Možnosti kybernetické kriminality v oblastech profesionální přípravy odborníků pro kybernetickou bezpečnost

Petr Nitrai

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Petr Nitrai**
Osobní číslo:	**L15196**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

Téma práce: **Možnosti kybernetické kriminality v oblastech profesionální přípravy odborníků pro kybernetickou bezpečnost**

Zásady pro vypracování:

1. **Zpracujte průzkum literárních pramenů.**
2. **Vytvořte odpovídající model pro modelování kybernetické kriminality.**
3. **Na vytvořeném modelu zhodnoťte přípravu odborníků.**
4. **Vyjádřete závěry modelování a návrhy pro praxi.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] JIROVSKÝ,Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing a.s.,2007.284 s. ISBN 978-80-247-1561-2.

[2] SMEJKAL,Vladimír. Kybernetická kriminalita. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk,2015.636 s. ISBN 978-80-7380-501-2.

[3] KOLOUCH, Jan. CyberCrime. CZ.NIC, z.s.p.o., 2016. 525 s. ISBN 978-80-88168-15-7.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **prof. Ing. Jiří Dvořák, DrSc.**
Ústav krizového řízení

Datum zadání bakalářské práce: **3. listopadu 2017**

Termín odevzdání bakalářské práce: **15. května 2018**

V Uherském Hradišti dne 15. listopadu 2017

doc. RNDr. Jiří Dostál, CSc.
děkan

L.S.

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby[1)];
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3[2)];
- podle § 60[3)] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60[3)] odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se bakalářská práce skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

V Uherském Hradišti 14. 5. 2014

.....
podpis studenta

---

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje bakalářské, diplomové, disertační a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy. Vysoká škola disertační práce nezveřejňuje, byla-li již zveřejněna jiným způsobem.

(2) Bakalářské, diplomové, disertační a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

(4) Vysoká škola může odložit zveřejnění bakalářské, diplomové, disertační a rigorózní práce nebo jejich části, a to po dobu trvání překážky pro zveřejnění, nejdéle však na dobu 3 let. Informace o odložení zveřejnění musí být spolu s odůvodněním zveřejněna na stejném místě, kde jsou zveřejňovány bakalářské, diplomové, disertační a rigorózní práce, jíž se týká odklad zveřejnění podle věty první, jeden výtisk práce k uchování ministerstvu.

2) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

3) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Práce se zabývá dvěma oblastmi, kyberprostorem a kriminalitou. V teoretické části uvádí základy a instituce dotčené kyberprostorem a systém prevence kriminality. V druhé části se zabývá modelováním prevence kriminality až po vybranou obec v Moravskoslezském kraji.

Klíčová slova: kyberprostor, kriminalita, systém, plán, analýza.

ABSTRACT

The work addresses two areas of cyberspace and criminality. In the theoretical part, presents the foundations and institutions of the cyberspace, and system of crime prevention. In the second part deals with the modeling of crime prevention up to the selected village in the Moravian-silesian region.

Keywords: cyberspace, crime, system, plan, analysis.

Děkuji panu prof. Ing. Jiřímu Dvořákovi DrSc. za odborné vedení, cenné rady a věnovaný čas při tvorbě bakalářské práce.

OBSAH

ÚVOD

Nemůžeme se nevšimnout, že pojem kyberprostor se začal objevovat a probírat čím dál častěji. To ukazuje na nástup jednoho z budoucích hlavních polí, na kterém se bude odehrávat podstatná většina celosvětových zájmů. Jistěže věci hmotného formátu budou přetrvávat, ale do popředí v důležitosti, pokud už tam nejsou, se budou dostávat informace a data a jejich možnost případné manipulace s nimi. Vyspělé a moderní země jsou si plně vědomy, jaké nepřeberné možnosti kyberprostor nabízí.

Obrana a ochrana různých států tohoto prostoru je neustále prověřována z řad jednotlivců i organizovanějších skupin či dokonce cizího státu. Nelze jednoznačně říci, zda-li jde o snahu pouze poškodit daný stát nebo o snahu změny uspořádání ve světe, ale nelze si nevšimnout, že vojenské agrese proti danému státu se právě přesunuly do kyberprostoru, kde není možné je jednoznačně prokázat. Na konferenci Stratcom summit, konané na začátku května letošního roku, předseda vojenského výboru Severoatlantické aliance generál Pavel ukázal na zaměření se světových velemocí na hybridní nástroje, hlavně propagandu, šířenou v klasických médiích i na sociálních sítích. Zranitelnost západních společností, poté spočívá v otevřenosti, kdy obsah zpráv je nekontrolovaný, a tudíž se nabízí prostor pro dezinformace.

Snaha ovládnout kyberprostor se nemusí odehrávat v globálním měřítku. Je správně, že bezpečnost v kybernetickém prostředí není státům lhostejná a vytváří právní prostředí, kde definuje rámec trestnosti. Také se snaží reagovat na nově vznikající hrozby a dát tak možnosti k vypátrání, stíhání a v konečném řešení i odsouzení pachatelů kybernetické trestné činnosti. Mezinárodní Úmluva o kyberkriminalitě, zákony a národní strategie o kybernetické bezpečnosti, pomocné metodiky a materiály pro hodnocení dopadu narušení bezpečnosti uvádí před čím se bránit, jak se bránit a kam směřovat další přípravu profesionálních odborníků k odhalení možných hrozeb či útoku. To jsou všechno známé nebo předvídatelné okolnosti.

Ale nabízí se otázka, jak právně, společensky a programově upravit činnost samotně smýšlející umělé inteligence, která je již začleňována do našeho běžného života a v budoucnu bude postupně nahrazovat lidské zdroje. Kdo bude odpovědný za její selhání? Bude to výrobce, provozovatel, obsluha nebo sama umělá inteligence? Bude se také lidstvo potýkat s problémy, kdy si samostatně myslící inteligence vyhodnotí, že je proti ní veden útok a bude se bránit nebo vytvářet koordinovanou činnost ve svůj prospěch? Myslím si, že to

jsou otázky naší blízké budoucnosti. Nebudeme řešit problémy, kdo ovládl nebo zneužil umělou inteligenci přes kyberprostor, ale zda-li na nás nebude působit sama.

I. TEORETICKÁ ČÁST

1 KYBERPROSTOR

Kyberprostor se stal globálním fenoménem bez teritoriálních hranic nesoucí velké riziko. Pomalu se zařazuje do operačního prostoru mezi vodu, vesmír, zemi a vzduch. Do našich životů, je již neoddělitelně včleněn kyberprostor, který musí být chráněn proti všem různým formám nelegálních aktivit (kyberkriminalitě). Ochraně kyberprostoru se věnuje neustále více pozornosti a důslednosti, a to nejen od právnických nebo fyzických osob, ale také jednotlivé státy se musí chránit v tomto prostoru. [1]

1.1 Definice kyberprostoru

Americký spisovatel William Gibson z počátku 80. let ve své povídce údajně použil jako první název kyberprostor. Stejný autor ve svém dalším románu popsal kyberprostor jako „sdílenou halucinaci“. Dále se tento prostor stal zájmem různých sociologů, ideologů, filozofů a dalších, čímž došlo k jeho rozšíření.

Tato spíše umělecká představa, i když velice výstižná, se současným a skutečným kyberprostorem nic společného nemá. Většinou je chápán jako virtuální prostředí, které nezná hranic národních států, nemá začátek ani konec a proto nelze určit jeho rozsah. Vzájemným propojením komunikačních a informačních systémů vzniká prostředí, ve kterém se vytváří, uchovávají a vyměňují informace. [2]

1.2 Legislativa

Vznik legislativy pro kybernetickou bezpečnost byl podmíněn stavem, kdy se osobní počítače staly běžně dostupné pro občany a staly se tak součástí každé domácnosti. Samotný počítač doma ještě nepředstavuje až takovou hrozbu, pokud nebudeme brát v potaz možnost fyzického odcizení formou krádeže. Samotné nebezpečí se naplnilo momentem, kdy vznikly počítačové sítě (především internet) a momentem vzniku možnosti ke vzdálenému přístupu k počítači. Problém nastává v případě, kdy pachatel a případná oběť se nachází na zcela odlišných místech. S postupným rozvojem technologií, kdy lze k síti připojit téměř cokoliv, se každý stává více součástí kyberprostoru, aniž by si sám uvědomoval, jak moc se do toho prostoru začleňuje každým připojením svého dalšího zařízení. Na nově vzniklé skutečnosti ohledně informačních technologií musela zareagovat legislativa, zatím vycházející z trestního zákoníku, který začal být nedostačující pro odhalení, vyšetřování a postih páchané trestné činnosti. Klasická kriminalita jistě nevymizela, ale s příchodem počítačových technologií se objevily nové druhy kriminality využívající tyto technologie a tím i

možnost skrýt identitu pachatele. Stále častěji se pak objevují nové druhy podvodů, útoky na funkčnost počítačů, které mají snahu omezit funkčnost počítačové infrastruktury nebo její úplné zastavení, porušování autorských práv, krádeže osobních údajů a jejich nelegální šíření, pornografie a další. [3]

S postupem času se ukázala nutnost vytvoření nové legislativy zahrnující IT technologii všech možných druhů na ochranu a bezpečnost před kyber útočníky. Zákonně nebyla stanovena povinnost na ochranu informačních systémů ani žádné prostředky jak jejich správce přimět k zavedení prostředků pro ochranu. Orgány státní moci, banky a vybrané instituce tvořily snad jedinou odlišnost. Vytvoření nové legislativy pro kybernetickou bezpečnost bylo nutností, ale i tak se musí neustále analyzovat a adekvátně odpovídat na případné hrozby. I přesto se stálé potýká s problémy v justici, kde vyvstávají problémy s kvalitním a účinným získáváním, předáváním a přijímáním elektronických důkazů v trestním řízení, které by vedly k odsouzení pachatele. Problémy nastávají v rozporu mezi zločinci, kteří nerespektují žádná pravidla a hranice a mezi orgány v trestném řízení. Mezinárodní justiční spolupráce dává oporu v právním základě, ale často bývá nedostačující a musí se hledat různé alternativy v efektivní implementaci. Neustále se naráží na překážky mezi národními a mezinárodními předpisy. Je vedena diskuze, neberoucí konce, o vytvoření společného jednotného přístupu, jak právně ošetřit uchování osobních údajů nebo vytvoření technických postupů pro sběr a zajištění důkazů. Další významnou roli hraje posílení a rozvoj spolupráce mimo evropský kontinent, především s partnerem z USA, kam patří významní globální hráči (Facebook, Google a další). [4; 5]

1.2.1 Rešerše zákonů pro kyberkriminalitu

Samotná kyberkriminalita se dotýká mnoha zákonů platných v České Republice, ale nejvíce se orgány činné v trestném řízení opírají o zákon č. 40/2009 Sb. trestního zákoníku, ve znění pozdějších změn a předpisů a zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

1.2.1.1 Trestní zákoník

Většina trestných činů pro kyberkriminalitu spadá do dvou oblastí trestního zákoníku:

- Trestné činy proti majetku –
    - ✓ Neoprávněný přístup k počítačovému systému a nosiči (§ 230),

- ✓ Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231),
- ✓ Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232),

- Trestné činy ve vztahu k datům (uloženým informacím), kdy počítač je prostředkem pro trestný čin:
  - ✓ Šíření pornografie (§ 191),
  - ✓ Výroba a jiné nakládání s dětskou pornografií (§ 192),
  - ✓ Navazování nedovolených kontaktů s dítětem (§ 193b),
  - ✓ Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270),
  - ✓ Hanobení národa, rasy, etnické nebo jiné skupiny osob (§ 355),
  - ✓ Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§ 356),
  - ✓ Šíření poplašné zprávy (§ 357),
  - ✓ Pomluva (§ 184),
  - ✓ Vydírání (§ 175) a mnohé další.

    [6]

1.2.1.2 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) vstoupil v platnost dne 29. srpna 2014 a v účinnost vstoupil prvního dne roku 2015. S neustálým vývojem v oblasti kybernetické bezpečnosti se zákon měnil zatím čtyřikrát, prostřednictvím zákonů č. 104/2017 Sb., 183/2017 Sb., č. 205/2017 Sb., a poslední změna byla uveřejněna v zákonu 35/2018 Sb., zákon o změně některých zákonů upravující počet zvláštních kontrolních orgánů Poslanecké sněmovny, kdy aktuální znění zákona je ke dni 7. března 2018.

V oblasti kybernetické bezpečnosti ukládá povinnosti a práva pro osoby, ale také vymezuje pravomoc a působnost orgánů veřejné moci. Do zákona byly už začleněny předpisy vydané Evropskou unií (směrnice NIS). Dále stanovuje, jakým způsobem se zajišťuje bezpečnost informačních systémů a komunikačních elektronických sítí. Jako hlavní cíle si stanovuje vytvoření základní úrovně bezpečnostních opatření, zpracovat lepší detekci bezpečnostních kybernetických incidentů, zavést systém jejich hlášení a zavedení systémů opatření

k reakci na kybernetické bezpečnostní incidenty. Nakonec také nastavit postupy pro činnost jednotlivých dohledových pracovišť. Úplné znění zákona je dostupné na stránkách Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

Kybernetický zákon dále doplňují vyhlášky a nařízení vlády:

- Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti),
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích,
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby,
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. [7]

1.2.2 Mezinárodní

Úmluva o kyberkriminalitě a dodatkový protokol k ní se staly v mezinárodních dokumentech hlavní páteří o kybernetické trestné činnosti a staly se tak hlavním nástrojem přispívajícím k ochraně společnosti. Tyto dokumenty nesou svůj význam hlavně ve stanovení základního rámce trestných činů a dále také přináší prostředky pro vyšetřování a odhalování kyberkriminality. [8]

1.2.2.1 Úmluva Rady Evropy č. 185 o kyberkriminalitě

Nejvýznamnějším právním dokumentem zabývajícím se kyberkriminalitou, se stala tato Úmluva, protože si vzala za jako hlavní cíl sjednocení národní právní úpravy v kyberkriminilatě. Dosahuje toho pomocí stanov, které ukládají smluvním stranám povinnost zapracovat do svých národních právních řádů nástroje. Tyto nástroje budou pak nápomocny k objasnění a uložení postihu za kybernetické trestné činy. Přesná, jasná a důkladná definice skutkové podstaty trestného činu je nejdůležitější k využití právních trestních norem v kyberprostoru. Další důležitý faktor Úmluvy je vytvoření právního rámce pro jednotný a společný postup. Tento právní rámec pak umožňuje postih pachatelů, kteří spáchali trestný čin na poli kyberkriminality a nemusí brát zřetel, na kterém místě byl tento trestný čin spáchán. [8]

8. listopadu 2001 byla Úmluva o kyberkriminalitě schválena Výborem ministrů Rady Evropy a dalších 15 dnů později 23. listopadu 2011 byla otevřena k podpisu v Budapešti.

Úmluva o kyberkriminalitě vstoupila v platnost 1. července 2004. Ke dni 5. 1. 2018 byla podepsána 56 státy, z toho 4 státy podepsaly, ale neratifikovaly. Česká republika podepsala 9. února 2005 a až 22. srpna 2013 ji ratifikovala. V platnost v ČR vstoupila 1. prosince 2013. V článku 14 - 21 této Úmluvy je stanoveno pro členské státy EU povinnost vnést do svých právních řádů taková ustanovení, která budou mít schopnost objasnit a vyšetřit trestnou činnost v kyberkriminalitě. K této Úmluvě se rovněž připojily i státy, které nejsou členy EU. Podepsali a ratifikovali ji státy jako Kanada, Spojené státy americké nebo Japonsko. [8]

Úmluva Rady Evropy č 185 o kyberkriminalitě se skládá z preambule a 48 článků. Tyto články jsou pak dále rozděleny do 4 kapitol. Nejvýznamnější jsou kapitola druhá, která pojednává o přijetí opatření na vnitrostátní úrovni a kapitola třetí, která vymezuje mezinárodní spolupráci. [9]

Jedinečnost této Úmluvy spočívala v identifikaci čtyř základních skupin trestných činů uvedených v kapitole druhé, článků 2 – 13 a dalších z trestního práva hmotného. Země, které podepsaly Úmluvu o kyberktiminalitě, tak dostaly nástroj k efektivnímu stíhání kybernetických útoků. Především se jedná o trestné činy s porušováním autorských práv a práv souvisejících, trestné činy spojeny s počítači, trestné činy související s obsahem a trestné činy proti utajování, integritě a dostupnosti počítačových dat a systémů. [8]

1.2.2.2 Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě

Dne 28. ledna 2003 byl dodatkový protokol přijat k Úmluvě o kyberkriminalitě, která se nezbývala oblastí trestných činů a definuje tuto oblast. Úmluva Rady Evropy č. 185 se nevěnovala trestným činům, které pomocí šíření různých materiálů podněcují k rasové nenávisti ať rasistickým nebo xenofobním způsobem či jiným projevem rasové diskriminace. [8]

Dodatkový protokol je složen z preambule a 16 článků. Tyto články jsou rozděleny do 4 kapitol:

Kapitola první -

uvádí obecná ustanovení, vymezuje pojem rasistický a xenofobní materiál

Kapitola druhá -

se zabývá opatřeními na vnitrostátní úrovni, která mají být přijata

- Článek 3 - Šíření rasistického a xenofobního materiálu skrze počítačový systém
- Článek 4 - Rasisticky a xenofobně motivovaná výhružka
- Článek 5 - Rasisticky a xenofobně motivovaná urážka
- Článek 6 - Odmítnutí, hrubé zlehčování, schvalování nebo ospravedlňování genocidy nebo zločinů proti lidskosti

Kapitola třetí -

Vyjadřuje vztah mezi dodatkovým protokolem a Úmluvou Rady Evropy č. 185

Kapitola čtvrtá -

Uvádí závěrečná ustanovení [10]

1.3 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) byl vytvořen v rámci, změny zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, který nahradil zákon číslo 205/2017 Sb. Vznikl 1. srpna 2017, se sídlem v Brně, kde v jeho čele stojí ředitel jmenovaný vládou. Vznikl, jako ústřední správní orgán pro kybernetickou bezpečnost a také pro ochranu utajovaných informací v rámci informačních a komunikačních systémů a kryptografické ochrany. Součástí úřadu se stala starost o problematiku neveřejné služby v rámci družicového systému Galileo.

Mezi hlavní oblasti činnosti NÚKIB patří:

- Provozovat Vládní CERT České republiky (GovCERT.CZ),
- Spolupracovat s ostatními národními CERT a CSIRT týmy,
- Spolupráce na mezinárodní úrovni s CERT a CSIRT týmy,
- Připravovat bezpečnostní standarty pro informační systémy KII a VIS,
- Šíření kybernetické bezpečnosti a podpora vzdělávání v této oblasti,
- Výzkum a vývoj pro kybernetickou bezpečnost,
- Kryptografická ochrana,
- Národní kontaktní místo PRS – služba evropského satelitního systému Galileo (NCPRS). [11]

1.4 Govert. cz

Vládní CERT (GovCERT.CZ) tým a týmy typu CSIRT nesou důležitou až klíčovou roli v oblasti ochrany kritické infrastruktury a důležitých informačních systémů. Dnes již každá země má své kritické systémy připojeny k internetu, musí být tedy schopna je účinně a efektivně bránit před bezpečnostními hrozbami. Nedílnou součástí je propracovaný systém řízení v předcházení, identifikaci, schopnosti reakce, koordinovaného postupu při působení vlivu bezpečnostního incidentu. Další úlohou těchto týmů je být pomocnou rukou pro orgány státu, organizace a občany, a to hlavně jako prvotní zdroj bezpečnostních informací a být nástrojem na zvyšování vzdělanosti v oblasti bezpečnosti na internetu. Zákon o kybernetické bezpečnosti vymezuje, které orgány a osoby musí plnit určité povinnosti vůči národnímu CERT týmu. Národní CERT tým zaštiťuje organizace CZ.NIC. [12]

Národní centrum kybernetické bezpečnosti (NCKB) a jeho vládní tým GovCERT.CZ vyplývající z jejich činnosti, pak nabízí pro organizace služby, které mohou pomoci v zajištění kybernetické bezpečnosti:

- Koordinační činnost a pomoc při řešení incidentů –

  pomoc při řešení bezpečnostních incidentů formou technické podpory a návrhy pro preventivní opatření. V případě útoku na více subjektů najedou koordinovat společný postup při řešení události.

- Zprostředkování kontaktů –

  rozsáhlá spolupráce, jak v národní tak i mezinárodní sféře mezi organizacemi zabývajícími se bezpečností, přináší spousty kontaktů, které lze poskytnout.

- Sdílení dat –

  spolupráce vládního týmu a různých nadnárodních organizací, zabývajících se kybernetickou bezpečností, přináší nepřeberné množství dat a reportů, které lze poskytnout.

- Nasazování honeypotů –

  síťové pasti umožňující detekci neautorizovaného přístupu do systémů a sledování chování útočníků.

- Penetrační testování –

slouží jako jedna z možností při preventivních aktivitách, jde o externí legální pokus průniku do testovaných systémů, kdy na základě výsledné analýzy lze navrhnout adekvátní bezpečnostní opatření.

- Informační HUB –

na internetových stránkách lze nalézt analýzy, články související s aktuálními bezpečnostními hrozbami. Každý měsíc vychází bulletiny, které uvádějí významné bezpečnostní incidenty v ČR i v zahraničí.

- Vzdělání a výzkumná činnost –

příprava přednášek a školení z kybernetické bezpečnosti (legislativní i technické).

- Forenzní laboratoř a scada laboratoř –

nabízí možnosti technického vyšetření a analýzy ve forenzní laboratoři pro již napadené zařízení nebo při zjištění odůvodněné obavy ukazující možnosti napadení zařízení. [12]

1.5 Příprava profesionálních odborníků

Přijetím a schválením Národní strategie kybernetické bezpečnosti České republiky na období let 2015 – 2020 se Vláda ČR zavázala k naplňování cílů kybernetické bezpečnosti. Jeden z klíčových bodů této Strategie je potřeba celospolečenská osvěta a vzdělávání. Jednotlivé konkrétní body Strategie jsou rozpracovány v Akčním plánu k národní strategii kybernetické bezpečnosti ČR na období 2015 - 2020, který mimo jiné definuje tři hlavní cíle vzdělávání v oblasti kybernetické bezpečnosti:

- Navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti jak u žáků základních a středních škol, studentů vyšších odborných a vysokých škol, tak u široké veřejnosti, respektive koncových uživatelů, pomocí podpory iniciativ a osvětových kampaní, pořádáním konferencí pro veřejnost apod.,
- Modernizovat stávající vzdělávací programy na základní a středoškolské úrovni a podporovat na vysokoškolské úrovni nové studijní programy, které budou přímo vzdělávat experty na kybernetickou bezpečnost,
- Vzdělávat a školit zaměstnance veřejné správy působící nejen v oblasti kybernetické bezpečnosti a informační kriminality.

