadenia EÚ: smernica č. 2016/1148 (NIS), nariadenie č. 2016/679 (GDPR) a smernica č. 2015/2366 (PSD2).

Vzhľadom na definíciu počítačovej bezpečnosti je možné poukázať na dve skupiny počítačových trestných činov, a to:

- Trestné činy, ktorých cieľom je počítač.
- Trestné činy, pri ktorých je počítač používaný ako nástroj na ich spáchanie.

V prvom prípade je počítač alebo jeho služba cieľom útoku.

Protiprávne konanie spočíva napríklad v prieniku do počítača alebo siete za účelom „krádeže“ dát, súborov či dokumentov, v neoprávnenom zásahu do informačných systémov alebo aj vo vydieraní založenom na hrozbách zo zverejnenia odcudzeného obsahu alebo jeho nežiadúcom zašifrovaní. V tomto prípade dochádza k neoprávanému prístupu k počítaču, t. j. k hackerstvu. Keďže počítač je majetkom/vlastníctvom, neoprávnený prístup k počítaču je podobný nepovolenému vkročeniu na cudzí pozemok. Avšak, kým neoprávnené vkročenie na cudzí pozemok či do obydlia sa týka reálneho sveta, neoprávnený prístup k cudziemu počítaču sa týka kyber priestoru.

Špecifikom je aj povaha nástrojov a technológií, ktoré sú použité k páchaniu tejto trestnej činnosti, a ktoré zároveň sú aj jej terčom. Tieto technológie sú čím ďalej, tým viac dostupné (napr. nezabezpečené webkamery, domáce routre, P2P siete atď.), čím umožňujú páchanie trestnej činnosti bez zložitejšej prípravy každému. Špecificky v tomto smere vytvára takmer neobmedzený priestor rozširujúci sa fenomén tzv. internet vecí (IoT). Súčasní trend pripájania všetkých vecí na internet (napr. telefóny, tablety, televízie, domáce spotrebiče, termostaty, hračky, baby monitory, autá, rôzne senzory, bezpečnostné zariadenia, atď.) menia pôvodný koncept, ktorý namiesto toho aby počítače zabudovával do vecí (tzv. embeded technológie), tak veci pripája k počítačom. V takto vytvorenom priestore si potenciálne obete buď vôbec neuvedomujú svoju zraniteľnosť a potrebu ochrany, alebo ochrana a zabezpečenie technológií, informácií a osobných údajov je finančne nákladná a teda často zanedbávaná oblasť, čím dochádza k uľahčovaniu páchania počítačovej trestnej činnosti.

Špecifickým prípadom je využitie kybernetického priestoru ako komunikačného prostredia, ako napríklad ilegálny predaj drog, zraní, ľudských orgánov, detskej pornografie prostredníctvom internetu (napr. Darknet alebo sociálne siete).

Ako uvádza Španko [6,7] najčastejšie sa stretávajú s týmto druhom počítačovej kriminality:

- útoky na počítač, program, údaje, komunikačné zariadenia a siete,
- neoprávnené získavanie programov a dát,
- neoprávnené využívanie počítačov alebo komunikačných zariadení,
- neoprávnený prístup k osobným údajom a informáciám,
- získavanie utajovaných informácií,
- zneužívanie sociálnych sietí,
- zmena v programoch a dátach,

- softvérové pirátstvo,
- krádež počítača, programu, údajov a komunikačných zariadení,
- zneužívanie počítačov na páchanie akejkoľvek inej trestnej činnosti šírenie poplašných a nepravdivých správ, šírenie detskej pornografie.

3. ŠPECIFICKÉ ZNAKY POČÍTAČOVEJ KRIMINALITY

Od klasickej kriminality sa počítačová kriminalita odlišuje viacerými zvláštnosťami a osobitnými charakteristikami, ktoré je potrebné brať v úvahu v procese zameriavania a realizácie prevencie, a to hlavne:

- anonymitou páchateľa,
- nízkym počtom ohlasovaní trestnej činnosti,
- neuvedomením si obetí o trestnej činnosti na nich páchanej,
- chýbajúcim prvok viktimizácie,
- nedostatkom dôkazného materiálu,
- neobmedzeným priestor pôsobenia.