Ochrana národní kritické informační infrastruktury (KII) a významných informačních systémů (VIS), které jsou uvedeny v Akčním plánu, mají zásadní vliv na fungování ČR, a proto osvěta a vzdělávání v této problematice je základem prevence a ochrany informačních a komunikačních systémů.

Národní bezpečnostní úřad (NBÚ) a jeho centrum pro kybernetickou bezpečnost (NCKB) je hlavním zastřešujícím garantem v oblasti vzdělávání pro kybernetickou bezpečnost, který vydal koncepci pro vzdělávání. Snahou koncepce je získat celistvé povědomí o cílových skupinách, analyzovat jejich potřeby, rozpracovat a navrhnout prostředky k realizaci těchto potřeb tak, aby byly naplněny stanovené úkoly vzdělávání, které ukládá Akční plán. Koncepce neukládá úkoly ani nevyžaduje jejich plnění, ale je podpůrným materiálem a metodickým návodem pro jednodušší členění veřejnosti (laické i odborné) do skupin. Rozdělení slouží k lepší orientaci v tématu kybernetické bezpečnosti a efektivnímu nastavení parametrů pro vzdělávání.

Koncepce vznikala ve spolupráci s Ministerstvem školství, mládeže a tělovýchovy, Národním ústavem pro vzdělávání, Ministerstvem práce a sociálních věcí a Národním centrem bezpečnějšího internetu, které vydaly Strategii digitálního vzdělávání do ruku 2020 a Strategii digitální gramotnosti ČR na období 2015 – 2020. Snahou koncepce je podat celkový přehled o účinnosti, struktuře a potřebách těchto strategií.

NBÚ a NCKB při tvorbě koncepce, také vycházela z dokumentu Evropa 2020 vydaného Evropskou komisí, který stanovuje kroky pro inteligentní a udržitelný růst podporující začlenění. Mezi priority procesu začlenění patří podpora vzdělávání, odborné přípravy digitální společnosti. [13]

2 KRIMINALITA

Než se začneme zabývat prevencí kriminality, jen nutné vysvětlit co si lze pod pojmem kriminality představit a uvést její dělení, abychom se mohli zamyslet nad tím, jak této problematice předcházet.

2.1 Definice kriminality

Dle normativního vymezení, představuje kriminalita společenský jev, kterým se rozumí souhrn trestné činnosti nebo kriminálního chování v určité oblasti za určitého období. Podle sociologického pohledu na kriminalitu ji lze zkoumat v širších souvislostech. Ty se pak zaměřují na sociální podmíněnost a důsledky kriminálního chování. Kriminalitu jako takovou pak můžeme rozdělit do několika druhů. [14]

2.1.1 Druhy kriminality

Majetková kriminalita – je jednání trestně postižitelné, kdy je cílem majetek bez ohledu na formu vlastnictví. Volně řečeno, jedná se o útok pachatele proti cizímu majetku. Trestné činy majetkové se dělí na:

- krádeže prosté (např. automobilů, věcí z automobilů, kapesní krádeže),
- krádeže vloupáním (např. do bytů, rodinných domů, chat či podnikatelských objektů),
- majetková kriminality ostatní (např. poškození majetku, podvody).

Násilná kriminalita – je jednání trestně postižitelné, nejčastěji za použití fyzické síly nebo pod výhružkou jejího použití, byla-li způsobena újma nebo hrozí-li újma na zdraví a životě člověka nebo je tím omezena svoboda a lidská důstojnost. Hrozbou fyzického násilí anebo i užitím fyzického násilí může být motivováno pro:

- nepřátelství (ze msty spáchána vražda),
- násilí jako prostředek pro další účel (obohacení, loupež),
- vydírání,
- únos,
- ublížení na zdraví,
- útok na veřejného činitele,
- porušování domovní svobody,
- domácí násilí,

Mravnostní kriminalita – neboli sexuální kriminality, spočívá v uspokojení pohlavního pudu formami, se kterými se společnost neztotožňuje, a tudíž jsou pro ni nepřijatelné. Mravnostní čin je vázaný k jedné nebo více osobám, které hrály roli sexuálního objektu přímo nebo zprostředkovaně, a tím mohl pachatel jimi určitým způsobem disponovat k ukájeních svých soukromých potřeb a přání. Do mravnostní kriminality můžeme zařadit:

- znásilnění,
- obchod se ženami,
- kuplířství,
- pohlavní zneužívání,
- ohrožování mravnosti,

Hospodářská kriminalita – je kriminalita, která se týká ekonomiky v soukromém, veřejném i státním zájmu, často páchané skupinami, ale také i jednotlivci pro finanční zisk nebo profesní výhody. Většinou se jedná o směsici trestných činů, začínající obyčejnými krádežemi, zpronevěrami, daňovými úniky, přes kyberzločiny, zneužití pravomoci nebo podvody.

Drogová kriminalita – jsou všechny trestné činy spojené s omamnými a psychotropními látkami (OPL). Každý rok vydává Národní protidrogová centrála výroční zprávu, která je na internetu volně přístupná, kde můžeme zjistit vývoj drogové kriminality za daný rok. Nejčastěji se pak sledují v obecném měřítku jednotlivé druhy OPL jako kokain, heroin, metamfetamin, marihuana nebo obchod s anabolickými steroidy. Do drogové kriminality patří:

- nedovolená výroba a držení OPL,
- šíření toxikománie,
- trestné činy páchané pod vlivem OPL,

Kriminalita proti mládeži – jde o velice ztížené objasňování z hlediska důkazů a svědků. Více patrné poté je, že kriminalita proti mládeži nese možné důsledky v budoucí kriminalitě páchané samotnou mládeží. Podstatným pojmem v oblasti kriminality proti mládeži je zabezpečení blaha dítěte. Tím se rozumí, že dítě nesmí být zneužito rodiči, jinými osobami rodině blízké nebo institucemi zabezpečující výchovu dítěte a to závažným zraněním, tělesným nebo duševním poškozením nebo ohrožením jeho budoucího vývoje. Dítě a jeho blaho pak může být ohroženo členy své rodiny i vně této komunity. Ohrožení se může rozdělit do čtyřech forem:

- Tělesné zneužití (působící bolest a vede ke zranění – údery rukou, nohou, popálení, škrcení), jednorázově nebo opakovaně formou trvalého týrání,
- Zanedbání péče situačně, opakovaně, trvale (osoby nesoucí odpovědnost tak jednají z důvodu nezpůsobilosti, neznalosti, nouze nebo vlastních zkušeností), osoby tak činící vytváří riziko vzniku následků, a to fyzického nebo duševního na zdraví dítěte, anebo už proces vývoje dítěte nenávratně ovlivnili vznikem těchto následků,
- Duševní zneužití spočívá v negativním ovlivnění vývoje osobnosti dítěte, vlivem odmítnutí, strašení, terorizování, korumpování atd.
- Sexuální zneužití dospělou osobou (také i starší mladistvou osobou), spočívá ve zneužití dospělé osoby své autority, fyzické a psychické závislosti dítěte na dospělém a tudíž zneužití jeho zvědavosti, důvěry či náklonosti. [15]

Ostatní kriminalita – sem lze zařadit ostatní trestné činy:

- úmyslné a nedbalostní dopravní nehody, kdy je vedeno trestní řízení,
- týrání zvířat,
- řízení bez řidičského oprávnění,
- zanedbání povinné výživy.

2.1.2 Kritéria hodnocení kriminality

Sociálně patologické jevy, mezi které patří i kriminalita, jsou popisovány základními pojmy jako rozsah, intenzita, struktura a dynamika vývoje. Mezi základní kritéria hodnocení kriminality na našem území patří stav, dynamika a struktura.

Stav kriminality (početní ukazatel neboli kvantitativní) – udává počet evidovaných trestných činů, spáchaných v určitém období a na sledovaném území (může se dělit na území republiky, krajů, okresů nebo jinak určených částí území dle potřebné analýzy). Nejčastějším východiskem jsou hodnoty celých výsledných čísel, vypovídající o kriminalitě a jejím rozsahu. Nebo také se může stav kriminality, udávat v tzv. indexu kriminality, vypovídající o intenzitě kriminality, která je brána vzhledem k hustotě obyvatel soustřeďujícím se na hodnoceném území.

Struktura kriminality (kvalitativní ukazatel) – udává stav kriminality závisejícím na jejím obsahu a to v určitém časovém období a dle jejího charakteru spáchaných trestných činů (jednotlivých skupin trestných činů), které jsou rozděleny dle jednotlivých předem stanovených kritérií.

Dynamika kriminality – uvádí odchylky od rozsahu, struktury a intenzity kriminality v delším časovém horizontu na daném území. Nejčastěji se pak vyjadřuje pomocí kritérií ve změně trendu, v růstu či poklesu nebo stagnaci kriminality.

2.2 Prevence kriminality

Je obsáhlý soubor aktivit zasahující do oblastí všech složek. Skládající se ze stáních, veřejnoprávních a soukromých subjektů, které se snaží působit na potencionální pachatele trestné činnosti a tím předcházet nebo alespoň snížit rozsah páchání kriminality. Dále se snaží působit na oběti trestné činnosti a zmírnit tak jejich obavy z důsledků vzniklých kriminalitou, která byla na nich spáchána. Prevence kriminality si vzala za své, jako hlavní cíl zvyšování pocitu bezpečí občanů. Nejvíce stresující typy kriminality působící na běžné občany, se zaznamenaly mezi majetkovou a násilnou trestnou činností. Na tyto typy je vedena největší část opatření při prevenci, která nese i největší účinek. [14]

2.2.1 Objekty a opatření prevence kriminality

Objekty prevence kriminality:

- kriminogenní faktory – sociální prostředí, příčiny a podmínky kriminality,
- potenciální nebo skuteční pachatelé trestné činnosti,
- potenciální nebo skutečné oběti trestných činů,

Opatření při prevenci kriminality:

- Sociální prevence – se snaží působit formou aktivit na probíhající proces socializace a integrace do sociálních skupin, kde mají tyto aktivity snahu změnit vývoj nepříznivých ekonomických a společenských podmínek. Nepříznivé podmínky jsou často označovány za původce při páchání trestné činnosti. Nejčastěji jsou aktivity sociální prevence zaměřené na:
  - ✓ sport (hřiště, skate a in line areály, sportovní vybavení),
  - ✓ zájmové aktivity (umělecké, klubové, technické),
  - ✓ nízkoprahová zařízení a streetwork (pomoc pro mládež bez vázání se k zařízení),
  - ✓ terapeutické pobyty a výchovné pobyty, poznávací akce,
  - ✓ poradenská zařízení, krizová zařízení (azylová, výchovná),

- ✓ specializované projekty (na zvýšení právní vědomosti, proti šikaně, bezpečnosti na internetu ne jen pro seniory),
- ✓ pomoc obětem trestné činnosti.

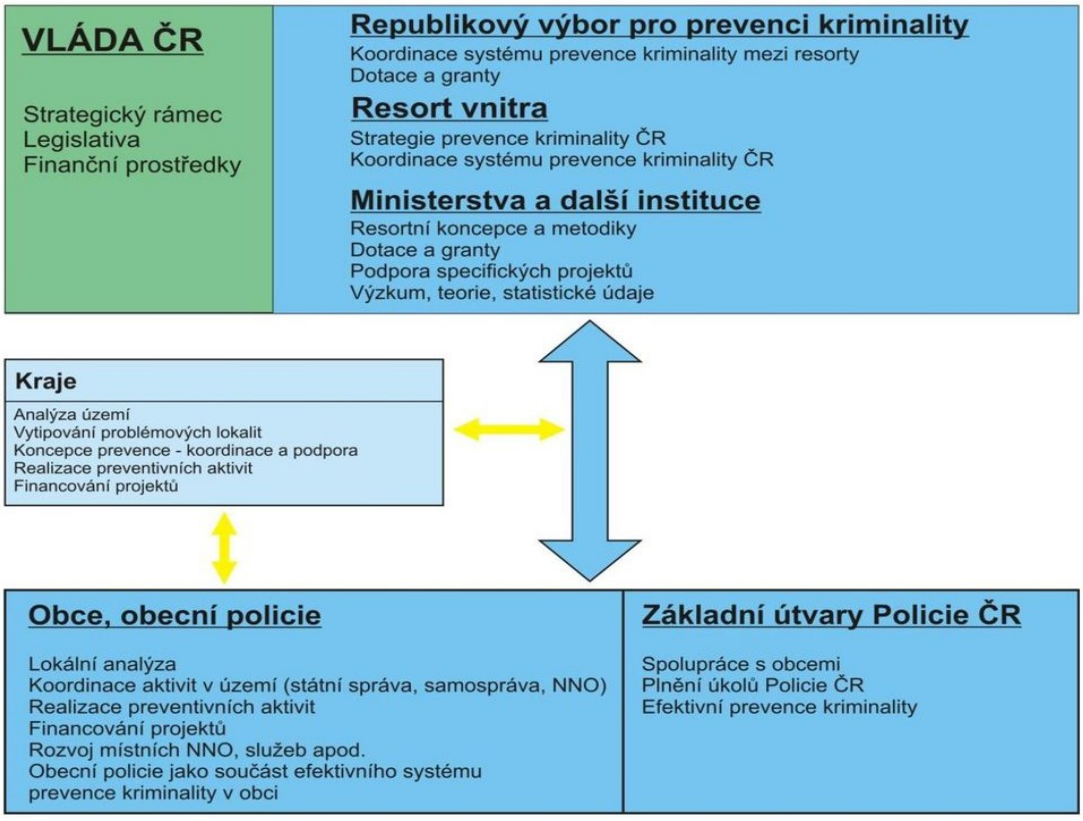
- Situační prevence – vychází ze znalostí, zkušeností a analýzy dat jednotlivých druhů trestné činnosti, které se většinou opakují a mívají znaky vázané na určité místo, dobu a za určitých okolností. Nejvíc úspěšná je situační prevence v oblasti majetkové kriminality, kde využívá prostředky, na její snížení, pomocí technických, fyzických a režimových druhů ochrany (městské kamerové systémy, osvětlení, oplocení, pulty centralizované ochrany a další). Hlavními úkoly situační prevence se pak stává:
  - ✓ zvýšení ochrany objektů, osob a věcí, kde se předpokládá trestná činnost, a tím snížení dostupnosti cílů a výnosů z trestné činnosti,
  - ✓ ve vytipovaných oblastech, vytvoření bezpečných zón,
  - ✓ koordinace postupu bezpečnostních složek a tím zvýšení jejich efektivity
  - ✓ možnost použití instalovaných opatření, jako důkazního prostředku při páchání trestné činnosti, a tím zvýšit možnost zachycení, identifikaci a dopadení pachatelů trestné činnosti.
- Prevence viktimnosti a pomoc obětem trestné činnosti – je spojením sociální a situační prevence a spočívá v prevenci jak se nestát obětí trestného činu nebo pomocí jeho obětem formou psychologické, zdravotní a právní pomoci, dále také v různých programech, které učí obrannou strategii a možnosti ochrany před trestnou činností. Hlavním nositelem zajišťující prevenci je Policie ČR, která má své poradní týmy zřízené na všech krajských ředitelstvích a územních odborech PČR, dále se také do prevence zapojuje Městská policie. Do podvědomí občanů se snaží vštěpit zásady prevence, pomocí pořádání projektů o informovanosti obyvatelstva a komunikaci s veřejnosti formou přednášek, poradenských center, praktických kurzů sebeobrany, informačními materiály nebo venkovními varovnými prostředky. [14]

2.2.2 Směry prevence kriminality

Všechny druhy prevence se navzájem prolínají a doplňují a tvoří tak základ pro jednotlivé směry prevence:

- Primární prevence – snaží se trestné činnosti předcházet pomocí poradenských, výchovných, vzdělávacích a volnočasových projektů se zaměřením na nejširší veřejnost. Větší pozornost je pak věnována na děti a mládež, kde se snaží působit pozitivně pomocí sportovních aktivit a využití volného času.
- Sekundární prevence – je pozornost zaměřena na rizikové jedince nebo skupiny osob, které mají předpoklady pro potenciální páchání trestné činnosti anebo se stanou obětí této činnosti, a to projevem jejich sociálně patologickými jevy jako alkoholovou nebo drogovou závislostí, gamblerstvím nebo také dlouhodobou nezaměstnaností. Tyto patologické jevy pak můžou být příčinou kriminogenních sklonů.
- Terciární prevence – spočívá ve snaze v opětovném začlenění lidí s kriminální minulostí a to pomocí při hledání práce (případná rekvalifikace), bydlení, psychologickým poradenstvím v rodinném a sociálním prostředí. Cílem terciární prevence je udržení výsledků předešlých intervencí. [14]

2.2.3 Model a systém prevence kriminality v ČR



Obrázek 1 Model prevence kriminality v ČR

Zdroj: [16]

Systém prevence kriminality v ČR je organizován do tří úrovní:

- Republiková – včasná intervence a vytvoření týmů pro mládež na celorepublikové úrovni, účelné čerpání finančních prostředků z Evropských fondů, vymezení prevence kriminality v legislativě.
- Krajská – vytvoření koncepce programů pro prevenci na krajské úrovni a s tím spojené vyčlenění prostředků pro její realizaci.
- Městská (místní) – vychází z možností a potřeb daná místa a kombinuje situační a sociální prevenci, do které zapojuje instituce působící na území obce. Zapojeny by měly být orgány veřejné správy, policie i nevládní organizace. [14]

2.3 Kyberkriminalita

Podvodná jednání

Policie nejvíce eviduje přečin Podvod podle § 209 trestního zákoníku a také neoprávněný přístup k počítačovému systému nebo nosiči informací a to podle § 230 trestního zákoníku. Mezi činy naplňující skutkovou podstatu můžeme zařadit podvodné e-shopy, které byly vytvořeny za účelem podvodného finančního zisku, kdy po dosažení cíle jsou finanční prostředky odeslány za hranice našeho státu, pro dezinformaci a utajení finančních cest nebo také mohou být převedeny na virtuální měny. Doba trvání takového e-shopu je velmi krátká a rychle zaniká. Stejného postupu je využíváno při nabídkách podvodných inzerátů, kterých je nespočet. Neopatrný člověk pak může nevědomky naletět při prodeji automobilů, pronájmu bytu, prodeji elektroniky nebo živých zvířat. K podvodnému jednání lze připsat také krádeže peněz z bankovních účtů pomocí phishingu nebo také podvržené emaily. [17]

Hacking

§ 230 trestního zákoníku o neoprávněném přístupu k počítačovému systému a nosiči informací lze aplikovat téměř na všechny trestné činy označované jako hacking. Jedná se o narušení systému, narušení dat a také ke zneužití zařízení. Nejčastější případy vyšetřování, se týkají pachatelů, kteří zvládnou překonat zabezpečení počítačového systému. Ovládnou tak přístup ke své potencionální oběti a získají tak možnost vlastnit údaje o její osobě a jakkoliv dle svého uvážení s nimi manipulovat. Velmi často je tento čin doprovázen instalací škodlivých kódů zvaných backdoory. Samotnou neopatrností a podceňováním zabezpečení se vystavujeme možnosti napadení účtů emailových, na sociálních sítích nebo i in-

ternetového bankovnictví, kde se nachází citlivé informace a dáváme tak možnost vniknout do našeho soukromí. Vzniká tak možnost kompromitovat naše údaje, kdy je pachatel může poškodit, zničit nebo uchovávat ke svému dalšímu finančnímu prospěchu a tím se vystavit další činnosti ze strany pachatele formou vydírání, pronásledování, podvodům nebo krádežím z účtů.

Jako další problém se ukazuje porušení tajemství dopravovaných zpráv podle § 182 trestního zákoníku, kde se zachytávají citlivé informace nebo obsah při běžné komunikaci v síti. Nejvíce dat se pak získává z nezabezpečených wi-fi sítí nebo napadením domácích routerů. Povaha dat, které jsou získávána, se pak liší od postavení jednotlivého typu osobnosti, od které jsou získány a možnosti dalšího využití na poškození pověsti, vytvoření nátlaku nebo finanční zisk. [17]

Blagging

Různorodost podvodů na internetu nezná mezí a tak někteří neztrácejí čas s prolamováním hesel, ale raději využívají sociálního inženýrství. Jde v podstatě o umění klamu, které spočívá v manipulaci s lidmi pro vytvoření určité pachatelem chtěné akce nebo získání potřebných informací. Nebezpečnost při dobře vedeném útoku je v neuvědomění si oběti, že provedla nebo poskytla informaci neoprávněné osobě. [18]

Typ podvodu využívající sociálního inženýrství je tzv. CEO – Command Executive Order. jde o fiktivní příkaz oprávněného k provedení nějaké činnosti, v tomto případě platby na účet. Podvodníci nejdříve nastudují a pak se velmi dobře orientují na trhu, ve struktuře společnosti a v jejich zákaznících, které pak využívají při manipulaci se svou vybranou obětí. Po prvotním kontaktu se pachatel vydává za různé hlavní funkcionáře firmy nebo důvěryhodného partnery společnosti, kdy pod touto záminkou ovlivní předem vybraného zaměstnance, který netuší, že se jedná o podvod, ale žije v domnění v komunikaci s těmito funkcionáři. Ten pak provede akci, která je po něm vyžadována (splatnost pohledávky, uzavření smlouvy). [17]

Podvodné e-shopy

Nákupy přes internetové obchody mají neustálou vzestupnou tendenci. Bezesporu je zde hodně výhod, které tyto nákupy přinášejí, od jednoduchého vyhledání zboží a srovnáním cen v jednotlivých obchodech, rychlost výběru zboží a časová nezávislost kdy neexistuje otvírací doba, přes pohodlí výběru, vyhnutí se frontám u pokladen, značnému počtu lidí v obchodech v obdobích největší poptávky, až po doručení na určenou adresu. Všechny

výhody jsou ale doprovázeny i určitými riziky. Anonymita prodejce, za kterou se může skrývat podvodník je zřejmě největší nevýhodou. Lidé by si měly dávat pozor při nákupu na neověřené e-shopy, u nabídek s velmi neadekvátní nízkou cenou oproti běžným cenám stejného výrobku, není zde možnost zboží prohlédnout, vyzkoušet a u podvodných prodejců bývá většinou jediná možnost platby – předem.

Mravnostní trestné činy

Jsou trestné činy zakotvené v třetí hlavě zvláštní části trestního zákoníku (§ 185 – 193b). Jedná se o skupinu zasahující důstojnost oběti v sexuální oblasti, kde patří trestné činy:

- ohrožující svobodu rozhodování v oblasti pohlavního života - znásilnění a sexuální nátlak,
- ohrožující zdravý mravní a tělesný vývoj dětí – pohlavní zneužití, svádění dítěte k pohlavnímu styku a zneužití dítěte k výrobě pornografie,
- ohrožující některé mravní zásady – výroba a jiné nakládání s dětskou pornografií, kuplířství. [19]

Trestné činy proti autorskému právu

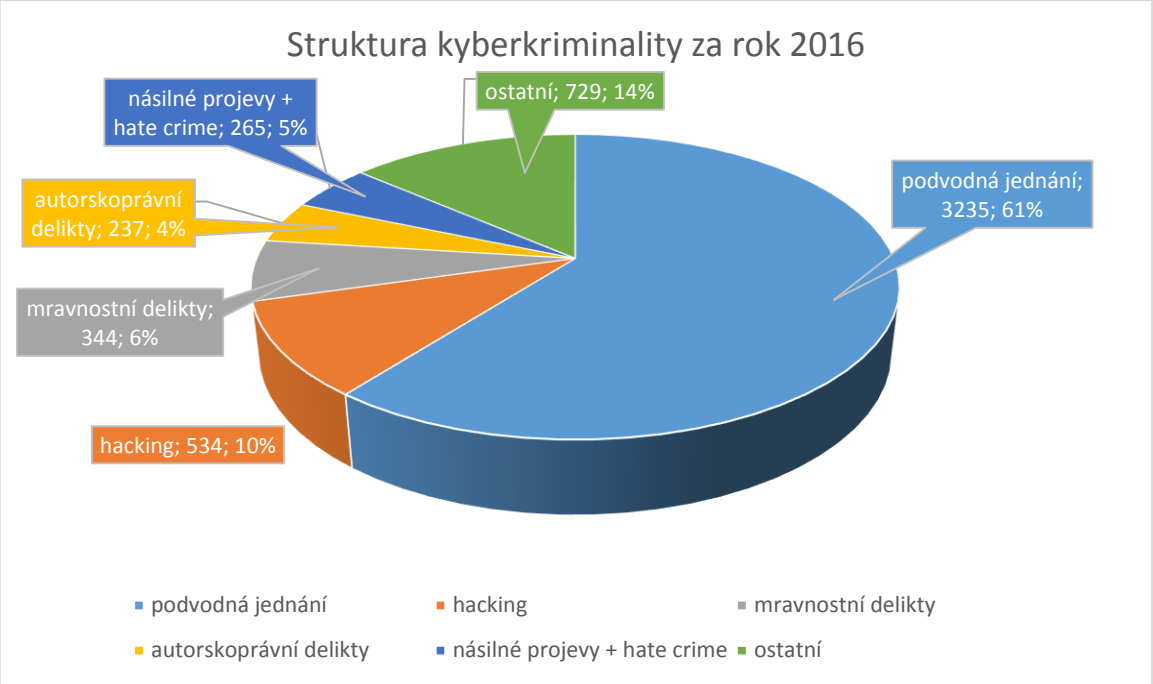
Vychází z trestního zákoníku uvedeného pod § 270, který se zabývá porušením autorského práva, práv souvisejících s právem autorským a práv k databázi. Nejčastěji se jedná o rozpor s autorským právem v šíření hudebních skladeb, filmů a softwaru pomocí velkokapacitních úložišť. [17]

Násilné projevy a hate crime

Za použití informační technologie získávají trestné činy, v této oblasti využívající prostředků a služeb podporující anonymitu. Mezi nejznámější trestné činy patřící do této kategorie v trestním zákoníku se řadí:

- Vydírání § 175,
- Nebezpečné vyhrožování § 353,
- Nebezpečné pronásledování (stalking) § 354,
- Šíření poplašné zprávy § 357,
- Hanobení národa, rasy, etnické nebo jiné skupiny osob § 355,
- Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod dle § 356.

Pražská policie zavedla preventivní program zaměřený na chování dětí a mládeže se znaky rasismu, xenofobie, antisemitismu, diváckého násilí a další projevy z nenávisti. Tento projekt je zaměřen na poslední dva ročníky základní školy a první dva ročníky střední školy. Během přednášky se studenti dozvídají různé druhy projevu extremismu a je kladen důraz na právní aspekty těchto projevů. Na svých stránkách policie spustila aplikaci na upozornění na závadný obsah nebo aktivity na internetu. [20]



Graf 1 Struktura kyberkriminality

Zdroj: [17]

2.4 Dílčí závěr teoretické části

Dynamický rozvoj kyberprostoru přinesl nezbytnou reakci, na kterou museli vládní představitelé reagovat, pokud chtějí ochránit a zabezpečit státní infrastrukturu pro dobře fungující stát. Infrastruktura se s rozvojem informačních technologií přenáší stále ve větší míře do kyberprostoru, který byl Severoatlantickou aliancí uznán jako další operační doména. ČR se rozhodla pro vznik samostatného Národního úřadu pro kybernetickou bezpečnost v područí Národního bezpečnostního úřadu, jako ústředního orgánu pro kybernetickou bezpečnost. V neohraničeném kyberprostoru se nabízí stéle větší možnosti kyberkriminality, která vychází ze samotné podstaty obecné kriminality, jen se stala více anonymní, odhalitelná a postihnutelná. Snížení kriminality obou forem je spjatá s dobře fungujícím systémem prevence kriminality, vzděláváním a přípravou odborníků v této problematice.

II. PRAKTICKÁ ČÁST

3 NÁRODNÍ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI

S nástupem moderních technologií a jejich bleskovým rozšířením do většiny domácností, kdy s každým rokem jsou tyto technologie čím dál víc propracovanější a na vyšší úrovni, se stále více lidských činností a aktivit přesouvá do kyberprostoru. Získání informací a komunikace, je tak daleko jednoduší, než tomu bylo dříve, ale na druhou stranu vyvstala nová hrozba ve formě zajištění kybernetické bezpečnosti, která je jednou z největších výzev pro státy.

Národní autoritou v oblasti kybernetické bezpečnosti je již od roku 2011 Národní bezpečnostní úřad (NBÚ). Ze Strategie pro oblast kybernetické bezpečnosti České republiky vydané na období 2012 – 2015 bylo splněno mnoho úkolů. Přijetí zákona o kybernetické bezpečnosti a otevření Národního centra kybernetické bezpečnosti se tak podařilo naplnit mimo jiné dva důležité cíle pro kybernetickou bezpečnost.

S končící platností strategie a splněním zásadních cílů se musela začít připravovat nová Národní strategie kybernetické bezpečnosti na období 2015 – 2020, která už nemusí řešit vybudování kapacit pro zajištění kybernetické bezpečnosti, ale může se plnohodnotně věnovat hlubšímu a pokročilejšímu zajišťování kybernetické bezpečnosti. [21]

3.1 Národní strategie kybernetické bezpečnosti ČR na období 2015 - 2020

Česká republika zde představuje své vize v oblasti kybernetické bezpečnosti, kde se staví mezi moderní středoevropské země a aktivního člena Evropské unie, Severoatlantické aliance, OSN a dalších mezinárodních organizací. Své úsilí bude zaměřovat na rozvoj expertní základny, vzdělání a aktivní spolupráci nejen s mezinárodními partnery s cílem zaujmout přední postavení v oblasti kybernetické bezpečnosti.

Zabezpečení kritické informační infrastruktury, jako jeden z důležitých faktorů, pro plnohodnotně fungující prostředí, které bude bezpečné pro realizaci zahraničních i tuzemských investic, pro které je funkční a bezpečná informační infrastruktura zcela zásadní. Zajištění KII, kyberprostoru a bezpečnost sítí jsou základními prvky dobře fungujícího státu, který chrání své obyvatele a podporuje tak jejich ekonomické a sociální zájmy. Podporování výroby, výzkumu a zavádění nových technologií, jako možného prostředku k co možná nejvyššímu zabezpečení kyberprostoru.

Výzvy, před kterými Česká republika stojí:

- Česká republika jako možný testovací objekt,
- Nedostatečná důvěra veřejnosti ve stát,
- Vzrůstající počet uživatelů internetu, informačních a komunikačních technologií a narůstající kritičnost jejich selhání,
- Se vzrůstajícím počtem uživatelů mobilních platforem stoupá i množství mobilního malware,
- Bezpečnostní rizika spjatá s elektronizací veřejné správy (eGovernment),
- Nedostatečné zabezpečení malých a středních podniků,
- Ochrana průmyslových řídicích systémů a informačních systémů ve zdravotnictví,
- Vzrůstající závislost obranných složek státu na informačních a komunikačních technologiích,
- Nárůst informační kriminality,
- Hrozby a rizika spjaté s užíváním sociálních sítí na internetu,
- Nízká digitální gramotnost koncových uživatelů,
- Nedostatek odborníků na kybernetickou bezpečnost a nutnost revize stávajících studijních programů ve školství,
- A další. [21]

3.2 Akční plán k národní strategii kybernetické bezpečnosti ČR na období 2015 - 2020

Je nedílnou součástí pro úspěšné naplnění a dosažení hlavních cílů Národní strategie kybernetické bezpečnosti na období 2015 – 2020 pomocí plnění úkolů stanovených v akčním plánu, kdy je nezbytná součinnost a spolupráce všech zúčastněných subjektů.

V Akčním plánu k národní strategii kybernetické bezpečnosti ČR na období 2015 – 2020 je stanoveno osm oblastí, kde v každé jsou uvedeny hlavní cíle. Z hlavního cíle jsou uvedeny pod kódy, jednotlivé úkoly a neméně důležité informace o tom, kdo nese odpovědnost za daný úkol a v jakém časovém rámci ho musí splnit. Průběh naplňování plánu, je pod dozorem NBÚ a jeho pracoviště NCKB, který je uveřejněn v rámci každoroční Zprávy o stavu kybernetické bezpečnosti v České republice.

Hlavní oblasti:

- Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti,
- Aktivní mezinárodní spolupráce,
- Ochrana národní kritické informační infrastruktury (KII) a významných informačních systémů (VIS),
- Spolupráce se soukromým sektorem,
- Výzkum a vývoj / Spotřebitelská důvěra,
- Podpora vzdělávání, osvěta a rozvoj informační společnosti,
- Podpora rozvoje schopností PČR vyšetřovat a postihovat informační kriminalitu,
- Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce) Účast na tvorbě a implementaci evropských a mezinárodních pravidel. [22]

Celý Akční plán k národní strategii kybernetické bezpečnosti ČR na období 2015 – 2020 je uveden v příloze číslo II.

3.3 Zpráva o stavu kybernetické bezpečnosti za rok 2016

Rok 2016 potvrdil důležitost kybernetické bezpečnosti, na kterou musí Česká republika být schopna adekvátně reagovat. Klíčovou roli sehrály usnesení Vlády ČR o rozvoji kapacit Národního centra kybernetické bezpečnosti (NCKB) do roku 2025 a oddělení ze struktur Národního bezpečnostního úřadu a vytvoření samostatného Národního úřadu pro kybernetickou a informační bezpečnost.

V témže roce se zahájili kontroly kritické informační struktury a významných informačních systémů. Přijetím zákona o kybernetické bezpečnosti v souvislosti se zaváděním požadavků směrnice Evropského parlamentu a Rady EU o bezpečnosti sítí a informačních systémů (NIS) se ČR zařadila mezi nejlépe připravené státy. Prohlubování mezinárodní spolupráce a účastnění se mezinárodních cvičeních tak ČR upevnila svou pozici důvěryhodného partnera v oblasti kybernetické bezpečnosti. [23]

3.3.1 Kritická informační infrastruktura a významné informační systémy

Kritická infrastruktura je určována Národním bezpečnostním úřadem podle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury v aktuálním znění. Posuzování, zda systémy, splňují daná kritéria, probíhá ve spolupráci se správcem systé-

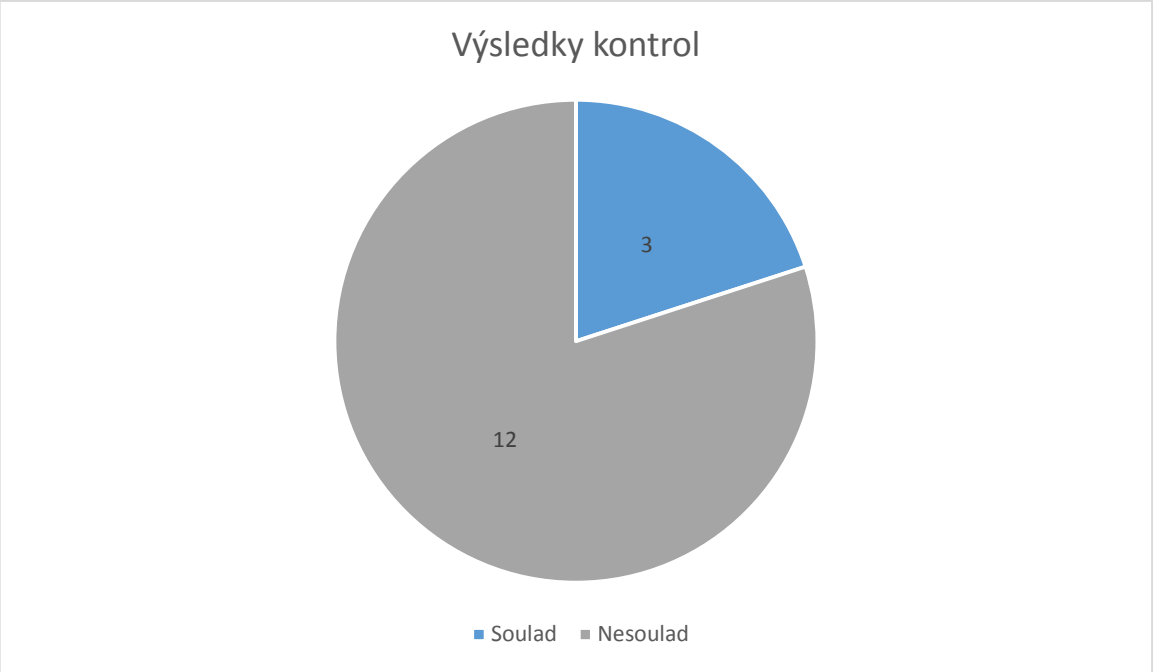
mu, pomocí analýzy dopadu incidentů a dalších podkladů. Určení systému, jako systému kritické infrastruktury poté probíhá podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a závisí na povaze subjektu.

K 31. prosinci 2016 evidovalo NCKB 48 KII a 158 VIS ve správě 80 orgánů veřejné správy a 51 KII a 20 správců v soukromém sektoru. Během roku proběhly kontroly na dodržování zákona o kybernetické bezpečnosti. Pověřeným orgánem kontroly je NBÚ a fyzickým kontrolním orgánem se stává Národní centrum kybernetické bezpečnosti. Kontrola proběhla u celkem 15 správců a 24 systémů, kde byla kontrola většinou zaměřena na významné informační systémy.

Kontroly slouží k získání důkazů (nálezů) o zjištěných nedostatcích a rozlišují se čtyři typy zjištění:

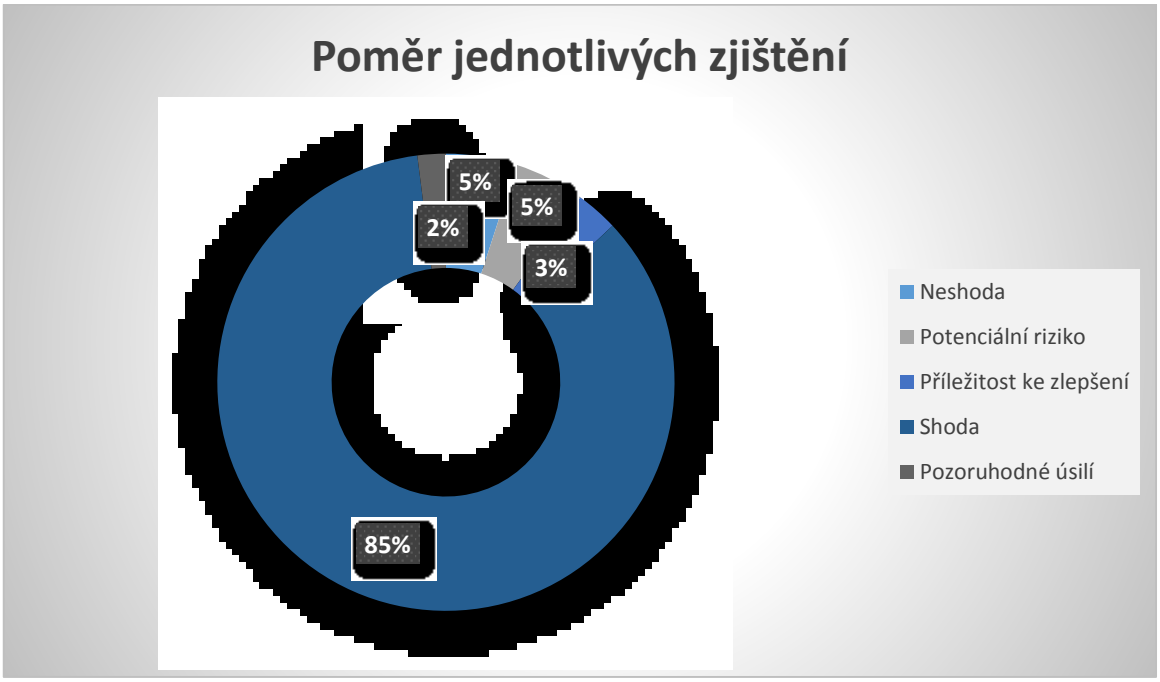
- Neshoda, kterou se rozumí nesplnění požadavku podle stanovených kritérií nebo odchýlení praxe od dokumentovaných postupů v organizaci (nesoulad). Zjištění typu neshoda je důvodem k zahájení správního řízení. U neshod je dále uváděn i termín, do kterého musí dojít k nápravě,
- Potenciální riziko. Jde o typ zjištění, kdy kontrolující upozorňuje na možné riziko,
- Příležitost ke zlepšení. Jde o typ zjištění, které má charakter doporučení a vychází ze zkušeností kontrolujícího,
- Shoda. Shodou se rozumí splnění požadavků podle stanovených kritérií (soulad). Nálezy shod nejsou zahrnuty do kontrolního protokolu,
- Pozoruhodné úsilí. Pozoruhodným úsilím se rozumí nadstandardní hodnocení dané oblasti.

Z výsledků kontroly je patrné, že u 3 byl zjištěn celkový soulad (žádná neshoda) a u 12 případů byl shledán nesoulad (porušení zákona o kybernetické bezpečnosti). [23]



Graf 2 Výsledky kontrol za rok 2016

Zdroj: [23]



Graf 3 Poměr jednotlivých zjištění za rok 2016

Zdroj: [23]

3.3.2 Legislativa a koncepční dokumenty

Národní bezpečnostní úřad se podílel na přípravě zavádění evropské směrnice č. 2016/1148 opatření k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS) do české legislativy a to formou novelizace zákona o kybernetické bezpečnosti a implementace akčního plánu k národní strategie kybernetické bezpečnosti.

Neopomenutelnou součástí práce NBÚ v roce 2016 bylo upozornění vlády České republiky na tzv. bílé místa v zajišťování kybernetické bezpečnosti. Upozorněno bylo také mimo jiné na nedostatečnou úpravu vztahů mezi správci KII a VIS a dodavateli ICT služeb, které by mohly ohrozit funkci některých systémů a na nedostatek odborníků na kybernetickou bezpečnost ve veřejném sektoru. [23]

3.3.3 Mezinárodní spolupráce

Sdílení a předávání informací patří neomylně k základům mezinárodní spolupráce, která pak tvoří jeden ze základních kamenů k zajišťování kybernetické bezpečnosti státu. Tradičními partnery v mezinárodní spolupráci jsou Severoatlantická aliance a Evropská unie. Díky vyslání cyber attaché a zřízení stálého místa v Bruselu má Česká republika lepší povědomí a přehled o otázkách projednávajících se v souvislosti s kybernetickou bezpečností napříč všemi orgány EU a pracovními skupinami Rady.

Varšavský summit byl nejvýznamnější události v Severoatlantické alianci, kde nejvyšší představitelé členských států uznali kyberprostor jako další operační doménu. Cílem bylo upozornit na důležitost kybernetické obrany a bezpečnosti při vedení aliančních operací. Spolupráci s NATO se nevěnuje pouze NBÚ, ale začleněno je i Ministerstvo obrany, které se zúčastnilo aliančních cvičení Cyber Coalition a Locked Shields. Česká republika je na půdě Severoatlantické aliance velmi aktivní, podílí se na více projektech a lidé z oblasti kybernetické bezpečnosti jsou jedni z předních pracovníků v této alianci. [23]

3.3.4 Spolupráce v rámci ČR

Neméně důležitou částí je spolupráce na národní úrovni, která je nezbytná k zajištění kybernetické bezpečnosti v České republice. NBÚ, jako hlavní koordinátor a gestor, vede aktivní spolupráci s ostatními rezorty státní sféry. Klade důraz za pomocí akademických institucí na přípravu odborníků a zvyšování povědomí o kybernetické bezpečnosti. Mezi vládním týmem CERT a národním týmem CSIRT.CZ probíhá dlouhodobá a dobrá výměna

informací, zkušeností a know-how v oblasti zranitelností. Spolupráce s českými bezpečnostními týmy není spojena jen s výměnami dat a informacemi o incidentech, ale všichni se podílejí na vývoji a výzkumu nových nástrojů pro kybernetickou bezpečnost.

V měsíčních cyklech se schází instituce odpovědné za kybernetickou obranu České republiky a boji s počítačovou kriminalitou, kam vedle Národního bezpečnostního úřadu, patří také Police ČR a Vojenské zpravodajství. Zástupci organizací se navzájem informují o aktuálních hrozbách, proběhlých incidentech a důležitých událostech v oblasti kybernetické bezpečnosti. Národní centrum kybernetické bezpečnosti vydává měsíčně bulletin, kde jsou uvedeny bezpečnostní incidenty za každý měsíc.