Počítačová kriminalita sa vyznačuje veľkou anonymitou páchateľov, vzdialenosťou páchateľa a obete, v mnohým prípadoch aj časovým odstupom medzi jednaním a následkom trestného činu a často presahuje hranice jedného štátu. Trestné činy páchané pomocou počítača možno spáchať za relatívne krátky čas bez toho, aby sa páchateľ nachádzal na mieste činu. Využívaním počítačov a internetu sa zmenili podmienky páchania trestných činov, ako aj typy páchateľov a obetí.

Počítačová kriminalita patrí medzi najmenej ohlasované druhy trestnej činnosti, vyznačuje sa vysokou latentnosťou, ktorá sa podľa prieskumov pohybuje až v medziach 90%. Odhaduje sa, že orgány činné v trestnom konaní sa dozvedia len o 10 percentách z celého jej množstva [8]. Obete zo súkromného sektora spravidla nemajú záujem nahlásiť možnú trestnú činnosť a riskovať následné zverejnenie skutočnosti, že boli napr. obeťou hackerov alebo kybernetického útoku, alebo sa obávajú škôd na povesti a dobrom mene, zvýšenej nedôvery verejnosti a následných ekonomických škôd (napr. banky). Sekundárna viktimizácia sa tak stáva rozsiahlejšou než prvotná. Pramení to nielen z dôvodu neochoty obetí tieto trestné činy oznamovať, či s obťažnosti obete identifikovať a lokalizovať, ale aj z rôznych iných dôvodov. Obete počítačovej kriminality napr. často používajú nelegálny software alebo inak porušujú autorské práva a boja sa odhalenia. Takáto neochota oznamovať trestnú činnosť pritom zvyšuje množstvo páchanej počítačovej kriminality.

Obete počítačovej kriminality sa často nedozvedia, že sú alebo boli predmetom útoku páchateľov, (napr. ak došlo k odcudzeniu ich osobných údajov) a v niektorých prípadoch je dôvodom aj nedostatok právneho vedomia, čo má za následok, že obeť nevie, že predmetné konanie je trestným činom. Viktimizácia nemusí byť však v každom prípade zistená, veľké množstvo počítačových útokov je vykonávaných spôsobom, ktorý obmedzuje alebo znemožňuje rozpoznanie (napríklad vo forme rôznych spyware). Zistiť, že sa niekto stal obeťou počítačovej trestnej činnosti je zložité a bez technických

znalostí spravidla nemožné. V prípade koncových užívateľov bez základného bezpečnostného povedomia často ani k odhaleniu nepríde. Odhaľovanie páchateľov počítačovej kriminality je v zásade zložité. Túto trestnú činnosť páchajú predovšetkým mladí ľudia, ktorí majú odborné i praktické skúsenosti z oblasti výpočtovej techniky. Ide najmä o mužov vo veku od 15 do 35 rokov, bez záznamu v registri trestov.

Špecifikom je aj povaha nástrojov, teda technológií, ktoré sú použité k páchaniu tejto trestnej činnosti, a ktoré zároveň sú aj jej terčom. Sú relatívne ľahko dostupné (najmä pokiaľ uvažujeme o softvérovom pirátstve – CD, DVD, Blu-ray mechaniky s možnosťou zápisu a iné), čím umožňujú páchanie trestnej činnosti bez zložitejšej prípravy každému. Určitým aspektom nesporne je aj nízka kúpyschopnosť obetí a teda ich neochota (neschopnosť) zaobstarať si bezpečné a originálne produkty. Ochrana a zabezpečenie hardvéru a softvéru, informácií a osobných údajov je finančne nákladná a teda často zanedbávaná oblasť, čím dochádza k uľahčovaniu páchania počítačovej trestnej činnosti.