Policie ČR v roce 2016 nadále pokračovala v plnění úkolů z Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období 2015 – 2020 a provedla u svých struktur organizační změny a personální navýšení u jednotlivých částí, které se specializují na odhalování, vyšetřování kybernetické kriminality a expertní činnosti. Probíhá nábor odborníků ze soukromého sektoru a dále je kladen důraz na vzdělávání a odborný růst v oblasti kybernetické bezpečnosti. Centrum kybernetických sil, které se postupně buduje a je součástí vojenského zpravodajství, nutně potřebovalo konzultace a pomoc při přípravě ICS (Industrial Control System) laboratoří pro řízení technologických celků.

Pro zvyšování kybernetické bezpečnosti jsou jedním z důležitých faktorů vzdělání a příprava budoucích odborníků, příprava a realizace kybernetických cvičení a sdílení informací a zkušeností. NBÚ mám jako partnera akademickou sféru, kde zejména úzce spolupracuje s Masarykovou univerzitou v Brně. V přípravě budoucích odborníků se NCKB podílí na výuce předmětů na vysokých školách. Kybernetická bezpečnost je přednášena na Přírodovědecké fakultě Univerzity Palackého v Olomouci a na Fakultě sociálních studií Masarykovy univerzity v Brně. Přehled VŠ studijních programů, oborů a předmětů vztahující se ke kybernetické bezpečnosti je uveden na webových stránkách Govcert.cz. [23]

3.3.5 Audit národní bezpečnosti

Z rozhodnutí Bezpečnostní rady státu vytvořilo Ministerstvo vnitra na začátku roku 2016 skupinu, jejímž úkolem bylo provést analýzu odolnosti České republiky proti bezpečnostním hrozbám a navrhnout opatření v nejrizikovějších oblastech. Ke konci roku byl vytvořen materiál obsahující deset témat, kde jedním z témat byly hrozby v kyberprostoru. Rozděleny byly do pěti konkrétních hrozeb ohrožujících bezpečnost ČR:

- Kybernetická špionáž,
- Narušení nebo snížení odolnosti IT infrastruktury
- Nepřátelské kampaně,
- Narušení nebo snížení bezpečnosti eGovernmentu,
- Kyberterorismus. [23]

3.3.6 Činnost vládního CERT týmu

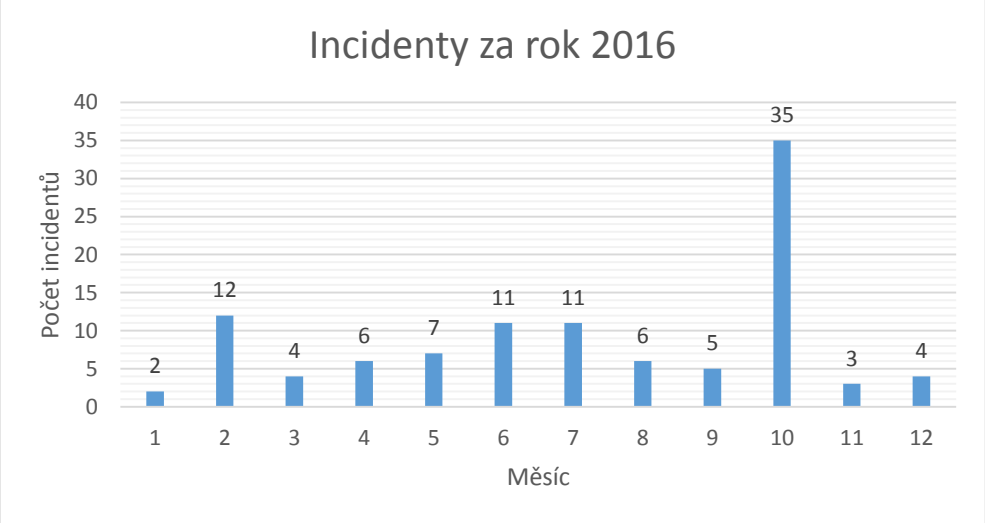
Předpokladem pro dobré fungováním CERT týmu jsou dostatečné odborné kapacity technického i personálního charakteru a vysoké nároky na analytické schopnosti při šetření bezpečnostních incidentů. Nedílnou součástí je také forenzní laboratoř poskytující nástroje a prostředí pro fyzické zajištění zařízení (paměťová média, mobilní telefony, počítače), analýzu těchto zařízení a zabezpečení citlivých materiálů dle potřebné úrovně zabezpečení. Spuštěna byla služba penetračního testování a příprava projektu schopnosti detekce kybernetických útoků ve státní správě. Význam vládního CERT týmu, jehož systém a funkce je popsána v teoretické části, bude každým rokem nabývat na významu.

V průběhu roku 2016 obdržel GovCERT.CZ tým celkem 298 věrohodných hlášení o bezpečnostních incidentech od českých i zahraničních partnerů. V oblasti působení tohoto týmu poté bylo vyhodnoceno, zpracováno a vyřešeno vlastními prostředky 106 kybernetických bezpečnostních incidentů spadající do KII, VIS a veřejné správy. Při řešení incidentů byl vždy kladen důraz na rychlé a včasné informovaní zodpovědných osob dotčených institucí a dohledání dalších možných potenciálních poškozených. Zpětná vazba některých dotčených institucí prokázala zabránění kybernetického útoku.

Vládní CERT tým dává souhrnné zdroje informací do zprávy o stavu kybernetické bezpečnosti, které má rozděleny do čtyřech čtvrtletí, dále pak uvádí nejvýznamnější incidenty v měsících v jednotlivých čtvrtletí, kde popisuje, jakým způsobem byl útok proveden a kdo byl cílem.

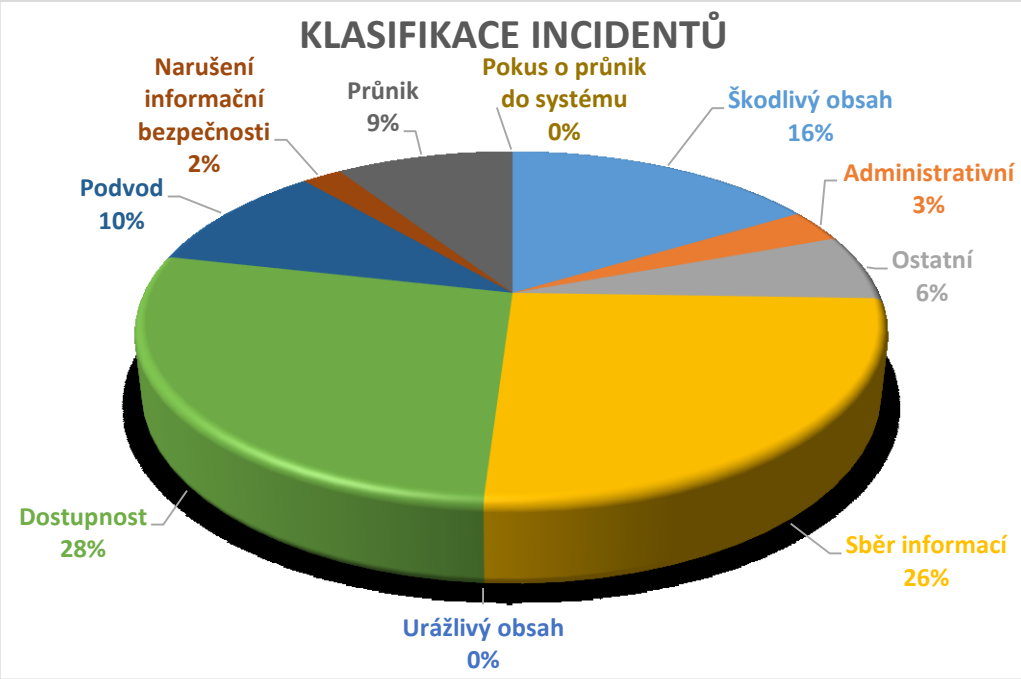
Graf 4 Počet příchozích hlášení o incidentech za jednotlivé měsíce v roce 2016

Zdroj: [23]



Graf 5 Počet řešených incidentů za jednotlivé měsíce v roce 2016

Zdroj: [23]



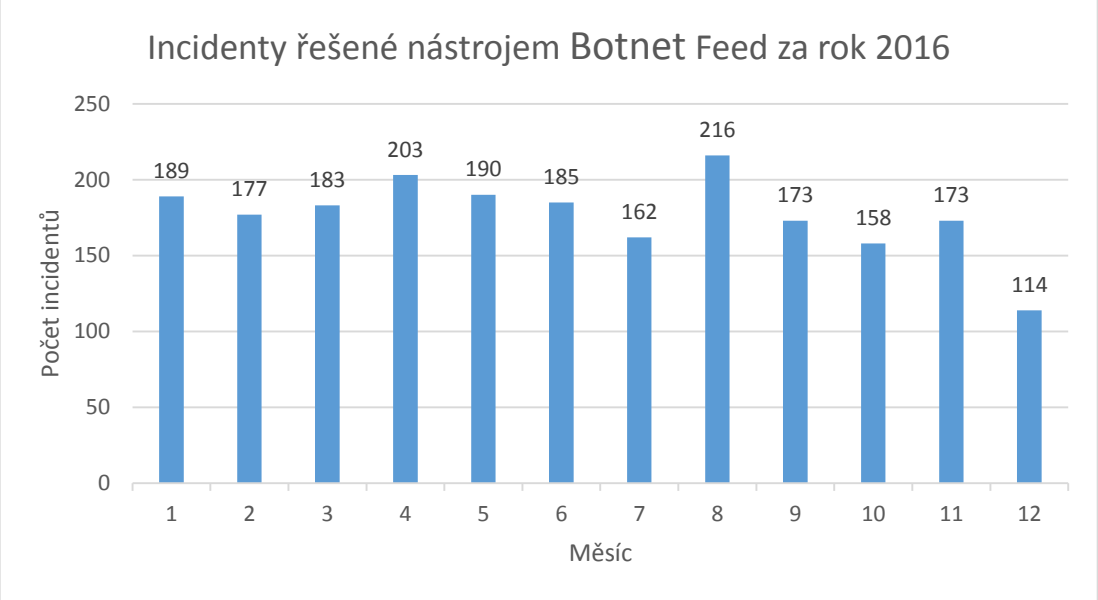
Graf 6 Klasifikace řešených incidentů za rok 2016

Zdroj: [23]

Popis kategorií vychází z formuláře pro hlášení incidentů (formulář hlášení je k dispozici na internetových stránkách GovCERT.CZ):

- Urážlivý obsah (např. spam, kyberšikana, nevhodný obsah),
- Škodlivý obsah (např. virus, červ, trojský kůň, dialer, spyware),
- Sběr informací (např. skenování, sniffing, sociální inženýrství),
- Pokus o průnik do systému (např. pokus zneužití zranitelnosti, kompromitace aktiva, "0-day" útok),
- Průnik (např. úspěšná kompromitace aplikace nebo uživatelského účtu),
- Dostupnost (např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží),
- Narušení informační bezpečnosti (např. neautorizovaný přístup nebo neautorizovaná změna informace, atd.),
- Podvod (např. phishing, neoprávněné využití ICT - porušení licenčních práv, krádež identity, aj.),
- Administrativní = tato kategorie se liší od kybernetických incidentů. Příkladem může být soudní rozhodnutí o vypnutí systému, který je součástí KII / VIS.

Při proaktivních činnostech o kompromitaci systémů, GovCERT.CZ získává a analyzuje data pomocí různých nástrojů, kde nejdůležitější je Botnet Feed. Ten je vyvíjen týmem GovCERT.CZ na sběr a zpracování dat o koncových stanicích zapojených do sítí botnetů, kdy data jsou získávána ze zajištěných řídících serverů. Původcem dat je společnost Microsoft. Denně se z těchto dat zpracovávají zprávy, které jsou určeny pro komerční sféru. Během roku 2016 bylo zpracováno a vyhodnoceno, jako potencionální bezpečnostní hrozba v ČR, přibližně 114,5 miliónů záznamů, ze kterých bylo odesláno 2123 reportů.



Graf 7 Počet incidentů za jednotlivé měsíce roce 2016

Zdroj: [23]

3.4 Vzdělávání v kybernetické bezpečnosti

Mezi hlavní činnosti Národního centra pro kybernetickou bezpečnost patří osvěta, podpora a vzdělávání v oblasti kybernetické bezpečnosti, které jsou popsány v kapitole 1.3.

Koncepce vzdělávání vydaná NCKB vycházející z dokumentů Strategie digitálního vzdělávání do roku 2020 (vzdělávání dětí, žáků a studentů), Strategie digitálního gramotnosti ČR na období 2015 – 2020 a dalších materiálů ne jen na vnitrostátní úrovni, která rozdělila přípravu a vzdělávání do dvou skupin.

Definované cílové skupiny obecného vzdělávání:

- Děti předškolního věku a žáci 1. stupně ZŠ,
- Žáci 2. stupně ZŠ,

- Žáci SŠ,
- Pedagogičtí pracovníci,
- Preventisté,
- Sociální pracovníci a pomáhající profesionálové,
- Odborná a zájmová sdružení,
- Rodiče,
- Senioři,
- Široká veřejnost.

Definované cílové skupiny specifického vzdělávání:

- Správci KII a VIS,
- Vysoké školy a akademická sféra,
- Veřejná správa,
- Policie ČR,
- Armáda ČR,
- Státní zástupci a soudci,
- Soukromý sektor,
- Pracoviště typu CERT a CSIRT (operátoři, analytici, specialisté),
- Administrátoři a bezpečnostní správci systémů a sítí. [13]

NCKB je garantem přípravy pro budoucí odborníky na kybernetickou bezpečnost, která je pak prezentována formou seminářů k zákonu o kybernetické bezpečnosti, školení zaměstnanců veřejné správy a v organizacích. Pro vysokoškolské studenty jsou pořádány stáže na NCKB, které jim pomohou rozšířit znalosti v oboru kybernetické bezpečnosti a ukázat základy pro použití v praxi. Vše je mířeno na získání budoucích pracovníků pro NCKB. V ČR se uskutečnil první ročník kybernetické soutěže pro střední školy, kdy cílem soutěže bylo zvýšení znalostí, poskytnutí podpory pro středoškolské pedagogy a objevení mladých talentů pro kybernetickou bezpečnost.

V činnost byla uvedena spousta projektů, mezi které patří zejména pilotní fáze interaktivního vzdělávacího modulu – digitální stopa. Zaměřena byla na problematiku rizikového chování a závadového jednání na internetu, kde mezi hlavní témata patřila kyberšikana, sexting a další sociálně patologické jevy. Hlavním zjištěním bylo nedostatečná znalost funkcí sociálních sítí a to hlavně s nastavením zabezpečení svých účtů a ochranou informací o své osobě. Obdobného typu, na závadové jednání a pravidla bezpečného chování na

internetu, je Školní diář, který je každoročně distribuován do škol po celé ČR. Projekt „Zvol si info“ si dává za cíl zvýšení mediální gramotnosti a podporu kritického myšlení, jako prostředku proti dezinformacím a mediální propagandě. [23]

3.5 Metodika k vodítkům pro hodnocení dopadů

Dokument sloužící k hodnocení dopadu narušení bezpečnosti informací u aktiv, informačních a komunikačních systémů, ICT služeb a k následnému řízení rizik. Obsahuje komentované vodítka pro hodnocení dopadu narušení bezpečnosti informací, které lze dále použít i pro posouzení systému, zda spadá pod působnost zákona o kybernetické bezpečnosti.

Účelem tohoto podpůrného materiálu je nabídnout:

- Hodnocení důležitosti informačních a komunikačních systémů,
- Hodnocení důležitost aktiv a s tím související řízení rizik,
- Odvození požadavků na bezpečnost zpracovávaných informací a informačních systémů,
- Nastavení jednotících kritérií dopadu narušení bezpečnosti informací (dostupnost, důvěrnost, integrita),
- Pomoc správcům informačních a komunikačních systémů se zařazením jejich systémů do správné kategorie podle zákona č. 205/2017 Sb., (zákona o kybernetické bezpečnosti) – tedy zařazení mezi významné informační systémy, informační či komunikační systémy kritické informační infrastruktury či informační systémy základní služby. [24]

Celá metodika je uvedena v příloze číslo I.

4 MOŽNOSTI MODELOVÁNÍ PREVENCE KRIMINALITY

V obecném měřítku se stává cílem preventivní práce v oblasti kriminality udržitelné chování jednotlivých členů společnosti v pomyslném rámci norem, hodnot a zvyků nastavených společností jako akceptovatelná. Tudíž by prevence měla usilovat o to, aby nedocházelo k závažnějšímu narušení těchto regulí. V samotné podstatě lze prevenci kriminality chápat jako intervenci realizovanou různými subjekty na různých stupních, kdy hlavní snahou je zabránění trestné činnosti dříve než k ní dojde, tedy kriminalitě předcházet.

4.1 OSN a Evropský kontext

Pravděpodobně každý stát má svůj systém prevence kriminality, ale také mezinárodní organizace se podílejí na řešení této problematiky. Organizace spojených národů (OSN) se už dlouhou dobu věnuje otázce prevenci kriminality a vychází z principů, které vyplývají z Všeobecné deklarace lidských práv a Charty OSN. Normy a standardy vytvořené OSN vycházejí nejen z těchto dokumentů. Kongresy OSN o prevenci kriminality a trestní justici sehrály významnou roli při přijímání a formulaci těchto norem. Kongresy se schází pravidelně v pětiletých periodách. [14]

4.1.1 Organizace spojených národů

Z nejvýznamnějších dokumentů, vytvořené OSN v problematice prevence kriminality, lze uvést tzv. Rijádskou směrnici (United Nations Guidelines for the Prevention of Juvenile Delinquency) – směrnice OSN pro prevenci delikvence mladistvých, a Směrnice pro prevenci kriminality (Guidelines for the Prevention of Crime).

Rijádská směrnice

Tato směrnice roku 1990 obsahuje obecná doporučení a klade důraz na prevenci kriminality u mládeže. Hlavní důraz je kladen na hloubkovou analýzu problému a vymezení zodpovědnosti jednotlivých subjektů, koordinaci aktivit a prognostických studiích, které musí být neustále sledovány a vyhodnocovány. K projektům by se měly přidat i metody minimalizující příležitosti pro páchání trestné činnosti. Hlavní úsilí by mělo být kladeno na přístupy usnadňující socializaci a integraci dětí a mladých lidí, pomocí rodiny, škol, komunity, a odborné přípravy.

Směrnice pro prevenci kriminality

Obsahuje obecné standardy pro předcházení trestné činnosti a vydána byla v roce 2002. Dobrá plánovaná strategie prevence kriminality a viktimizace vede ke zvýšení bezpečnosti a správnému rozvoji zemí, a to nejen na zvýšení kvality života občanů, ale také šetří finanční prostředky, které by byly vynaloženy na případný soudní proces a na další náklady spojené s odsouzením pachatele. Ve směrnici se rozumí, že prevence kriminality je strategie a souhrn opatření mající za výsledek snížení rizika výskytu trestného činu a negativního efektu na společnost. Směrnice je poměrně obecným dokumentem, ale obsahuje řadu konkrétních doporučení k organizaci, plánování, řízení a obsahu preventivních aktivit vycházejících z teoretických poznatků a praktických zkušeností. Pro kvalitní systém prevence je nevyhnutelné zapojení mnoha subjektů (státu, místní samosprávu, podnikatelský sektor a společnost v konkrétní oblasti). [14]

4.1.2 Evropský kontext

K zajištění ochrany občanů Evropské unie v rámci bezpečnosti, spravedlnosti a svobody slouží článek 29 Amsterdamské smlouvy, který se zabývá prevencí organizovaného a jiného zločinu z května 1999. Ze závěru zasedání v Tampere vyplynula potřeba vytvoření efektivních koncepcí prevence kriminality v EU. V květnu 2001 byla vytvořena Evropská síť prevence kriminality (EUCPN) a upravena v roce 2009. Je stálým orgánem zabývající se prevencí kriminality na evropské úrovni s cílem podpory aktivit na prevenci kriminality na místní i národní úrovni.

Do hlavních cílů patří:

- Vyhledávání osvědčených preventivních strategií a zprostředkování poznatků a zkušeností získaných členskými státy v oblasti prevence,
- Sběr a vyhodnocení dat z preventivních aktivit,
- Výměna informací v rámci sítě,
- Usnadnění spolupráce mezi členskými státy,
- Přínos k rozvoji preventivních strategií na místní a národní úrovni,
- Podpora aktivit pomocí organizování seminářů a konferencí v oblasti prevence kriminality. [14]

4.2 Příklady prevence kriminality

Teorie zabývající se příčinami a prevencí kriminality většinou vychází ze stejného základu. Různé teoretické postupy, i když jsou uvedeny jejich rozdíly, mají většinou velmi podobné rysy v praktických opatřeních a dají se aplikovat různé druhy kriminality popsané v kapitole 2.1.1. V každém jednotlivém programu nebo případu je žádoucí sledovat efektivnost a vyhodnocovat jeho působení abychom zjistili, zda zavedený program pracuje správně podle našeho očekávání. Proces hodnocení preventivní intervence se nazývá evaluace. Jde o systematický sběr, analýzu a interpretaci informací o účinnosti preventivní intervence a jejich dopadech. Získané informace jsou nadále zpracovávány a využívány při rozhodování o možnostech, jak intervenci zlepšit, rozšířit nebo ji ukončit. Základem úspěchu je dobře připravená a provedená evaluace, která je nositelem hodnověrných výsledků o tom, jak program doopravdy pracuje. Samozřejmě i samotná evaluace podléhá stejným kritériím. Při prevenci kriminality je, z hlediska typu užitého výzkumu, považovaný jako nejspolehlivější tzv. experimentální typ evaluace.

Experimentální evaluace předpokládá použití experimentální části (podrobila se intervenci) a kontrolní části (bez intervence) skupiny, která byla vybrána náhodným výběrem a porovnáváme (měříme) stav před a po provedení intervence, popřípadě i v jejím průběhu. Na závěr porovnáváme výsledky (rozdíly) u obou skupin. [14]

4.2.1 Negativní výsledky z vybraných příkladů

Program zvaný Scared Straight se dá použít jako reprezentativní příklad neefektivního typu. Vznikl v 70. letech v USA v New Jersey, kde hlavní podstatou je návštěva věznic organizované pro problémovou mládež. Ti se setkávají s odsouzenými vězni na doživotí, kteří je seznamují se životem zločince a jeho důsledcích. Hlavním cílem programu je zastrašování. Ukázka reálného vězeňského života má působit jako prevence před páchaním trestné činnosti a vyvolat strach z možného důsledku v podobě trestu. Přehledy evaluací tohoto typu programu ukázaly, že program více škodí, než pomáhá při prevenci. Z výsledných informací evaluace se ukázalo, že větší procento pachatelů páchajících trestnou činnost, pocházelo ze skupiny, která prošla programem, než ze skupiny, která se ho neúčastnila. I přes neefektivnost programu, jak se ukázalo z výsledků výzkumu, je program v USA nadále provozován, a snaha o jeho zrušení se setkala s velkým odporem. Jako jeden z dalších často uváděných neefektivních preventivních programů je program DARE (Drug Abuse Resistance Education). Program vytvořený na prevenci zneužívání návykových lá-

tek a násilné kriminality. Vytvořen byl na počátku 80. let v USA, a byl převzat do více než 50 zemí. Postaven byl na lektorské činnosti policisty, který učí žáky, jak odolávat tlaku svých vrstevníků a okolí. Program DARE, jako jeden z mála, byl podroben důsledné evaluaci. Program byl pozitivně hodnocen účastníky, ale nebyla prokázána efektivnost a snížení kriminality a zneužívání návykových látek mezi studenty. Skupiny, které prošly programem a skupina, která jím neprošla, vykazovala stejnou míru v užívání drog.

Ministerstvo zdravotnictví USA zařadilo program do kategorie neúčinných a vláda ho přestala finančně podporovat. Je podivuhodné, že program je nadále rozvíjen, s alibistickou výmluvou, že se alespoň něco dělá v oblasti prevence zneužívání návykových látek a kriminality. [14]

4.2.2 Účinné programy z vybraných příkladů

Nejvíce účinných programů se podařilo zrealizovat ve školním prostředí na snižování trestné činnosti u dětí.

Projekt efektivních škol (The Effective Schools Project) zavádí opatření na zlepšení srozumitelnosti pravidel a jednotnosti při jejich prosazování, spolupráce při učení, kontrola práce žáků, více mimoškolních aktivit, zvyšování motivace a účasti při volbě povolání.

Prevence šikanování byl jako projekt poprvé spuštěn v Norsku. Tento projekt dal oporu a poradenství učitelům, vytvořil pravidla, která jasně definovala šikanu, podporoval oběti a povzbuzoval je při oznamování šikany, zlepšil dohled při přestávkách mezi vyučováním a aktivně zapojil rodiče.

Americký program, který se zaměřuje na žáky první a druhé třídy základních škol, tzv. Hra na dobré chování (Good Behaviour Game). Cílem je pomoc dětem při adaptaci na školní prostředí a omezení agresivního chování. Touto strategií se prokazatelně dosáhlo výrazného zlepšení vztahů mezi žáky a snížení jejich agresivity. Upravenou verzi zavedlo 13 škol v Rotterdamu a Amsterdamu, kde byli žáci zapojeni do vytváření vlastních třídních pravidel a při možnostech společných odměn se aktivně podíleli na jejich dodržování. [14]

4.3 Strategie prevence kriminality v České republice na léta 2016 – 2020

Prevence kriminality v ČR je tvořena už od vzniku samostatné České republiky v roce 1993. První strategie prevence kriminality byla přijata v roce 1996 a od té doby se neustále vyvíjí a zdokonaluje systém prevence na celorepublikové a místní úrovni. Zúčastněny jsou

orgány státní správy i samosprávy, které se snaží neustále pracovat na zlepšení a rozvoji postupů a přístupů k řešení jednotlivých druhů kriminality.

Strategie má dané východiska z Programového prohlášení vlády ČR. Vláda se usnesla, že v oblasti prevence kriminality bude výhodnější se zaměřit na prevenci u mladistvých, dále poté vytvářet preventivní aktivity ve vybraných oblastech s nižší úrovní bezpečnosti. Strategie navazuje na další strategické obecné dokumenty vlády ČR ohledně vládní politiky nebo problematiky bezpečnosti, mezi které patří:

- Bezpečnostní strategie ČR,
- Strategie vnitřní bezpečnosti a ochrany obyvatelstva,
- Strategický rámec udržitelného rozvoje ČR.

Cíle a úkoly dané v každé strategii vychází z každoročního vyhodnocování preventivních aktivit a úkolů, spolupráce a sdílení informací všech členů Republikového výboru pro prevenci kriminality, krajských a obecních samospráv či neziskových organizací, které se věnují této problematice. Nedílnou součástí Strategie se pak stávají i poznatky z mezinárodní spolupráce. [25]

4.3.1 Globální cíl, strategické cíle a základní principy politiky prevence kriminality v České republice na léta 2016 až 2020

Moderní demokratické země, mezi které se řadí i Česká republika, pracují na zajišťování bezpečnosti a veřejného pořádku formou preventivních přístupů, ke kterým vytváří vhodné systémové, organizační i finanční předpoklady.

V současné době se Česká republika řadí mezi země s dobře rozvinutým a stabilním systémem prevence kriminality odpovídajícím mezinárodním standardům a doporučení. Plánování prevence je uskutečňováno v periodických 4 – 5ti letých cyklech prostřednictvím Strategie prevence kriminality. Globálním cílem se rozumí závazek, že v následujícím období bude ČR tento systém udržovat a posilovat. K zajišťování bezpečnosti a veřejného pořádku bude podporovat preventivní přístupy ve smyslu principů moderního demokratického státu.

Trend poklesu kriminality v naší zemi je důkazem dobře rozvinutého systému prevence a jeho dobré schopnosti efektivně reagovat na nově vnikající trendy a řešit je už v počátcích. U všech druhů kriminality registrované Policií ČR je vykazován meziroční pokles. Rok

2013 byl jedinou odchylkou ve statistikách, která je připisována nečekané amnestii prezidenta republiky, na kterou nebyly instituce připraveny.

4.3.2 Strategické cíle

Východiskem každé vydané strategie na další období se stávají úspěšné aktivity, navázání na dobrou praxi ze získaných zkušeností z nových poznatků a mezinárodních zkušeností z minulého období. Cílem pro českou republiku se stává:

- Rozvoj systému prevence, posílení spolupráce, kompetencí a kapacit partnerů, rozšíření prostoru pro dobrovolníky v oblasti zajištění bezpečnosti a veřejného pořádku, mezinárodní spolupráce a vědecké poznatky,
- Rozšíření a zkvalitnění pomoci a poradenství obětem trestné činnosti
- Předcházení recidivy, zlepšení začlenění pachatelů trestného činnosti zpět do společnosti, prevence kriminality u dětí a mládeže,
- Komplexní přístup v sociálně vyloučených lokalitách, kde má kriminalita hluboké kořeny,
- Reakce na nové trendy a hrozby a aplikace nových efektivních přístupů k jejich předcházení, [25]

4.4 Metodika pro tvorbu strategických dokumentů prevence kriminality a víceletých bezpečnostních analýz

Metodika je výstupem z úkolu, který vláda ČR nařídila Ministerstvu vnitra v rámci Strategie prevence kriminality v České republice na léta 2012 – 2015.

Je rozdělena do tří částí, problematika bezpečnostního auditu (analýzy), metodiky přípravy strategických dokumentů (koncepcí, plánů, strategií) prevence kriminality v obcích a krajích, poslední část se zaměřuje na způsoby a kritéria stanovování míry rizikovosti území ve vztahu k prevenci kriminality. [26]

Celá metodika je uvedena v příloze číslo IV.

4.5 Bezpečnostní analýza Moravskoslezského kraje pro rok 2017

Moravskoslezský kraj pracuje na zlepšení své bezpečnosti již řadu let. První bezpečnostní analýzu vytvořil v roce 2008, na podporu pro Koncepce prevence kriminality Moravskoslezského kraje na období 2009 – 2011. Každý rok aktualizuje svou bezpečnostní analýzu

pro vyhodnocení svého nastaveného systému prevence. Krajský program prevence kriminality se v současnosti označuje jako Program prevence kriminality na místní úrovni, jehož vyhlašovatelem je Ministerstvo vnitra. Moravskoslezský kraj pravidelně žádá o dotace, na realizaci projektu Programu prevence kriminality, které jsou podmíněny prováděním bezpečnostních analýz.

Bezpečnostní analýza Moravskoslezského kraje pro rok 2017, byla zpracována na základě Metodiky pro tvorbu strategických dokumentů prevence kriminality a víceletých bezpečnostních analýz. Metodiku vydal Odbor bezpečnostní politiky a prevence kriminality Ministerstva vnitra České republiky. Bezpečnostní analýza musí obsahovat podle požadavků metodiky statistická data k trestné činnosti v kraji, a to v porovnání mezi roky 2015 a 2016. Moravskoslezský kraj ještě připojil data k počtu obyvatel, nezaměstnanosti a další vybrané jevy a to z důvodu celkového přehledu o bezpečnostní situaci v kraji. Na vytvoření analýzy byly použity následující dokumenty:

- Zpráva o situaci v oblasti vnitřní bezpečnosti a veřejného pořádku na území ČR v roce 2016 ve srovnání s rokem 2015 – podklady za Moravskoslezský kraj,
- Bezpečnostní analýza Moravskoslezského kraje (aktualizace 2016),
- Závěrečná zpráva z výzkumu pocitu bezpečí občanů MS kraje [27]

4.5.1 Moravskoslezský kraj

Z mezinárodního pohledu kraj sousedí na severu a východě s Polskem a na jihovýchodě se Slovenskem. Na území České republiky sousedí s Olomouckým a Zlínským krajem. Součástí Moravskoslezského kraje jsou 4 euroregiony – Beskydy, Praděd, Silesia, Těšínské Slezsko.

Kraj v počtu obyvatel 1 210 849 se umístil na třetím místě v ČR a svou rozlohou zaujímá 6,9 % z rozlohy České republiky a řadí se tak na 6. místo mezi kraji. Územně je vymezen šesti okresy (Bruntál, Frýdek-Místek, Karviná, Nový Jičín, Opava a Ostrava-město). Většina obyvatel kraje (téměř 60 %) žije ve městech nad 20 tisíc obyvatel, a to je v rámci ČR rarita. V pořadí nezaměstnanosti obsadil kraj druhou příčku s hodnotou 7,14 procent. [27]

4.5.2 Zajištění prevence kriminality institucemi

Prevence kriminality se v Moravskoslezském kraji věnují územní samosprávy, neziskové organizace a další instituce. Aktivně se zapojuje do problematiky prevence a podporuje aktivity spojené s předcházením kriminality. Jednotlivé odbory vzájemně spolupracují a

předávají si poznatky se specialisty z jednotlivých oblastí. Zapojuje se krajský manažer prevence kriminality, krajský školský koordinátor prevence, krajský protidrogový koordinátor, krajský metodik sociální prevence, krajský koordinátor pro národnostní menšiny a romské záležitosti a další zúčastněné osoby v rámci krajské pracovní skupiny v oblasti prevence kriminality.

Samotné obce v kraji se také podílejí na realizaci projektů v rámci prevence na lokální úrovni, kdy tyto činnosti zajišťují vedoucí pracovníci, velitelé městských policií nebo místní manažeři prevence kriminality. V neposlední řadě se podílí na systému prevence i neziskové nebo soukromé organizace věnující se ohroženým dětem a mládeži. Provozují programy pro mladistvé a mladé pachatele trestné činnosti, programy pro oběti trestné činnosti nebo poradenství. [27]

4.5.3 Analýza kriminality Moravskoslezského kraje

Trestná činnost je zaznamenávána pomocí informačního systému, který je schopen sledovat vývoj trestné činnosti z jednotlivých územních odborů až k jednotlivým obvodním oddělením policie.

Hlavní kriminogenní faktory jsou dlouhodobé a neměnné:

- příhraniční poloha (fluktuace kriminálně rizikových osob ze sousedních teritorií i států),
- vysoká míra nezaměstnanosti,
- sociálně vyloučené lokality,
- vysoký počet burz, zastaváren a bazarů (nekontrolovatelný pohyb zboží),
- vysoký podíl obyvatelstva s nízkým právním vědomím a nižší úrovní vzdělanosti
- průmyslové a obchodní zóny,
- velký počet kulturních, společenských a sportovních akcí (velký počet návštěvníků, kteří se sjíždějí z celé republiky i ze zahraničí),
- vysoký podíl recidivistů na objasněné trestné činnosti,
- zvyšující se počet trestných činů páchaných prostřednictvím internetu,
- zvyšující se množství přestupků v dopravě spojených s řízením pod vlivem alkoholu a drog.

Tabulka 1 Kriminalita v Moravskoslezském kraji v porovnání s ČR za rok 2016

	ČR – POČET	ČR – V %	MS KRAJ – POČET	MS KRAJ– V %	ODCHYLKA (V %) MS KRAJ – ČR
CELKOVÁ TČ	218 432	100	26 528	12,26	XXX
Z TOHO:					
MAJETKOVÁ	118 218	54,1	14 483	54,6	+ 0,5
NÁSILNÁ+ MRAVNOSTNÍ	16 494	7,6	2 560	9,7	+ 2,1
OSTATNÍ KRIMINALITA	25 613	11,7	2 922	11	-0,7
ZBÝVAJÍCÍ KRIMINALITA	29 246	13,4	3 809	14,4	+1
HOSPODÁŘSKÁ	28 396	13	2 754	10,3	-2,7
VOJENSKÁ	10	0,2	0	0	-0,2

Zdroj: [27]

V roce 2016 se objasněnost trestných činů pohybuje za hranicí 50 % a škody přesáhly více než 1,68 miliardy Kč. Celkem 14 678 osob bylo stíháno za protiprávní jednání, kdy ženy tvořily 15,2 % (2 237) ze všech osob.

Recidivu se v kraji dlouhodobě nedaří zvládnout, která je stabilně větší o 10 % než jinde v České republice. U recidivistů se počet stíhání vyšplhal na 57,8 % (8 477) a spáchali 69,8 % z objasněných trestných činů.

V roce 2016 se stalo obětmi kriminality celkem 4 527 osob a to je o 497 méně než v loňském roce. Kriminalita byla páchána více na mužích než na ženách, kdy obětmi trestné činnosti se stalo 2 473 mužů a 2 054 žen.

Trestných činů za rok 2016 bylo v Moravskoslezském kraji spácháno celkem 26 528, kdy podstatná většina (11 187) se stala v okrese Ostrava-město a nejméně jich bylo provedeno v okrese Bruntál (1 674).

Tabulka 2 Kriminalita v okresech Moravskoslezského kraje v letech 2015 a 2016

OKRES	POČET REGISTROVANÝCH TRESTNÝCH ČINŮ - 2015	POČET REGISTROVANÝCH TRESTNÝCH ČINŮ - 2016	ROZDÍL 2015 A 2016
BRUNTÁL	1 858	1 674	- 174
FRÝDEK-MÍSTEK	3 812	3 437	- 375
KARVINÁ	6 331	5 295	- 1 036
NOVÝ JIČÍN	2 657	2 325	- 332
OPAVA	2 957	2 402	- 555
OSTRAVA - MĚSTO	12 479	11 187	- 1 292

Zdroj: [27]

Z přehledu statistik v rámci Moravskoslezského kraje je patrné, že roku v 2016 došlo k celkovému úbytku spáchaných trestných činů v celém kraji, ale také i v jednotlivých okresech. Nejvyšší úbytek byl zaznamenán v okresech Ostrava-město a Karviná. Kraj přes pokles celkové kriminality, vykazuje v porovnání s celorepublikovým průměrem, výrazně vyšší počet zaregistrovaných činů násilné kriminality, kde se podílí 16,2 % na násilné trestné činnosti v České republice. Mezi významný problematický faktor při páchání kriminality v Moravskoslezském kraji se považuje jeho příhraniční oblast se sousedící Polskou a Slovenskou republikou. [27]

4.6 Koncepce prevence kriminality Moravskoslezského kraje na období 2017 – 2021

Při zpracování nové Koncepce prevence kriminality Moravskoslezského kraje na období 2017 – 2021 se vychází z dokumentů vydaných ČR a z dalších materiálů vytvořených již dříve pro Moravskoslezský kraj. Mezi tyto dokumenty patří:

- Strategie prevence kriminality v ČR na léta 2016 až 2020,
- Akčního plánu prevence kriminality na léta 2016 až 2020,
- Program prevence kriminality,
- Strategie protidrogové politiky Moravskoslezského kraje na období 2015 – 2020,
- Strategie integrace romské komunity Moravskoslezského kraje na období 2015 – 2020,
- Strategie prevence rizikového chování u dětí a mládeže v Moravskoslezském kraji na období 2013 – 2018,
- Střednědobý plán rozvoje sociálních služeb Moravskoslezského kraje na období 2015 – 2020. [28]

Příprava Koncepce prevence kriminality pro Moravskoslezský kraj, zahrnuje nejen směry prevence, objekty a opatření prevence kriminality. Dodržuje také model prevence kriminality v ČR

4.6.1 Výzkum pocitu bezpečí občanů

Jako podkladový materiál pro vytvoření nové Koncepce prevence kriminality Moravskoslezského kraje na období 2017 – 2021 byl využit Výzkum pocitu bezpečí občanů Moravskoslezského kraje. Výzkum probíhal v měsících březnu až září roku 2016 ve všech 22

obcích s rozšířenou působností v kraji. Pro výběr respondentů byly stanoveny tři věkové kategorie 15 až 19 let (5,5 %), 20 až 64 let (74 %), víc jak 65 let (20,5 %), kde v jednotlivých věkových kategoriích byl výběr náhodný. Výběr respondentů, tak odrážel reálnou věkovou strukturu obyvatel. Celkem bylo dotázaných 1222 občanů Moravskoslezského kraje, mezi nimiž převažovaly mírně ženy nad muži, které tvořily 56,4% oslovených. Z hlediska vzdělanostní struktury, kdy byli osloveni respondenti jak se základním, středoškolským i vysokoškolským vzděláním, uvedl nejvyšší podíl respondentů jako nejvyšší dosažené středoškolské vzdělání a to v podílu 40,4%. Realizátorem byla Fakulta sociálních studií Ostravské univerzity. Celé znění dotazníku výzkumu je uvedeno v příloze číslo III.

4.6.2 Výstupy z výzkumu

Koncepce uvádí vybrané výstupy z výzkumu:

- Na otázku, zda lidé považují MS kraj za nebezpečný kraj, odpověděli respondenti v největší míře (přes 50%), že jej vnímají jako „spíše bezpečný“, a to bez ohledu na jejich pohlaví, věk, či vzdělání. Rozdíly bylo možné spatřovat pouze v názorech v rámci jednotlivých ORP, kdy např. v ORP Karviná, Orlová a Vítkov byly shodně označeny varianty „spíše bezpečný“ a „spíše nebezpečný“ (cca kolem 40%), ve variantě odpovědi „rozhodně nebezpečný“ pak největšího podílu dosáhlo ORP Ostrava a Vítkov (v podílu 9,1%). Naopak za „rozhodně bezpečný“ považují v největší míře respondenti z ORP Bohumín, Opava a Rýmařov (přes 10%),
- Na otázku, která místa lidé považují v MS kraji za nebezpečná, se objevily mj. i obecnější definice jako např. nádraží, romská ghetta, parky, neosvětlené ulice či odlehlá zákoutí nebo fotbalová utkání,
- Z hlediska vybraných oblastí majících vliv na kriminalitu vyplynulo ze získaných odpovědí, že největší vliv na kriminalitu má nezaměstnanost a sociální a ekonomická situace (shodně cca 40% odpovědí) nejmenší vliv má naopak zdravotnictví (cca 32%) a životní prostředí (cca 26%),
- Jako nejefektivnější opatření k prevenci kriminality, lidé vyhodnotili přítomnost policie v ulicích a pouliční osvětlení (cca 24%). Téměř 20% odpovědí obdržel také kamerový systém,
- U otázky, zda se dotazovaní stali někdy obětí trestné činnosti, převážili z hlediska pohlaví muži nad ženami v poměru 43,0% ku 38,3%, z pohledu věkové kategorie

se nejčastěji jednalo o osoby ve věku 20 až 64 let. Z hlediska ORP, do které spadá bydliště respondenta, vyšlo najevo, že nejvíce obětí trestného činu pochází z ORP Ostrava, Havířov, Opava, Frenštát pod Radhoštěm a Kopřivnice, naopak obětmi trestného činu se dle odpovědí respondentů nikdy nestali obyvatelé z ORP Bílovec, Hlučín a Český Těšín,

- V případě, že se již stali oběti nějakého protiprávního jednání, se nejčastěji dotazovaní obraceli na Policii ČR (cca 36% odpovědí) a rodinu či příbuzné (cca 20% odpovědí),
- Z výzkumu vyplývá, že 76,4% respondentů používá nějaká opatření pro zvýšení své bezpečnosti. U otázky zaměřené na to, jaká opatření ke zvýšení vlastní bezpečnosti respondenti používají, bylo oběma pohlavími shodně nejčastěji uváděno důsledné zamykání domu či bytu (cca 25% odpovědí) a nevpouštění cizích osob do bytu (cca 12%). K nejméně používaným opatřením naopak patří vlastnictví střelné zbraně (cca 1%). Stejných výsledků bylo dosaženo také v případě dělení respondentů dle věku. [28]

4.6.3 Hlavní cílové skupiny Koncepce

Opatření uvedené v Koncepci prevence kriminality Moravskoslezského kraje na období 2017 – 2021 budou směřována především k obyvatelům kraje, ale budou také zaměřena na návštěvníky, kteří do kraje přijedou a chtějí se cítit bezpečně. Koncepce si stanovuje cílové skupiny, na které bude kladena větší pozornost:

- zvlášť zranitelné oběti (děti, senioři, osoby ohrožené mravnostní kriminalitou a domácím násilím, osoby se zdravotním postižením),
- pachatelé TČ (děti mladší 15 let, které se dopustily činu jinak trestného, mladiství, kteří se dopustili provinění, recidivisté),
- osoby jako potencionální pachatelé nebo oběti (děti a mládež ohrožené společensky nežádoucími jevy, děti s nařízenou ústavní výchovou a uloženou ochrannou výchovou, osoby opouštějící zařízení pro výkon ústavní nebo ochranné výchovy anebo pěstounskou péči, osoby propuštěné z výkonu trestu odnětí svobody, osoby bez přístřeší, dlouhodobě nezaměstnaní, osoby ohrožené dluhy anebo sociálním vyloučením, obyvatelé SVL, osoby ohrožené závislostmi a závislostním chováním, multiproblémové rodiny, osoby s rizikovým chováním nebo radikálové),

- pracovníci působící v oblasti prevence kriminality (manažeři prevence kriminality, kurátoři pro děti a mládež a dospělé, obecní i státní policisté a další odborníci pracující s cílovými skupinami Koncepce. [28]

4.6.4 SWOT analýza Moravskoslezského kraje

Na vymezení silných a slabých stránek a také hrozeb a příležitostí se podíleli členové krajské pracovní skupiny prevence kriminality, manažeři prevence kriminality obcí s pověřeným obecním úřadem. V analýze je také brán zřetel na požadavky Strategie prevence kriminality v ČR na léta 2016 – 2020 a výsledky z dotazníkového výzkumu pocitu bezpečí občanů.