Výška prípadnej škody je ťažko zistiteľná a vyčísliteľná. Typickým je nedostatok dôkazného materiálu, spravidla dochádza k okamžitej likvidácii stôp. Dôkazný materiál je špecifický a jeho zaisťovanie znamená vyššie nároky na orgány činné v trestnom konaní. Pri útokoch na vybrané objekty je možné takmer s istotou vylúčiť svedka, a tým sťažiť zisťovanie, odhaľovanie a vyšetrovanie. Na strane používateľov a teda potencionálnych obetí sa vyskytujú, ako jednotlivé fyzické osoby, tak osoby právnické, korporácie či štátne inštitúcie (známy útok hackerov na Národný bezpečnostný úrad, viacero útokov na bankový, finančný a poisťovací sektor). Dôvodov prečo je tomu tak je viacero. Fungovanie orgánov štátnej a verejnej správy, samosprávy je dnes takmer v celom rozsahu digitalizované, pričom väčšina informácií je aj vysoko dôvernej povahy (vrátane osobných údajov) a je uchovávaná elektronicky.

4. ŠTATISTICKÉ UKAZOVATELE

Podľa štatistických ukazovateľov počítačovej kriminality SR je zrejmé relatívne nízke percento zistenej a následne aj objasnenej počítačovej kriminality. Za rok 2016 bolo zistených približne 230 trestných činov počítačovej kriminality, objasnených bolo približne 40%, pričom v porovnaní z prechádzajúcim obdobím je trendom mierny rast. Tento stav zodpovedá situácii, kedy sa spoločnosť nezaoberá efektívnymi spôsobmi reagovania na zmeny bezpečnostnej situácie a vytváraniu účinných nástrojov na predchádzanie počítačovej kriminality. Viaceré prieskumy v informačnej bezpečnosti naznačujú narastanie významu ochrany osobných údajov, ochrany databáz a citlivých informácií, know-how a pod. Výsledky prieskumov naznačujú, že dôraz bude musieť byť kladený na koncového používateľa (ľudský faktor), ktorý predstavuje najväčšie bezpečnostné riziko.

Na nárast významu vzdelávania a budovania bezpečnostného povedomia zamestnancov (koncových užívateľov) poukazuje aj prieskum stavu informačnej bezpečnosti spracovaný Ministerstvom financií SR v roku 2011. Ako je vo výstupoch

prieskumu konštatované poučenie zamestnancov o pravidlách bezpečného používania informačných systémov by malo byť štandardnou súčasťou bezpečnostných opatrení v každej inštitúcii. Prispieva k budovaniu bezpečnostného povedomia zamestnancov a pomáha predchádzať chybám, neželaným následkom a odvracaniu škôd [9].

Trendy rastu počítačovej kriminality a dôležitosti jej predchádzania potvrdzuje aj štatistika počítačovej kriminality EÚ, zameraná na obyvateľov podľa ktorej [10]:

- 74% obyvateľov EÚ si myslí, že môžu byť obeťou počítačového zločinu,
- 59% cíti, že nie je informovaná o rizikách kybernetického priestoru,
- 40% sa obáva zneužitia osobných údajov,
- 12% bolo podvedených online,
- 8% bola odcudzená identita,
- 53% si nezmenilo heslá za posledný rok,
- 52% používa sociálne siete,
- 48% využíva online banking.

V kontexte iných medzinárodných štatistík je zrejmé aj nasledovné [11]:

- globálne škody spôsobené počítačovou kriminalitou budú narastať a do roku 2019 môžu dosiahnuť až 2 bilióny dolárov,
- podstatná časť trestnej činnosti ostane nezistená a to najmä v oblasti nelegálneho získavania citlivých a utajovaných informácií,
- bude narastať množstvo únikov osobných informácií, pričom celkovo sa odhaduje, že tento druh trestnej činnosti rastie ročne približne o 38%,
- narastať budú sofistikované útoky (najmä phishing, ransomware)) s cieľom získavať informácie o platobných kartách, prístupové heslá k mailovým kontám, sociálnym sieťam a informačným systémom.