SILNÉ STRÁNKY	SLABÉ STRÁNKY
– dlouhodobá existence strategie prevence kriminality v ČR včetně programu prevence kriminality – zvýšený počet policistů – zvýšení objasněnosti TČ – komunikace mezi manažery prevence kriminality obcí – existence platformy pracovní skupiny prevence kriminality na úrovni kraje/města včetně zastoupení odborníků – podpora prevence kriminality ze strany vedení kraje/města	- absence legislativního ukotvení prevence kriminality - neexistence definice bytové politiky - nárůst recidivistů jako pachatelů TČ - nedostatečná finanční podpora prevence kriminality z rozpočtu obcí - nedostatek policistů a strážníků - nedostatečná/nefunkční meziresortní spolupráce - nízká udržitelnost preventivních projektů a převažující jednoleté projekty
PŘÍLEŽITOSTI	**HROZBY**
– finanční podpora prevence kriminality včetně využití zdrojů z evropských fondů – snížení nezaměstnanosti – zvýšení informovanosti občanů – legislativní změny (soc. dávky, zaměstnanost, drogy, zastavárny aj.) – příklady dobré praxe a výměna zkušeností a příkladů dobré praxe (z ČR i ze světa) – víceleté projekty včetně jejich financování	– nové způsoby páchání TČ – dlouhodobá nezaměstnanost a nárůst závislostí – změna významu role rodiny ve společnosti – demografická struktura a charakter území MS kraje – odliv odborníků působících v oblasti PK – vznik nových soc. vyloučených lokalit – bagatelizace prevence kriminality ze strany politiků – společenské změny v Evropě – vysoká míra recidivy pachatelů

Obrázek 2 SWOT analýza Moravskoslezského kraje

Zdroj: [28]

4.7 Plán prevence kriminality města Bruntál na léta 2016 – 2018

Prevenci kriminality ve městě Bruntál je prováděna v samostatné působnosti, kterou má na starost Městský Úřad Bruntál v zastoupení odboru sociálních věcí, pomocí metody komunitního plánování. [16]

4.7.1 Východiska plánu

Základní dokumenty pro tvorbu programu prevence kriminality města Bruntál na období 2016 – 2018 jsou:

Strategie prevence kriminality v České republice na období 2012 – 2015

V době tvorby plánu, nebyla vydána nová Strategie prevence v ČR na období 2016 – 2020, která byla vydána až v lednu 2016 prostřednictvím Ministerstva vnitra ČR.

Vybrané strategické materiály Moravskoslezského kraje

Plán PK města Bruntál na rok 2016 navazuje na cíle a výsledky vybraných dokumentů:

- Koncepce prevence kriminality Moravskoslezského kraje na léta 2012 – 2016,
- Strategie protidrogové politiky Moravskoslezského kraje na období 2015 – 2020,
- Strategie integrace romské komunity Moravskoslezského kraje na období 2015 – 2020.

Vybrané strategické materiály města Bruntál

- Sociodemografická studie Bruntálu (DRAGON 2 od měření k řešení),
- IV. Komunitní plán rozvoje sociálních služeb 2015 – 2017,
- Analýza výskytu rizikového chování adolescentů 2014,
- Analýza Substance use risk profile scale 2014 (škála osobnostních rysů představujících riziko z hlediska užívání návykových látek),
- Programy prevence rizikového chování pro základní a střední školy města Bruntál,
- Analýza sociálně vyloučených osob – Bruntál 2014. [16]

4.7.2 Bezpečnostní analýza města Bruntál

Město Bruntál má rozděleno bezpečnostní analýzu do tří částí:

Protiprávní analýza – vývojové trendy trestné činnosti a přestupků

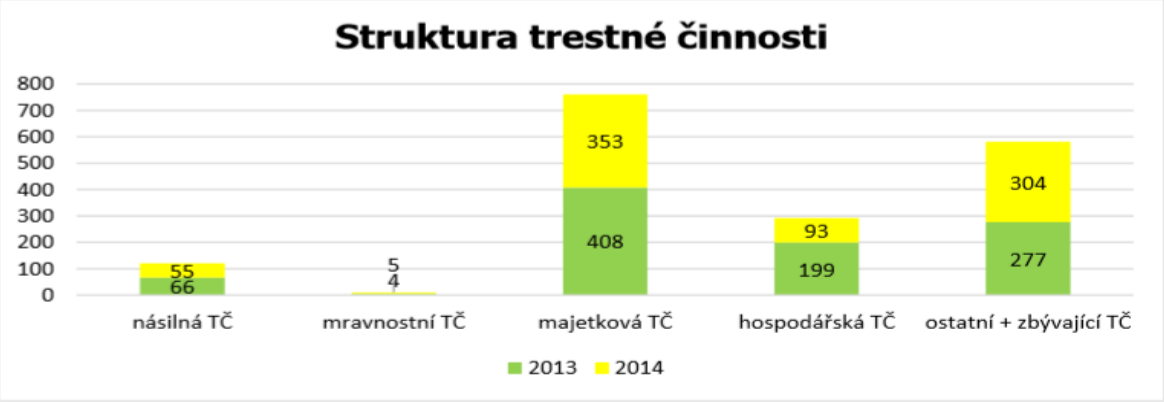
Vývoj trestné činnosti byl zpracován na základě dat z obvodního oddělení PČR, která jsou z období 2013 a 2014.

Tabulka 3 Kriminalita v městě Bruntál

	počet obyvatel města Bruntál			počty kriminality			index na 10 tis. obyv.		
druhy kriminality	k 1.1.2014	k 1.1.2015	změna oproti roku 2013	2013	2014	změna oproti roku 2013	2013	2014	změna 13 - 14 (index)
násilná TČ	17.298	17.160	-138	66	55	**-11**	38,15	32,05	**-6,1**
mravnostní TČ				4	5	**1**	2,31	2,91	**0,6**
majetková TČ				408	353	**-55**	235,87	205,71	**-30,16**
krádeže prosté/krádeže vloupáním				184/164	191/121	**7/-43**	106,37/ 94,81	111,31/70,51	**4,94/-24,3**
zbývající TČ (zanedbání povinné výživy, ohrožení pod vlivem návykové látky,..)				174	207	**33**	100,59	120,63	**20,04**
ostatní TČ (např. i **drogová TČ**, maření výkonu úředního rozhodnutí, výtržnictví,..)				103 z toho **25 DTČ**	97 z toho **26 DTČ**	**-12**	59,54/14,45	56,53/15,15	**3,01 0,7**
hospodářská TČ				199 (pozn. Kyperské fondy)*	93	**-106**	115,04	54,2	**-60,84**
celkový počet trestných činů				**955**	**810**	**-145**	552,09	472,03	**-80,06**
objasněnost				**60,63%**	**57,65%**				

Celková trestná činnost je sumář všech trestných činů spáchaných na území města Bruntál.
* Kyperské fondy – zvýšený počet úvěrových podvodů.

Zdroj: [16]



Graf 8 Struktura trestné činnosti

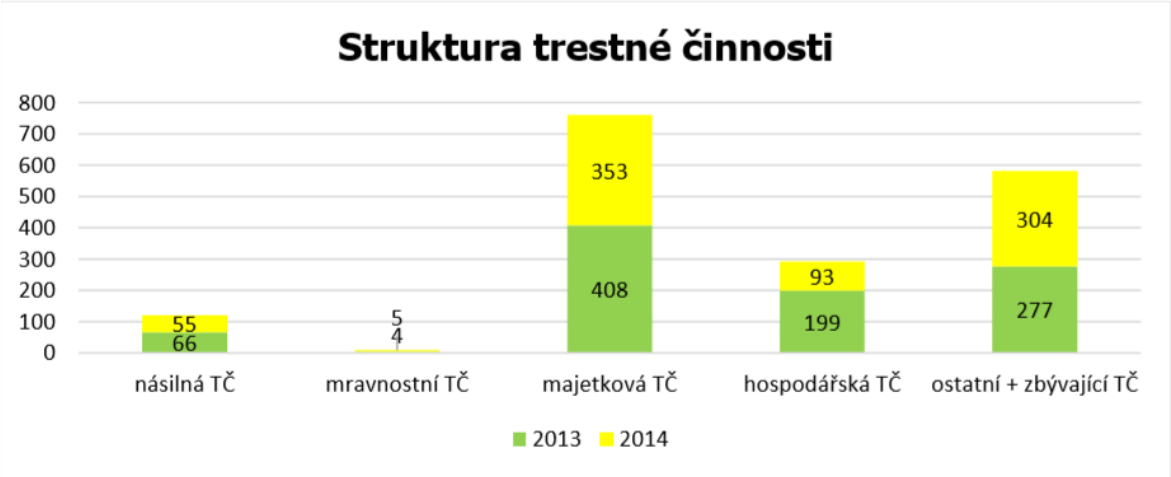
Zdroj: [16]

Tabulka 4 Pachatelé trestné činnosti

	počet obyvatel města Bruntál						index na 10 tis. obyv.		
pachatelé	k 1.1.2014	k 1.1.2015	změna oproti roku 2013	2013	2014	změna oproti roku 2013	2013	2014	změna 13 - 14 (index)
stíháno osob	17.298	17.160	-138	512	389	-123	295,99	226,69	-69,3
recidivisti				378	300	-78	218,52	174,83	-43,69
nezletilí				10	8	-2	5,78	4,66	-1,12
mladiství				22	12	-10	12,72	6,99	-5,73
ženy				102	69	-33	58,97	40,21	-18,76

Trestná činnost nezletilých dětí a mladistvých byla zaznamenána především u majetkové TČ.

Zdroj: [16]



Graf 9 Struktura trestné činnosti

Zdroj: [16]

Sociálně-demografická analýza – rozbor vybraných ukazatelů (vývoj nezaměstnanosti, chudoba)

Město Bruntál leží v Moravskoslezském kraji a je centrem okresu Bruntál. Z historického pohledu se jedná o jedno z nejstarších měst na území České republiky. Nachází se v oblasti Nízkého Jeseníku přibližně 55 km od Olomouce. V okolí města byla významná těžba drahých kovů. Bruntál se dlouhodobě potýká s vyšší mírou nezaměstnanosti, než celorepublikový průměr. Celková míra nezaměstnanosti v městě a okolních obcí se zastavila v prosinci 2014 na 14,9 procentních bodech.

Tabulka 5 Vývoj nezaměstnanosti v obci Bruntál

Rok 2014	6/2014		7/2014		8/2014		9/2014		10/2014		11/2014		12/2014	
	UoZ	PNO v %	UoZ	PNO v %	UoZ	PNO v %	UoZ	PNO v %	UoZ	PNO v %	UoZ	PNO v %	UoZ	PNO v %
Bruntál	1 785	14,5	1 821	14,8	1 811	14,7	1 799	14,6	1 772	14,3	1 749	14,1	1 846	15,0

Rok 2015	1/2015		2/2015		3/2015		4/2015		5/2015	
	UoZ	PNO v %	UoZ	PNO v %	UoZ	PNO v %	UoZ	PNO v %	UoZ	PNO v %
Bruntál	1 830	14,9	1 814	14,6	1 791	14,5	1 676	13,6	1 619	13,3

Zdroj: [16]

Dalším problémem, se kterým se musí město potýkat, je existence tzv. vyloučených lokalit. Na území obce jsou v současné době dvě sociálně vyloučené lokality. V západní části města, která je tvořena třemi ulicemi (Dlouhá, Pěší, Rýmařovská), žije přibližně 1636 osob z toho 25 % je romská populace. Druhou lokalitou je tzv. Jižní. Jedná se o ubytovnu v soukromém vlastnictví, kde žijí osoby bez trvalého pobytu na území Bruntálu a většinou se přistěhovali z oblastí Vítkova, Opavska a Vyškova.

Institucionální analýza – se zaměřením na činnost subjektů působících v oblasti prevence kriminality a prevence sociální

Ve městě Bruntál působí veliké množství subjektů zabývající se sociální prevencí a prevencí kriminality. Pro základní přehled můžeme uvést Městský úřad Bruntál, Městská policie Bruntál, obvodní oddělení policie, Junák (svaz skautů a skautek), Drom (romské středisko), azylové domy, a terénní služby.

4.7.3 SWOT analýza prevence kriminality města Bruntál

Analýza byla zpracována na území města Bruntálu pro zjištění faktorů ovlivňující oblast prevence kriminality, kterou provedli pracovní skupiny sociální prevence.

SILNÉ STRÁNKY	SLABÉ STRÁNKY
Snaha a zájem řešit problémy prevence kriminality. Existence Komunitního plánu, Plánu prevence kriminality a Plánu protidrogové politiky. Aktivní zájem MSK při řešení problematiky PK. Podpora MSK při schvalování finančních prostředků pro město a oblast PK (DOTACE). Zájem samosprávy o oblast PK v obci. Činnost pracovní skupiny prevence kriminality. Existence služeb NNO se zaměřením na PK (Open House, LIGA). Vytvoření nabídky primárně-preventivních programů pro školy a školská zařízení s nabídkou odborných preventivních programů. Vzdělaný a kvalifikovaný personál v NNO v oblasti PK. Úspěšnost obce v dotačních řízeních Ministerstva vnitra ČR. Existence městského kamerového dohlížecího systému. Funkční systém preventivních programů ze strany Policie ČR – ucelená nabídka preventivních programů pro zájemce zveřejněná na stránkách www.policie.cz Pokles trestné činnosti o 15%. Funkční systém veřejné služby v obci. Dostatečná nabídka volnočasových aktivit. Spolupráce mezi MěP a PČR.	Nemožnost zapojení obcí do některých vyhlášených dotačních řízení (př. MŠMT). Velmi úzké vymezení účelu pro poskytování investičních dotací ze strany MV. Nedostatečné informování široké veřejnosti v oblasti PK. Nízká schopnost zaměstnatelnosti ze sociálně vyloučené lokality. Nízká úroveň občanské spoluúčasti. Nedostatek asistentů škol pro individuální práci s dětmi, které mají výchovné problémy. Nárůst zbývající trestné činnosti o 18% - např. zanedbání povinné výživy, ohrožení pod vlivem návykové látky apod.
PŘÍLEŽITOSTI	**HROZBY**
Rozšíření možnosti zapojení obcí do vyhlášených dotačních řízení. Možnost financování a dofinancování projektů PK s využitím finančních prostředků z fondů EU. Využití stávajícího potenciálu nízkoprahových zařízení pro děti a mládež – dostupnost, kvalita. Zefektivnění spolupráce škol a školských zařízení s obcí v oblasti PK. Zvýšit informovanost obyvatel. Zapojení rodičů do programů PK. Plánované zapojení se do projektu forenzního značení jízdních kol.	Nedostatek a snižování finančních prostředků na programy PK. Pasivní účast škol a školských zařízení na řešení otázky PK. Vysoká nezaměstnanost obyvatel. Vysoká tolerance společnosti k sociálně nežádoucím jevům. Nadměrné zadlužování obyvatelstva. Majetková trestná činnost v souvislosti s nezaměstnaností a zadlužeností obyvatel. Zvýšení protiprávního jednání v souvislosti s požitím návykových látek – zejména řízení pod vlivem OPL a trestná činnost na úseku toxi problematiky (distribuce OPL).

Obrázek 3 SWOT analýza

Zdroj: [16]

4.7.4 Program prevence kriminality města Bruntál na období 2016 – 2018

Plán města na prevenci kriminality musí dodržovat a vycházet z cílů a priorit dle Strategie prevence kriminality v ČR. Město Bruntál si určilo hlavní cíle a zároveň představilo cílové skupiny, na které se bude zaměřovat v tomto období:

Hlavní cíle:

- snížení výskytu delikventní činnosti u cílových skupin nebo jejich ochrana,
- zvýšení bezpečí na veřejných prostranstvích,
- oslabování rizikových faktorů, které přispívají k výskytu delikventního jednání,
- vytvoření efektivního a stálého systému sběru, předávání a poskytování informací v oblasti prevence kriminality na jednotlivých úrovních i mezi všemi úrovněmi subjektů prevence kriminality.

Cílové skupiny:

Děti a mládež

Všechny projekty zaměřené na děti a mládež budou v souladu s principy projektu Systém včasné intervence v rámci aktivit Týmu pro děti a mládež (TDM), s jeho souhlasem nebo podle lokální strategie práce s rizikovými a ohroženými dětmi; jedná se např. o:

- projekty zaměřené na vyhledávání kriminálně rizikových dětí,
- projekty zaměřené na efektivní práci s kriminálně rizikovými dětmi s ověřovanými výstupy,
- projekty zaměřené na vyhledávání a efektivní práci s kriminálně rizikovými mladými dospělými.

Rodiny (s rizikem výskytu kriminálního chování u jejich členů)

- projekty zaměřené na konkrétní a efektivní podporu uvedených rodin, podmínkou je, aby v rodině bylo alespoň jedno kriminálně rizikové dítě, případně chování rodičů bylo kriminálně rizikové,
- projekty sanace těchto rodin,
- projekty zaměřené na efektivní spolupráci školy a rodiny (charakteristika rodiny viz výše).

Recidivisté (efektivní resocializace recidivujících pachatelů)

- projekty psychosociální a materiální podpory osob po návratu z VTOS,
- reintegrace do společnosti,
- projekty spolupráce věznic, sociálních odborů a organizací poskytujících podporu.

Oběti trestných činů

projekty zaměřené na skutečnou a efektivní pomoc a podporu, zejména prevenci viktimity) se zvláštním zřetelem na dětské oběti a seniory (zejména žijící osaměle, s omezenými sociálními kontakty

- komplexně pojaté projekty zaměřené na vyhledávání ohrožených seniorů a kontinuální práci s nimi, včetně informovanosti, zlepšování sociálních kontaktů a osobní bezpečnosti.

Komunity

Projekty a aktivity určené zejména pro obecní komunity jsou zaměřené např. na zvyšování odpovědnosti komunit za vlastní bezpečnost ve smyslu větší všímavosti, vzájemné informovanosti, zlepšení spolupráce s Policií ČR. [16]

4.8 Dílčí závěr praktické části

Bezpečnost v České republice má vzrůstající tendenci, která je výsledkem nastaveného, udržitelného a adaptabilního systému prevence kriminality i kybernetické bezpečnosti. Důležitou roli hrají národní strategie vycházející ve střednědobých horizontech, které mohou adekvátně reagovat na různé tendence a hrozby ohrožující stát. Komplexnost dobře fungujícího sytému je závislá na součinnosti a spolupráci všech zúčastněných subjektů, důvěře, vnímavosti a podpory systému od laické i odborné veřejnosti.

ZÁVĚR

Kyberprostor jako novodobá doména, je již ve své plném působení na své okolí. Vznik různých odborných týmů na kybernetickou bezpečnost, se stal nezbytností. Týmy úzce spolupracují mezi sebou, sdílí informace a navzájem pořádají společná cvičení. Zde pak navzájem testují své znalosti v problematice kybernetické bezpečnosti a navzájem se tak obohacují o poznatky a zkušenosti. Z mezinárodní i národní spolupráce, z proběhlých cvičení, neustálé analýzy bezpečnostního prostředí a předešlých poznatků sestavují jednotlivé národní bezpečnostní úřady své strategie a akční plány ke kybernetické bezpečnosti.

V ČR, je hlavní garant kybernetické bezpečnosti NBÚ, kdy pomocí Národního centra pro kybernetickou bezpečnost zabezpečuje přípravu na vysokých školách, e-lerning, odborné školení veřejného sektoru, ale také představuje styčný bod pro komunikaci napříč všemi sférami společnosti, které se dotýká kybernetická bezpečnost. Připravuje každoroční zprávu o stavu kybernetické bezpečnosti v ČR. Ze zprávy se poté vyhodnocuje naplněnost Akčního plánu, který se aktualizuje spolu s dalším vývojem možných hrozeb. NCKB vytváří metodiky a pomocné materiály k předvídání a hodnocení dopadů na informační bezpečnost. Také navrhl koncepci vzdělávání, která doplňuje systém informačního vzdělávání zavedeného Ministerstvem školství, mládeže a tělovýchovy a Ministerstvem práce a sociálních věcí. Do této koncepce se snaží zahrnout celé spektrum obyvatelstva, a tím šířit osvětu a svou činností také doplnit systém vzdělávání a přípravy odborníku o kybernetické bezpečnosti.

Problematika bezpečnosti a prevence kriminality má počátky už od samotného vzniku České republiky. V souhrnu je kriminalita na sestupné tendenci, kromě dvou odchylek. První byla hned po revoluci v roce 1993 spojená se samostatností a privatizací, další po vyhlášení amnestie Prezidentem republiky, který odhalil nepřipravenost systému na masové propuštění většího počtu lidí z věznic. Systém prevence se i nadále potýká s neúspěchem ve snížení recidivy a v pomoci propuštěným na svobodu, kteří se často vrací do nefunkčního prostředí. Ten je představován ztrátou bydlení, rozpadem rodiny, nedostatkem finančních prostředků.

Prevence kriminality se také neobejde bez národní i mezinárodní spolupráce, sdílení zkušeností, poznatků a na vyhodnocování úspěšných projektů prevence, ale také i těch bezvýznamných výsledků. Ze všech dostupných informací se poté připravuje střednědobá Strategie prevence kriminality v České republice. Strategie spolu s dalšími strategickými do-

kumenty, metodikami a pomocnými materiály jsou východiskem pro tvorbu jednotlivých koncepcí a plánů prevence kriminality krajů a obcí. Kraje nebo obce si provádí vlastní bezpečnostní analýzu nebo výzkumy pocitu bezpečí, které jsou také zahrnuty do jednotlivých koncepcí, plánů, programů a projektů předcházení kriminalitě. Vysoká míra recidivy ukázala na špatně nastavené projekty, na znovu začlenění vracejících se osob z výkonu trestu, do běžného života. Možností do budoucna je v kvalitní prevenci u děti a mladistvých, aby se minimalizoval jejich kontakt s kriminálními faktory. Vytvoření lepších životních podmínek, vyplněním volného času, kvalitním vzděláním vedoucím k jejich osobnímu rozvoji a správnou výchovou se tak mohou vyhnout páchání trestné činnosti.

SEZNAM POUŽITÉ LITERATURY

1. **Diblíková, S.,M. CEJP, M. ŠTEFUNKOVÁ, P. ZEMAN, V. SMEJKAL, M. MARTINKOVÁ.** Institut pro kriminologii a sociální prevenciI. *Ediční řada STUDIE.* [Online] © Institut pro kriminologii a sociální prevenci, 2016. [cit. 2018-01-05]. http://www.ok.cz/iksp/docs/437.pdf. ISBN 978-80-7338-162-2.

2. **JIROVSKÝ, Václav.** *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha : Grada Publishing, 2007. [cit. 2018-01-05]. ISBN 978-80-247-1561-2.

3. **SMEJKAL, Vladimír.** Právní prostor. *Kybernetická kriminalita - fenomén dneška.* [Online] Právní prostor, Červenec 20, 2015. [cit. 2018-01-05]. https://www.pravniprostor.cz/clanky/trestni-pravo/kyberneticka-kriminalita-fenomen-dneska. ISSN 2336-4114.

4. **ŠVANDELÍKOVÁ, Klára.** Právní prostor. *Pět otázek pro profesora Vladimíra Smejkala.* [Online] Právní prostor, Březen 23, 2015. [cit. 2018-01-05]. https://www.pravniprostor.cz/clanky/trestni-pravo/pet-otazek-pro-profesora-vladimira-smejkala. ISSN 2336-4114.

5. Právní prostor. *Boj s kyberkriminalitou v EU.* [Online] Právní prostor, Leden 27, 2016. [cit. 2018-01-05]. https://www.pravniprostor.cz/aktuality/aktuality/boj-s-kyberkriminalitou-v-eu-klicove-je-zajisteni-dukazu-a-spolecny-dalsi-postup-rekl-robert-pelikan. ISSN 2336-4114.

6. **MICHÁLEK, Michal.** Policie České Republiky. *Kyberkriminalita.* [Online] © 2018 Policie ČR, Březen 31, 2017. [cit. 2018-01-05]. http://www.policie.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx.

7. Národní úřad pro kybernetickou a informační bezpečnost. *Aktuální legislativa.* [Online] NÚKIB, Červenec 23, 2014. [cit. 2018-01-12]. https://nukib.cz/download/kii-vis/ZKB_uplne_zneni.pdf.

8. **KOLOUCH, Jan.** *CyberCrime.* Praha : CZ.NIC, z. s. p. o, 2016. [cit. 2018-01-12]. ISBN 978-80-88168-18-8.

9. Úmluva Rady Evropy č. 185 o kyberkriminalitě. [Online] Listopad 23, 2001. [cit. 2018-01-12]. https://rm.coe.int/16804931c0.

10. Additional Protocol to the Convention on Cybercrime No. 189. [Online] Leden 28, 2003. [cit. 2018-01-12]. https://rm.coe.int/168008160f.

11. Národní úřad pro kybernetickou a informační bezpečnost. *Co je NÚKIB.* [Online] NÚKIB, 2017. [cit. 2018-03-05]. https://www.govcert.cz/cs/.

12. Národní úřad pro kybernetickou a informační bezpečnost. *Govcert.cz.* [Online] NÚKIB, 2017. [cit. 2018-03-05]. https://www.govcert.cz/cs/vladni-cert/govcert-cz/.

13. Poslanecká sněmovna Parlamentu České republiky. *Aktuality ze Sněmovny.* [Online] Parlament České republiky, 2015. [cit. 2018-04-28]. http://www.psp.cz/doc/00/08/56/00085617.pdf.

14. **ŠTEFUNKOVÁ, Michaela and ŠEJVL, Jaroslav.** *Základy prevence kriminality pro pedagogické pracovníky.* Praha : TOGGA, spol. s. r. o., 2012. [cit. 2018-01-18]. ISBN 978-80-87258-96-5.

15. **PROTIVÍNSKÝ, Miroslav.** Ministerstvo vnitra České Republiky. *Kriminalita páchaná na dětech.* [Online] © 2018 Ministerstvo vnitra České republiky, 2010. [cit. 2018-01-18]. http://www.mvcr.cz/clanek/kriminalita-pachana-na-detech-973715.aspx.

16. Elektronický katalog sociálních služeb města Bruntál. *Prevence kriminality.* [Online] 2015. [cit. 2018-05-01]. http://socialnisluzby.mubruntal.cz/frontend/webroot/uploads/files/2016/01/plan_prevence_kriminality_mesta_bruntal_na_leta_2016_-_2018141.pdf.

17. Police České Republiky. *Jednotlivé druhy kyberkriminality.* [Online] © 2018 Policie ČR, Březen 31, 2017. [cit. 2018-01-22]. http://www.policie.cz/clanek/jednotlive-druhy-kyberkriminality.aspx.

18. **KUNEŠ, Jakub.** PCWorld. *Co je sociální inženýrství? - 1. díl.* [Online] IDG Czech Republic, a. s., Červen 2, 2012. [cit. 2018-01-22]. http://pcworld.cz/internet/co-je-socialni-inzenyrstvi-1-dil-44361.

19. Policie České Republiky. *POMOC OBĚTEM TČ.* [Online] © 2018 Policie ČR, 2017. [cit. 2018-01-22]. http://www.policie.cz/clanek/sexualni-a-mravnostni-trestne-ciny.aspx.

20. **Beránek, Ladislav.** Policie České Republiky. *Hate crime … a co na to zákon?* [Online] 2015. http://www.policie.cz/clanek/hate-crime-a-co-na-to-zakon.aspx.

21. Databáze Strategií. *Česká republika.* [Online] © 2018 Ministerstvo pro místní rozvoj ČR, Únor 16, 2015. [cit. 2018-03-05]. https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/nskb-150216-final.pdf.

22. Databazé Strategií. *Česká republika.* [Online] © 2018 Ministerstvo pro místní rozvoj ČR, Květen 25, 2015. [cit. 2018-03-05]. https://www.dataplan.info/img_upload/7bdb1584e3b8a53d337518d988763f8d/akcni-plan-nskb-2015-2020-final-150408.pdf.

23. Národní úřad pro kybernetickou a informační bezpečnost. *Zpráva o stavu kybernetické bezpečnosti Česé republiky 2016.* [Online] NÚKIB, 2017. [cit. 2018- 04-02]. https://www.govcert.cz/download/Zpravy-KB-vCR/Zpr%C3%A1va-stavu-KB-2016.pdf.

24. Národní úřad pro kybernetickou a informační bezpečnost. *Podpůrné materiály.* [Online] NÚKIB, 2017. [cit. 2018-05-10]. https://www.govcert.cz/download/kii-vis/Metodika_k_voditkum_pro_hodnoceni_dopadu_NUKIB_v.1.2_s_prilohou.pdf.

25. Ministerstvo vnitra České Republiky. *Strategie prevence kriminality v České republice na léta 2016 až 2020.* [Online] © 2018 Ministerstvo vnitra České republiky, 2015. [cit. 2018-05-10]. http://www.mvcr.cz/clanek/strategie-prevence-kriminality-v-ceske-republice-na-leta-2016-az-2020.aspx.

26. Prevence kriminality v České republice. *Metodika pro tvorbu strategických dokumentů prevence kriminality a víceletých bezpečnostních analýz.* [Online] © 2018 made by Galileo Corporation s.r.o., 11 27, 2017. [cit. 2018-04-15]. http://www.prevencekriminality.cz/ke-stazeni/metodicke-materialy-1/metodika-pro-tvorbu-strategickych-dokumentu-prevence-kriminality-a-viceletych-bezpecnostnich-analyz-443cs.html.

27. Moravskoslezský kraj. *Aktuální dokumenty prevence kriminality.* [Online] WEBMASTER@MSK.CZ, 2016. [cit. 2018-04-25]. https://www.msk.cz/assets/socialni_oblast/bezpecnostni-analyza-moravskoslezskeho-kraje-_aktualizace-2017_.pdf.

28. Moravskoslezský kraj. *Aktuální dokumenty prevence kriminality.* [Online] WEBMASTER@MSK.CZ, 2016. [cit 2018-04-30]. https://www.msk.cz/assets/socialni_oblast/koncepce-prevence-kriminality-moravskoslezskeho-kraje-na-obdobi-2017---2021_1.pdf.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CEO	Command executive order.
CERT	Computer emergency response team.
CSIRT	Computer security incident response team.
ČR	Česká republika.
EU	Evropská unie.
ICT	Informační a komunikační technologie.
IT	Informační technologie.
KII	Kritická informační infrastruktura.
NBÚ	Národní bezpečnostní úřad.
NCKB	Národní centrum kybernetické bezpečnosti.
NIS	Směrnice Evropského parlamentu a Rady EU.
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost.
OPL	Omamné a psychotropní látky.
OSN	Organizace spojených národů.
PČR	Policie České republiky.
USA	Spojené státy americké.
VIS	Významné informační systémy.
VTOS	Výkon trestu odnětí svobody.

REJSTŘÍK

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: METODIKA K VODÍTKŮM PRO HODNOCENÍ DOPADŮ

Příloha 1 Vodítka pro hodnocení dopadů

Vodítka pro hodnocení dopadů

Pro posouzení závažnosti dopadů způsobených narušením bezpečnosti informací (důvěrnosti, dostupnosti, integrity) jsou navrženy následující oblasti dopadů.

A. Bezpečnost a zdraví osob	B. Ochrana osobních údajů
C. Zákonné a smluvní povinnosti	D. Trestně-právní řízení
E. Veřejný pořádek	F. Mezinárodní vztahy
G. Řízení a provoz organizace	H. Ztráta důvěryhodnosti
I. Finanční ztráty	J. Zajišťování nezbytných služeb

Oblasti dopadů A. až J. obsahují obecné scénáře, které by mohly nastat v případě narušení bezpečnosti zpracovávaných dat a informací (narušení důvěrnosti, dostupnosti nebo integrity).

Závažnost dopadů je v každé z oblastí rozdělena do 4 úrovní dopadů (nízký, střední, vysoký a kritický). Matice dopadů je vytvořena tak, aby si úrovně (závažnosti) dopadů v jednotlivých oblastech navzájem odpovídaly (byla mezi nimi přiměřená korelace). V případě, že je pro konkrétní případ hodnocení bezpečnosti dat poplatných více oblastí dopadů (např. je relevantní „A. Bezpečnosti a zdraví osob“ a „B. Ochrana osobních údajů“), použije se pro výsledné stanovení závažnosti dopadu nejvyšší dosažená hodnota v rámci hodnocených oblastí dopadů. Tento přístup ilustruje následující příklad.

		1	nízká	...	Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	...	Může narušit řádné řízení nebo fungování části nebo celé organizace.	Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace)	...
		2	střední	...	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2 % celkového ročního obratu - viz čl. 83/4 GDPR).	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.	...	Může omezit provádění důležitých činností organizace.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05% a 2 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	...
		3	vysoká	...	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na velkou skupinu osob (pokuta až 20 mil. EUR nebo 4 % celkového ročního obratu - viz čl. 83/5 GDPR).	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	...	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě PZS je hranice ztráty stanovena na 0,25 % HDP.	...
ZKB - KII, ISZS		4	kritická **		žádné vodítko	žádné vodítko		Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě KII je hranice ztráty stanovena na 0,5 % HDP.	...
	ZUI	Narušení bezpečnosti informací v oblasti "důvěrnosti" může způsobit újmu zájmům České republiky anebo nevýhodnost pro zájmy České republiky a zároveň je informace typově uvedena v seznamu utajovaných informací (§ 2 písm. a) zákona č. 412/2005 Sb.). Na základě tohoto dopadu by se za splnění dalších legislativně stanovených podmínek mělo jednat o utajované informace. Pro určení odpovídajícího stupně utajení je třeba postupovat v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. A to za splnění dalších stanovených podmínek, např. uvedených v nařízení vlády č. 522/2005 Sb.									

V rámci tohoto zjednodušeného příkladu je hodnocen určitý informační systém. Při hodnocení dopadu procházíme tabulku v příloze 1 a hodnotíme nejhorší možné dopady narušení bezpečnosti informací (důvěrnosti, dostupnosti, integrity) v tomto systému. Některé oblasti dopadu (slupce A. – J.) nemusejí být pro všechny systémy relevantní. Pro účely příkladu spisové služby to jsou oblasti (sloupce) A., D. – F. a J. Narušení bezpečnosti informací v tomto hodnoceném systému tedy nebude mít dopad například v oblasti A. Bezpečnost a zdraví osob. Tyto nerelevantní sloupce jsou pro účely tohoto příkladu vypuštěny. V rámci zbývající oblasti dopadu (sloupců) je rozhodný ten nejhorší možný dopad narušení alespoň jednoho z aspektů bezpečnosti informací (důvěrnost, dostupnost, integrita) v rámci jednotlivých oblastí. Podle toho nejhoršího dopadu narušení bezpečnosti informací tedy stanovíme celkovou úroveň dopadu hodnoceného systému.

V rámci příkladu je nejhorší dopad narušení bezpečnosti informací v oblasti B., G., H. Tedy systém je ohodnocen na úrovni 3 – vysoká. Za splnění dalších podmínek (například odvětvových kritérií podle vyhlášky č. 437/2017 Sb.) by měl být takový systém zařazen do kategorie významných informačních systémů nebo informačních systémů základní služby.

Základní východiska pro hodnocení dopadů narušení bezpečnosti informací

V rámci hodnocení jsou důležité tyto principy:

- Nezkoumají se příčiny (hrozby) narušení bezpečnosti.
- Neurčuje se pravděpodobnost výskytu jednotlivých scénářů.
- Posuzují se nejhorší možné „kritické“ scénáře.
- Neuvažují se existující bezpečnostní opatření.

Je nutné hodnotit narušení všech aspektů bezpečnosti informací, tedy narušení:

- důvěrnosti,
- dostupnosti,
- integrity.

Postup hodnocení dopadů

V rámci interview jsou garanti dotazováni na nastínění realistického scénáře nejhoršího případu, který by mohl vyplývat z následujících dopadů:

- Narušení dostupnosti
    - nedostupnost informačního systému (nedostupnost zpracovávaných informací),
    - ztráta dat od poslední zálohy, úplná ztráta dat a informací.
- Narušení důvěrnosti dat a informací (neoprávněné prozrazení a únik informací).
- Narušení integrity dat a informací (vlivem neúmyslné modifikace (chyby), úmyslné modifikace dat a systémové chyby).

Interview zpravidla probíhají podle následujícího scénáře:

- Získání základních informací o hodnoceném informačním systému: účel a rozsah zpracovávaných informací, relevantní legislativa a regulatorní požadavky, kritické termíny, úřední hodiny, lhůty apod.
- Vysvětlení způsobu a postupu hodnocení dopadů. Zejména je potřeba zdůraznit výše uvedené principy.
- Kritické scénáře (scénáře nejhoršího možného dopadu) popsané garantem se porovnají s obecnými vodítky pro hodnocení dopadů (viz příloha tohoto dokumentu). Pro určení závažnosti dopadů je použita stupnice o čtyřech úrovních dopadu (1 – nízký, 2 – střední, 3 – vysoký, 4 – kritický).

Poznámka: V případě, že se na danou situaci dá uplatnit více než jeden scénář současně (např. ohrožení bezpečnosti osob, ztráta důvěryhodnosti, finanční ztráta) se dopady nesčítají. Vždy se bere v rámci vyhodnocení v potaz nejvyšší dosažená úroveň dopadu pro každý z parametrů bezpečnosti.

Po zpracování výsledků interview je vhodné zaslat výstup z hodnocení garantovi k revizi a odsouhlasení provedeného hodnocení.

I. Hodnocení následků nedostupnosti

Hodnocení následků nedostupnosti vychází z předpokladu, že nedochází ke ztrátě dat, jen k jejich dočasné nedostupnosti způsobené výpadkem informačního systému. Následky vyplývající z nedostupnosti dat se mohou lišit v závislosti na délce nedostupnosti systému nebo dané ICT služby. Pro stanovení okamžiku, kdy se poprvé projeví dopady z nedostupnosti a toho jak se v čase tyto dopady vyvíjí, se hodnocení provádí v časových intervalech (tzv. časové řezy).

II. Hodnocení následků ztráty dat

Tento dopad zkoumá následky, které by mohly vzniknout v případě ztráty dat. Pro určení optimálního požadavku na frekvenci zálohování dat se hodnocení provádí pro následující časové intervaly.

Výsledek hodnocení úplné a trvalé ztráty dat ze systému může vyústit například v požadavek na umístění záloh v geograficky oddělené lokalitě.

III. Hodnocení následků narušení důvěrnosti dat

Tento dopad je možné zkoumat zejména z hlediska:

- Prozrazení v rámci organizace – prozrazení zaměstnancům, kteří však nemají oprávnění pro přistup k datům.
- Prozrazení smluvním partnerům – prozrazení smluvním poskytovatelům služeb (zaměstnancům třetí strany, kteří mohou mít oprávněný přístup k systému nebo síti, ale nikoli k datům – například organizace provozující outsourcované informační služby).
- Prozrazení vně organizace – únik informací na veřejnost.

IV. Hodnocení následků narušení integrity dat

Otázky zkoumané při vyšetřování tohoto dopadu se liší podle účelu hodnoceného informačního systému. Neodhalená změna nebo chyba v datech může způsobit zásadní dopady, neboť organizace pak funguje na základě špatných dat. Dopad je možné zkoumat z hlediska:

- Chyby malého rozsahu – neúmyslné modifikace dat, např. chyby při vkládaní dat uživatelem, duplikace vstupu.
- Chyby velké rozsahu – narušení správnosti a úplnosti informací velkého rozsahu, např. chyby v kódu informačního systému, porušení integrity dat vlivem technického selhání.
- Úmyslné modifikace – úmyslná změna provedená uživatelem nebo správcem systému nebo útočníkem.

Popis a příklady použití jednotlivých oblastí dopadů

A. Bezpečnost a zdraví osob

Neoprávněné prozrazení, modifikace nebo nedostupnost informací mohou vést k ohrožení bezpečnosti a zdraví osob.

Například:

- Prozrazení údajů určitých osob (např. adresa, identita agentů či chráněné osoby dle zákona č. 137/2001 Sb.) může způsobit, že se tyto osoby stanou cílem někoho, kdo jim chce způsobit újmu.
- Neoprávněná modifikace informací (např. informací v rámci komunikace složek integrovaného záchranného systému, informací spojených s výrobními procesy, výrobou energií, léčebnými postupy apod.) může způsobit chybnou funkčnost zařízení nebo může vést k nesprávným rozhodnutím, v jejichž důsledku dojde k ohrožení bezpečnosti nebo zdraví osob.
- Nedostupnost informací z některých systémů (např. komunikační systémy IZS, informace v letecké dopravě, zdravotní záznamy apod.), může vést k nesprávným nebo pozdním rozhodnutím, v jejichž důsledku mohou vzniknout negativní dopady na bezpečnost nebo zdraví určité osoby nebo skupiny osob.

Poznámka: V některých případech je pro určení maximálního dopadu doporučeno také zvážit dopady v oblastech Ochrana osobních údajů a Trestně-právní řízení.

B. Ochrana osobních údajů

Povinnosti správců a zpracovatelů osobních údajů a práva subjektů údajů nově upravuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR). Nařízení se použije od 25. května 2018, a to plošně ve všech státech EU.

Některé informační systémy uchovávají a zpracovávají údaje o zaměstnancích, externistech, smluvních partnerech (např. jejich osobní údaje, informace o jejich platu nebo osobním hodnocení). Jiné systémy byly určeny pro zpracování údajů o občanech, a obsahují například informace o jejich finančním či zdravotním stavu. Tyto informace umožňují identifikovat osobu, jíž se týkají.

Například:

- Prozrazení osobních nebo citlivých osobních údajů může způsobit danému jednotlivci psychické problémy, snížit možnost jeho společenského a pracovního uplatnění a může pak vést k občanskoprávnímu, správněprávnímu nebo trestněprávnímu řízení proti organizaci, která osobní údaje spravuje nebo zpracovává. Maximální výše ukládaných pokut je 20 000 000 €, resp. 4 % z globálního celoročního obratu podniku a to podle toho, která částka je vyšší (viz článek 83 GDPR).
- Neoprávněná modifikace dat v databázi (např. pozměnění pracovního hodnocení na negativní).
- Je důležité, aby nebyly údaje o osobách znepřístupněny nebo zničeny, což by mohlo vést k nesprávným rozhodnutím nebo k nečinnosti v době, kdy by bylo zapotřebí na základě těchto údajů konat (např. lustrace osob). Tato situace může mít podobné důsledky jako neoprávněné prozrazení nebo modifikace.

Poznámka: Pokud dopad spočívá v porušení zákona či smlouvy (např. zákona o ochraně osobních údajů, GDPR), je vhodné vzít při stanovení hodnot dopadů také v úvahu vodítko Zákonné a smluvní povinnosti, Trestně-právní řízení či Finanční ztráty. V některých případech, kdy dopad narušení bezpečnosti informací může mít vliv na bezpečnost osob, je třeba přihlédnout k vodítku Bezpečnost a zdraví osob.

C. Zákonné a smluvní povinnosti

Zpracovaní a správa dat organizací mohou podléhat požadavkům celé řady smluv a právních předpisů a z nich vyplývajících zákonných a smluvních povinností. Data mohou být také uchovávána a zpracovávána proto, aby organizace byla schopna tyto požadavky naplnit. Neplnění těchto požadavků, ať už úmyslné nebo neúmyslné, může vest k občanskoprávnímu, správněprávnímu nebo trestněprávnímu řízení proti osobám nebo celé organizaci. Toto řízení může vést k pokutám nebo případně až k trestům odnětí svobody. Za relevantní lze považovat všechny předpisy a smlouvy, jimiž se řídí provoz ICT.