5. NÁSTROJE SR PRI RIADENÍ KYBERNETICKEJ BEZPEČNOSTI

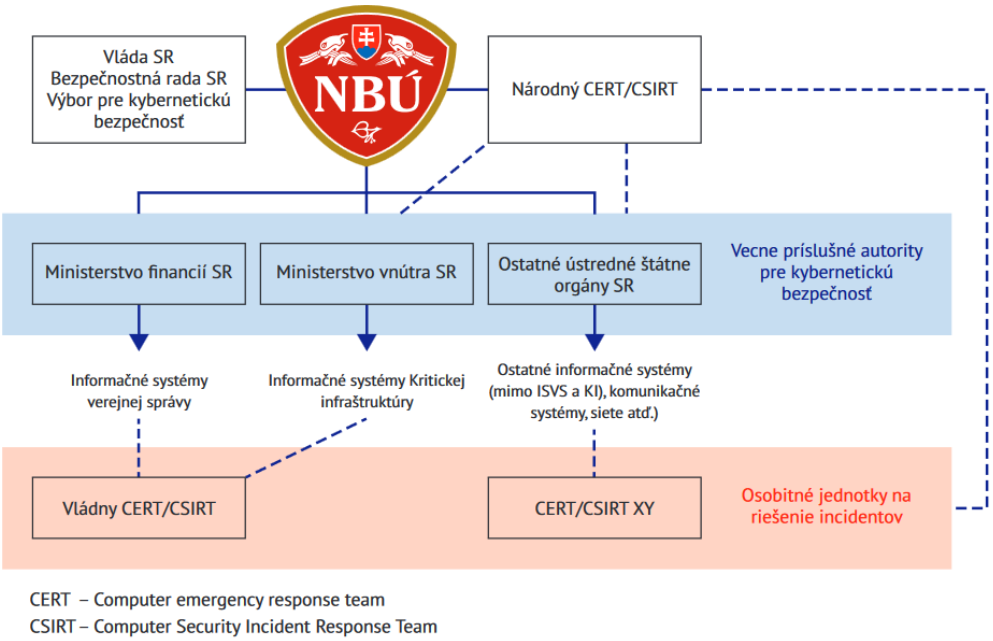
Môžeme konštatovať, že počítačová kriminalita je relatívne novým javom, ktorý vznikol v reakcií na technologický pokrok na konci dvadsiateho storočia. Existujúca právna úprava nedostatočne postihovala tento typ trestnej činnosti. Niektoré trestné činy počítačovej kriminality bolo možné subsumovať pod zákonné ustanovenia skutkových podstát existujúcich trestných činov a niektoré nie. Vznikla tu medzera v rámci zákonného rámca, na ktorú bolo treba reagovať. Snaha o reguláciu počítačovej kriminality prebieha nie len na národných úrovniach štátov, úniovej ale aj na úrovni medzinárodnej. Budovanie novej oblasti kybernetickej bezpečnosti, spolupráca subjektov či už súkromných alebo štátnych nie je možná bez vzájomného porozumenia. Prijatý zákon o kybernetickej bezpečnosti ovplyvní zásadným spôsobom fungovanie nie len bezpečnostného systému, ale aj iných oblastí napr. systému práva a krízového manažmentu.

Termín "kybernetický" sa postupne stáva zaužívaným v praxi a dokonca, ako už bolo uvedené je zavedený aj v niektorých predpisoch. Jeho obsahová náplň však nie je

jasná. Slovenská republika ešte nemá formálne ustálenú terminológiu v oblasti kybernetickej bezpečnosti. Slovo kybernetický, ako aj jeho ďalšie gramatické tvary sa nevyskytuje v žiadnom všeobecne záväznom právnom predpise, ani v terminologických slovníkoch. Jednoducho dať pred zaužívané termíny slovo "kyber" ešte neznamená, že vieme o čom hovoríme. Vznikajú následne rôzne nové spojenia kyberšikana, kyberútok, kyberterorizmus, kyberzločin a pod. Zatiaľ neexistuje v platnej legislatíve SR tento termín a už vôbec nie jeho naplnenie.

Typickým príkladom kde je nesúlad je oblasť trestného práva a zaužívaný pojem počítačová kriminalita. Pre účely slovenskej trestnoprávnej praxe sa používa definícia obsiahnutá v Dohovore rady Európy o počítačovej kriminalite, ktorý dňa 1. augusta 2007 ratifikovala SR. Všeobecne sa pod počítačovou kriminalitou rozumejú trestné činy zamerané proti počítačom ako aj trestné činy páchané pomocou počítača. Samotný pojem počítačová kriminalita nie je explicitne definovaný pojem v slovenskom Trestnom zákone [12] alebo v obdobnom normatívnom právnom akte. Platný a účinný Trestný zákon však pozná a definuje skutkové podstaty jednotlivých trestných činov, ktoré spolu tvoria počítačovú kriminalitu na Slovensku.

Do takejto situácie vstupuje zákon o kybernetickej bezpečnosti a zavádza sa prívlastok "kybernetický". Zákon pritom iba umelo oddelil informačnú a kybernetickú bezpečnosť. Odvoláva sa na Direktívu NIS [13], ale tá pojednáva o informačnej bezpečnosti a slovo kybernetický sa v nej uvádza iba niekoľko krát. Naopak v strategických dokumentoch NATO a EÚ sa pojem "kybernetický" používa. V procese prípravy zákona diskusia k terminológii vypadla. Je pravdepodobne len otázkou času, kedy bude tlak na zjednotenie terminológie dostatočný na to, aby sa začala seriózna diskusia. Koľko problémov však nejednotnosť terminológie spôsobí nie je možné odhadnúť, ukáže že až prax. Toto je však problémom viacerých krajín. V Českej republike bol vydaný Slovník kybernetickej bezpečnosti, práve s cieľom zjednotiť terminológiu v tejto oblasti [14]. Základný navrhovaný rámec SR pri riadení počítačovej – kybernetickej bezpečnosti je definovaný v dokumente „Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, viď. Obrázok 1 [15].



Obrázok 1 Návrh rámcovej štruktúry riadenia kybernetickej bezpečnosti [15]

Z obrázka 1 vyplýva, že počítačová, resp. kybernetická bezpečnosť na národnej úrovni, patrí do pôsobnosti príslušného ústredného orgánu štátnej správy, a to od 1. januára 2016. Kompetencie tohto úradu vymedzuje kompetenčný zákon a konkrétne určuje osobitný právny predpis zákon o kybernetickej bezpečnosti [16], ktorý sa stal účinným od 1.4.2018. Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti komplexne upravuje oblasť kybernetickej a informačnej bezpečnosti, zavádza základné bezpečnostné požiadavky a opatrenia dôležité pre koordinovanú ochranu informačných, komunikačných a riadiacich systémov. Taktiež upravuje rozsah a spôsob výkonu verejnej moci na úseku kybernetickej bezpečnosti, príslušnými ústrednými štátnymi orgánmi a ďalšími štátnymi orgánmi, v rámci konkrétnych vecných oblastí správy spoločensko-ekonomického prostredia štátu. Jednotlivé prepojenie je možné vidieť na obrázku č. 1. Zároveň do slovenského právneho poriadku transponuje európsku Smernicu o sieťovej a informačnej bezpečnosti (NIS).

6. ZÁVER

V článku bol predstavený teoretický rámec počítačovej kriminality podložený výsledkami najnovších prieskumov. Oblasť počítačovej kriminality a jej význam exponenciálne narastá vzhľadom na trend súčasného sveta - digitálnej agendy, ktorá má byť nasledujúcich rokoch i motorom ekonomiky EÚ. Okrem toho vzrastá potreba zvyšovania povedomia o tomto type kriminality a potreba prijímať preventívne opatrenia na každej úrovni spoločenského života, pretože počítačová kriminalita vzhľadom na jej špecifické charakteristiky sa týka celej spoločnosti, skupín v spoločnosti i jednotlivcov. Každá úroveň spoločnosti je vystavená tomuto druhu kriminality. Úlohou štátu je vytvoriť efektívny nástroj riadenie kybernetickej

bezpečnosti a tento nástroj neustále zlepšovať vzhľadom na rýchly vývoj informačných technológií.

LITERATÚRA

[1] Štatistika informačnej spoločnosti - domácnosti a jednotlivci. Dostupné na internete:<http://ec.europa.eu/eurostat/statistics-explained/index.php/Archive:%C5%A0tatistika_informa%C4%8Dnej_spolo%C4%8Dnosti_%E2%80%93_dom%C3%A1cnosti_a_jednotlivci>.

[2] Správa o stave Únie 2017 – Kybernetická bezpečnosť: Komisia chce, aby EÚ razantnejšie reagovala na kybernetické útoky. Dostupné na internete: <https://www.google.sk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwj1jY_0tqLaAhWJCCwKHXnwCFMQFggmMAA&url=http%3A%2F%2Feuropa.eu%2Frapid%2Fpress-release_IP-17-3193_sk.pdf&usg=AOvVaw2B3ZVp2lXVs3LY5D2RV-di>.

[3] Základy trestného práva. Počítačová kriminalita. Dostupné na internete: <https://www.google.sk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjsova_vKLaAhXIiywKHd_HDdAQFgguMAE&url=https%3A%2F%2Fwww.wolterskluwer.sk%2Fsk%2Fukazka.dm-12965.pdf&usg=AOvVaw3teeVjUleyKrYE4TDMIoyh>.

[4] MARKOVÁ, V. 2018. Súčasný stav a východiská počítačovej kriminality, In *Aktuálne Výzvy prevencie počítačovej kriminality*, 8/2018 APZ a BMSEC.

[5] ISO/IEC 27032 Information technology - Security techniques - Guidelines for cybersecurity.

[6] ŠPANKO, S. 2018. Počítačová kriminalita z pohľadu policajnej praxe, In *Aktuálne Výzvy prevencie počítačovej kriminality*, 8/2018 APZ a BMSEC.

[7] Počítačová kriminalita. Dostupné na internete:<http://info.egov.sk/node/79>.

[8] ŠOLTÉS, V., MARIŠ, L. 2018. Možnosti oznamovania kriminality páchanej v kybernetickom priestore bezpečnostným zložkám, In *Aktuálne Výzvy prevencie počítačovej kriminality*, 8/2018 APZ a BMSEC.

[9] NEDUCHAL, L. 2018. Informačná bezpečnosť - dosiahnutie rovnováhy medzi rizikom a výkonnosťou, eFOCUS 2/2018. ISSN 1336-1805.

[10] Recent developments in European Consumer Law. Dostupné na internete: <http://recent-ecl.blogspot.sk/2012/07/cybercrime-new-eu-statistics.html>.

[11] 20 Eye-Opening Cybercrime Statistics. Dostupné na internete: <https://securityintelligence.com/20-eye-opening-cybercrime-statistics/>.

[12] Zákon Národnej rady SR č. 300/2005 Z. z. o Trestnom zákone (Trestný zákon) a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

[13] Smernica Európskeho parlamentu a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Európskej únii zo 6. júla 2016, L194/1.

[14] JIRÁSEK,P.,NOVÁK,L.,POŽÁR,J.2014. Výkladový slovník kybernetické bezpečnosti, Policejní Akademie České republiky v Praze, Česká pobočka AFCEA, Praha 2014.
[15] Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015 – 2020. Dostupné na internete: <https://www.google.sk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwjo25rsqTaAhVCESwKHY3gDqwQFggsMAE&url=http%3A%2F%2Fwww.rokovania.sk%2FFile.aspx%2FIndex%2FMater-Dokum-187874&usg=AOvVaw0jKaV7pnuAsWUduvbn1sKH>.
[16] Zákon o kybernetickej bezpečnosti. Dostupné na internete: <http://www.zakonypreludi.sk/zz/2018-69>.