Například:

- Může být zákonnou povinností organizace určité informace chránit (např. informace podle zákon č. 101/2000 Sb., GDPR či obchodní tajemství). Jejich prozrazení může být úmyslné, nebo může být důsledkem neodpovídajících organizačních a

technických opatření, která organizace k ochraně zákonem stanovených informací realizuje.

- Neoprávněná modifikace informací může vést k porušení zákonem stanovených povinností.
- Nedostupnost informací může vést k porušení zákonem stanovených povinností vztahujících se ke zpřístupňování informací (např. podle zákonů č. 106/1999 Sb. a č. 101/2000 Sb.).
- Porušení smluvní povinnosti může vést k občanskému soudnímu sporu, v němž může být uložena náhrada škody způsobené porušením povinnosti plynoucí organizaci ze smlouvy.

Poznámka: Hodnocení podle této oblasti vodítek je vhodné založit na předběžné právní analýze vymezující právní předpisy a smlouvy, které mají bezprostřední vliv na zpracování informací v rámci organizace.

D. Trestně-právní řízení

Prozrazení nebo modifikace některých údajů může usnadnit spáchání trestného činu. Prozrazení, modifikace nebo nedostupnost některých údajů mohou také mít nepříznivý dopad na vyšetření nebo potrestání trestného činu. Nedostupnost informací může být způsobena i v důsledku úmyslného jednání zaměstnanců, snažících se získat neoprávněnou výhodu sobě nebo třetí osobě.

Například:

- Prozrazení osobních údajů může vést k vydírání, fyzickému násilí nebo ublížení na zdraví.
- Únik informací o zabezpečení systémů nebo havarijních plánů může napomoci ohrožení bezpečnosti a také ke spáchání závažných trestných nebo v některých případech i teroristických činů.
- Prozrazení, modifikace nebo ztráta některých informací v průběhu vyšetřování trestného činu může mít negativní vliv na úspěšnost tohoto vyšetřování (např. prozrazení adres nebo únik informací o klíčových svědcích, znehodnocení důkazů).

E. Veřejný pořádek

Některé organizace mohou zpracovávat data, u kterých by narušení bezpečnosti mohlo ohrozit veřejný pořádek. Mohou to být například informace o místních rozvojových projektech (např. o stavbě nové silnice) nebo životním prostředí, jejichž narušení by mohlo způsobit protesty, demonstrace či stávky.

Například:

- Nespolehlivé poskytování informací nebo dokonce jejich nedostupnost v období rozsáhlých povodní nebo jiných živelních pohrom může způsobit dopravní kolaps, komplikace v zásobování postižených oblastí nebo dokonce vážné problémy při záchranných akcích.
- Prozrazení (předčasný únik) informací o plánu uzavřít místní poštovní úřad, prozrazení návrhu na zmrazení mezd nebo propouštění ve státních podnicích může vyvolat místní nespokojenost, protesty nebo demonstrace.
- Modifikace informací o rozšíření systému dálnic s ekonomickými dopady (např. povinný odprodej pozemků nebo změny plánů územního rozvoje) mohou způsobit nespokojenost určité skupiny obyvatel.

F. Mezinárodní vztahy

Některé organizace vytváří informace, které ovlivňují vztahy mezi ČR a ostatními zeměmi či nadnárodními organizacemi (EU, NATO). Prozrazení nebo neoprávněná modifikace některých druhů informací by mohla ovlivnit vztahy s těmito partnery. Stejně tak by mohla negativně ovlivnit pozici ČR nedostupnost některých typů informací např. v kritických fázích vyjednávání.

Například:

- Únik nebo modifikace informací, které by vedly k podání oficiálního protestu, uvalení sankcí, odvolání velvyslance apod.
- Nedostupnost informací o připravenosti splnit vyjednávané podmínky (např. že byl vydán rozkaz k určitým akcím).

G. Řízení a provoz organizace

Informace mohou být takového charakteru, že jejich ohrožení může narušit efektivní provoz organizace. Pokud má organizace celonárodní význam, nebo poskytuje některé nezbytné služby (např. bankovnictví či energetika) může dojít k dopadům na velké množství osob, ekonomickým ztrátám apod.

Například:

- Informace týkající se změny politiky organizace vůči veřejnosti mohou v případě předčasného prozrazení vyvolat veřejné reakce v rozsahu, který realizaci takové politiky znemožňuje.
- Podobně také informace týkající se personálu organizace, jako jsou změny v pracovních podmínkách, mohou v případě předčasného prozrazení vést k negativním vztahům zaměstnanců s vedením a oslabit tak řízení celé organizace.
- Také modifikace nebo nedostupnost informací v souvislosti s finančními aspekty nebo počítačovým programovým vybavením mohou mít závažné důsledky z hlediska chodu organizace.

H. Ztráta důvěryhodnosti

Neoprávněné prozrazení, modifikace nebo nedostupnost informací může vést ke ztrátě dobrého jména organizace s následným poškozením pověsti, ztrátou důvěryhodnosti a dalšími nepříznivými důsledky. Bezpečnostní incidenty snižují důvěryhodnost organizace a tím i její vážnost v očích veřejnosti či obchodních partnerů. Od toho se odvíjí i vztah veřejnosti a dalších aktérů k těmto organizacím a komplikuje to jejich postavení při prosazování a plnění úkolů, které vyplývají z jejich účelu.

I. Finanční ztráta

V některých informačních systémech se uchovávají a zpracovávají informace, které se přímo týkají finančních transakcí nebo se vztahují k finančnímu fungování organizace nebo organizací jí spravovaných. V důsledku neoprávněného prozrazení a modifikace či nedostupnosti a zničení takových informací může vzniknout finanční ztráta. Tato oblast pokrývá také finanční ztráty způsobené narušením činnosti systému, při němž nedostupnost či zničení informací může způsobit újmu uživatelům, organizaci nebo i dalším stranám. Obnova po výskytu mimořádné události i sanace škod vyžaduje často vynaložení značného času, úsilí a financí, které je také třeba brát v úvahu. U tohoto faktoru je třeba finanční náklady odvodit od času stráveného pracovníky na obnově, ztrát způsobených zastavením činnost, kompenzací dotčených, pokut a plateb za sanaci škod.

Poznámka: Protože reálné dopady se mohou u různých organizací lišit, při použití vodítek v této oblasti je nutné přihlížet k reálnému objemu finančních prostředků spravovaných

danou organizací a podle něho modifikovat hodnoty uvedené v tabulce tak, aby vyjadřovaly reálné dopady na organizaci. Vodítko „finanční ztráty“ je z těchto důvodů nastaveno na procento ztráty z ročního rozpočtu či obratu.

J. Zajišťování nezbytných služeb

Některé ICT zpracovávají informace, jejichž narušení může přímo ovlivnit poskytování nezbytných služeb osobám či jiný významný zásah do každodenního života.

Například:

- Modifikací informací v informačním systému (např. doručení zprávy o reálně neexistujícím přepětí či jiné vadě na elektrickém vedení) může dojít k výpadku elektřiny pro určitý počet osob.
- Narušení informací v systému inteligentního řízení dopravy může vést k vytvoření falešné uzavírky na exponovaném dopravním uzlu.

PŘÍLOHA P II: AČNÍ PLÁN K NÁRODNÍ STRATEGII KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ LET 2015 – 2020

Příloha 2 Akční plán

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
A. Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti				
Vytvořit efektivní model spolupráce na národní úrovni mezi jednotlivými subjekty kybernetické bezpečnosti – pracoviště typu CERT a CSIRT, subjekty KII apod. – a posilovat jejich stávající struktury a procesy.	**A.1.01**	Vytvořit v koordinaci s ostatními subjekty schéma a podrobný model spolupráce v rámci zajišťování kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MV MZV MO MPO Zpravodajské služby	Q3 2015
	A.1.02	Provést analýzu agend v rámci problematiky kybernetické bezpečnosti a na jejím základě definovat národní zájmy a priority v této oblasti.	NBÚ/NCKB *ve spolupráci s:* MO MZV MPO Zpravodajské služby	Q4 2015
	A.1.03	Provádět technická i netechnická národní cvičení kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MO MV Zpravodajské služby	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Vytvořit národní, koordinovaný postup pro zvládání incidentů, který nastaví formát spolupráce, bude obsahovat komunikační matici, protokol postupu a definovat jednotlivé role aktérů.	**A.2.01**	Vytvořit jednotnou metodologii pro zvládání kybernetických bezpečnostních incidentů na základě ZKB a souvisejících právních předpisů.	NBÚ/NCKB	Q1 2016
	A.2.02	Vytvořit komunikační matici mezi vrcholovými aktéry kybernetické bezpečnosti (národní aktéři, KII, VIS).	NBÚ/NCKB	Q2 2015
	A.2.03	Poskytnout popis bezpečné komunikace s datovým (komunikačním) rozhraním, pomocí kterého bude NBÚ automatizovaně přijímat XML zprávy s hlášením kybernetických bezpečnostních incidentů. Součástí bude i popis XML schématu, které odpovídá obsahu formuláře pro hlášení kybernetických bezpečnostních incidentů uvedeného ve vyhlášce č. 316/2014 Sb., doplněného o další nepovinná pole.	NBÚ/NCKB	Q2 2015
	A.2.04	Vytvořit protokol osvědčených postupů v oblasti zajišťování kybernetické bezpečnosti.	NBÚ/NCKB	Q2 2016
Vytvořit metodologii pro hodnocení rizik v ČR na úrovni státu.	**A.3.01**	Zvolit metodologii hodnocení rizik a hrozeb pro oblast kybernetické bezpečnosti na národní úrovni.	NBÚ/NCKB	Q1 2018
	A.3.02	Provádět hodnocení hrozeb a rizik pro oblast kybernetické bezpečnosti na národní úrovni.	NBÚ/NCKB	od Q2 2018 průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Udržovat jednotný postoj ČR směrem do zahraničí, který bude koordinován s ostatními resorty zainteresovanými v oblasti kybernetické bezpečnosti.	**A.4.01**	Vytvořit efektivní model pro sdílení informací o zahraničních aktivitách mezi NBÚ a ostatními relevantními subjekty.	NBÚ/NCKB *ve spolupráci s:* MZV MO MPO MV ÚZSI	Q2 2016
	A.4.02	Koordinovat a harmonizovat s ostatními resorty pozice v EU, NATO a dalších mezinárodních organizacích.	NBÚ/NCKB *ve spolupráci s:* MZV MO MPO MV	od Q3 2015 průběžně
Zohledňovat odpovídajícím způsobem neustále se vyvíjející problematiku kybernetických hrozeb v rámci tvorby a aktualizací významných bezpečnostně-strategických materiálů ČR (Bezpečnostní strategie České republiky a další).	**A.5.01**	Implementovat Bezpečnostní strategii České republiky s ohledem na zvyšující se kybernetické hrozby a v případě změny bezpečnostního prostředí navrhnout její revizi.	NBÚ/NCKB MV MZV MO ÚV ČR Zpravodajské služby	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
B. Aktivní mezinárodní spolupráce				
V rámci svého členství v EU, NATO, OSN, OBSE, ITU a dalších mezinárodních organizacích se bude ČR aktivně podílet na mezinárodní diskuzi v aktivitách v rámci fór, programů, iniciativ apod.	**B.1.01**	Spolupracovat s EU v implementaci Strategie kybernetické bezpečnosti EU.	NBÚ/NCKB MPO MZV MV	průběžně
	B.1.02	Aktivně spolupracovat s EU, Evropskou komisí a jejími agenturami k zajištění větší koherence v kybernetických tématech v rámci EU.	NBÚ/NCKB MPO MZV MV MO	průběžně
	B.1.03	Spolupracovat a aktivně se podílet na práci ENISA v oblasti informační a síťové bezpečnosti.	NBÚ/NCKB	průběžně
	B.1.04	Aktivně se podílet v OBSE na vytváření a následné implementaci kybernetických opatření pro zvyšování důvěry mezi státy v kyberprostoru a případně dalších iniciativ v souladu s vizemi a principy NSKB ČR.	NBÚ/NCKB *ve spolupráci s:* MZV	průběžně
	B.1.05	Spolupracovat se spojenci při implementaci politiky NATO v rámci kybernetické obrany.	NBÚ/NCKB MO VZ	průběžně
	B.1.06	Podporovat spolupráci s NATO v oblasti kybernetické obrany, zejména s ohledem na reakci na kybernetické bezpečnostní incidenty a výměnu technických informací o hrozbách a zranitelnostech.	NBÚ/NCKB MO MZV VZ	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	B.1.07	Podporovat spolupráci s ITU ve věci tvorby a zavádění technických standardů v kybernetické bezpečnosti.	NBÚ/NCKB MPO ČTÚ	průběžně
	B.1.08	Rozvíjet dialog skrze „cyber diplomacy“ mezi členskými zeměmi OSN týkající se norem vztahujících se k používání ICT v jednotlivých zemích s cílem snížit společné nebezpečí, chránit důležitou národní a mezinárodní infrastrukturu a budovat důvěru a stabilitu mezi zeměmi.	MZV *ve spolupráci s:* NBÚ/NCKB	průběžně
	B.1.09	Aktivně participovat národní expertizou a prostředky v CCDCOE a podílet se průběžně na výzkumných aktivitách centra.	NBÚ/NCKB MO	průběžně
Ve středoevropském prostoru působit jako propagátor kybernetické bezpečnosti a dialogu mezi státy regionu.	**B.2.01**	Aktivně se podílet a podporovat spolupráci jak v rámci V4, tak ve Středoevropské platformě kybernetické bezpečnosti (CECSP).	NBÚ/NCKB *ve spolupráci s:* MZV MO	průběžně
	B.2.02	Aktivně se podílet a podporovat spolupráci s národními bezpečnostními týmy ve středoevropském a východoevropském regionu.	NBÚ/NCKB MO	průběžně
Navazovat a prohlubovat bilaterální spolupráci s dalšími státy.	**B.3.01**	Pokračovat a prohlubovat bilaterální spolupráci s vybranými státy v rámci kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MZV MO	průběžně
Účastnit se a organizovat mezinárodní cvičení.	**B.4.01**	Pravidelně se účastnit a aktivně se podílet na vytváření scénářů mezinárodních cvičení v oblasti kybernetické bezpečnosti.	NBÚ/NCKB MO MV	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Účastnit se a organizovat mezinárodní školení.	**B.5.01**	Účastnit se a organizovat mezinárodní školení, kurzy a semináře v oblasti kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MZV MO MV Zpravodajské služby	průběžně
Podílet se na vytváření efektivního modelu spolupráce a budování důvěry mezi pracovišti typu CERT a CSIRT na mezinárodní úrovni, mezinárodními organizacemi a akademickými centry.	**B.6.01**	Podporovat vytváření mezinárodních komunikačních a informačních kanálů mezi CERT/CSIRT pracovišti, mezinárodními organizacemi a akademickými centry.	NBÚ/NCKB MO	průběžně
	B.6.02	Aktivně se zapojit do výstavby a užívání NATO projektů pro řízení reakcí na kybernetické bezpečnostní incidenty a výměnu technických informací o škodlivých kódech mezi státy NATO.	NBÚ/NCKB MO	od Q3 2015 průběžně
Podílet se na vytváření mezinárodního konsenzu v rámci oficiálních i neoficiálních kanálů ohledně právních norem a chování v kyberprostoru, zajištění otevřenosti internetu, lidských práv a svobod.	**B.7.01**	Zapojit se do mezinárodní diskuze ohledně tvorby a způsobů implementace mezinárodněprávních norem v kyberprostoru, vč. lidských práv.	NBÚ/NCKB *ve spolupráci s:* MZV	Q3 2015
	B.7.02	Zapojit se do mezinárodní diskuze ohledně správy a řízení internetu.	NBÚ/NCKB *ve spolupráci s:* MZV MPO MV	Q2 2015

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
C. Ochrana národní KII a VIS				
Pokračovat v průběžné analýze a kontinuálním sledování zabezpečení systémů KII a VIS v ČR pomocí jasně definovaného protokolu.	**C.1.01**	Určovat průběžně subjekty KII a identifikovat VIS, jichž se dotýká ZKB a související právní předpisy.	NBÚ/NCKB *Ve spolupráci s:* MV	průběžně
	C.1.02	Konzultovat, komunikovat a poskytovat metodickou podporu subjektům KII a VIS.	NBÚ/NCKB	průběžně
	C.1.03	Podporovat a průběžně kontrolovat implementaci zákonných povinností u subjektů KII a VIS.	NBÚ/NCKB	průběžně
	C.1.04	Spolupracovat s mezinárodními partnery při hodnocení určování KII, zejména v oblasti přeshraničních závislostí.	NBÚ/NCKB	průběžně
Podporovat vznik dalších pracovišť typu CERT a CSIRT v ČR.	**C.2.01**	Informovat o výhodách a aktivně podporovat u soukromých subjektů (především spadajících pod KII) vznik CERT/CSIRT týmů k zajištění lepší spolupráce při řešení kybernetických bezpečnostních incidentů.	NBÚ/NCKB	průběžně
	C.2.02	Podporovat vznik CERT/CSIRT týmů v rámci resortů, dalších institucí státní správy a v rámci různých průmyslových odvětví.	NBÚ/NCKB	průběžně
	C.2.03	Vybudovat resortní CERT/CSIRT pracoviště MV k ochraně základních registrů a nejdůležitějších systémů pro fungování e-Governmentu.	MV *ve spolupráci s:* NBÚ/NCKB	Q1 2016

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Průběžně navyšovat odolnost, integritu a důvěryhodnost systémů a sítí KII a VIS.	**C.3.01**	Průběžně navyšovat kapacity NCKB, potažmo GovCERT.CZ a reflektovat personální a znalostní nároky vyplývající z vývoje stavu kybernetické bezpečnosti ve státě.	NBÚ/NCKB	průběžně
	C.3.02	Vytvořit doporučující základní rámec pro kybernetickou bezpečnost i mimo subjekty KII a VIS, tj. soubor standardů a osvědčených postupů, které pomohou organizacím zvládat kybernetická bezpečnostní rizika.	NBÚ/NCKB	Q3 2015
	C.3.03	Udržovat aktuální evidenci kybernetických bezpečnostních incidentů, vyhodnocovat je a navrhovat opatření.	NBÚ/NCKB	průběžně
	C.3.04	Určit minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů.	NBÚ/NCKB	Q4 2015
	C.3.05	Vytvořit a zavést honeypot systém k detekci kybernetických hrozeb.	NBÚ/NCKB	Q3 2016
	C.3.06	Mapovat vztahy mezi sítěmi veřejné správy a jejich ISP k zajištění efektivnější součinnosti v případě kybernetických bezpečnostních incidentů.	NBÚ/NCKB	od Q4 2015 průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	C.3.07	Zajišťovat a metodicky řídit nasazování detekčních systémů pro monitorování provozu sítí a kybernetických bezpečnostních událostí v rámci státní správy.	NBÚ/NCKB	Q1 2017
	C.3.08	Vytvořit laboratoř pro detekci a testování dopadů malware na informační systémy.	NBÚ/NCKB	Q2 2016
	C.3.09	Vytvořit a rozvíjet scénáře a programy simulace kybernetických bezpečnostních incidentů využitelné pro účely národních cvičení.	NBÚ/NCKB *ve spolupráci s:* MO MV Zpravodajské služby	od Q3 2015 průběžně
	C.3.10	Vytvořit a používat kapacity a schopnosti pro provádění kybernetických bezpečnostních testů.	NBÚ/NCKB	od Q3 2015 průběžně
	C.3.11	Vytvořit kapacity a zlepšovat schopnosti forenzní analýzy a dalších podpůrných služeb v rámci kybernetické bezpečnosti pro potřeby ČR.	NBÚ/NCKB	od Q3 2015 průběžně
	C.3.12	Podporovat projekt Fénix a zapojení významných sítí veřejné správy za účelem zachování funkcionalit a služeb během masivních kybernetických útoků.	NBÚ/NCKB *ve spolupráci s:* MV	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Kontinuálně provádět analýzu a monitoring hrozeb a rizik v ČR.	**C.4.01**	Provádět sběr a analýzu informací o hrozbách a rizicích, a tím zajišťovat aktuální přehled o situaci v kybernetické bezpečnosti jak v ČR, tak i ve světě.	NBÚ/NCKB *ve spolupráci s:* Zpravodajské služby	průběžně
	C.4.02	Detekovat anomálie v síťovém provozu a identifikovat potenciální kybernetické hrozby.	NBÚ/NCKB	Q1 2016
	C.4.03	Rozvíjet schopnosti aktivně získávat informace v kyberprostoru o možných hrozbách a rizicích pro kybernetickou bezpečnost ČR.	Zpravodajské služby	průběžně
	C.4.04	Analyzovat obsah informací o hrozbách a rizicích pro důležité zájmy ČR získaných v kybernetickém prostoru včetně jejich manipulativního působení na veřejnost a vytvořit proces vzájemného efektivního informování o relevantních hrozbách a rizicích mezi příslušnými subjekty.	Zpravodajské služby *ve spolupráci s:* NBÚ/NCKB	průběžně
	C.4.05	Podporovat koordinaci při preventivním působení v oblasti kybernetické bezpečnosti a získávání informací k plánování kybernetických útoků s cílem předcházení jejich provedení.	BIS ÚZSI	průběžně
	C.4.06	Modernizovat a personálně posílit jednotlivé specializované útvary zpravodajských služeb.	BIS ÚZSI	od Q1 2016 průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	C.4.07	Nastavit a rozvíjet spolupráci mezi zpravodajskými službami ČR i zainteresovanými věcně příslušnými národními či mezinárodními subjekty.	NBÚ/NCKB Zpravodajské služby	průběžně
Efektivně sdílet informace mezi státem a subjekty KII a VIS.	**C.5.01**	Zveřejňovat varování o kybernetických bezpečnostních hrozbách a incidentech s doporučením ke zvládání rizik.	NBÚ/NCKB	průběžně
	C.5.02	Vytvořit na základě dokončení mapování zabezpečovacích prvků u KII a VIS automatizovanou platformu na sdílení informací o kybernetických bezpečnostních hrozbách a incidentech vybraným ohroženým subjektům.	NBÚ/NCKB	Q4 2015
	C.5.03	Rozšířit možnosti hlášení kybernetických incidentů o webový formulář a komunikaci mezi systémy.	NBÚ/NCKB	Q1 2015
	C.5.04	Vytvořit na národní úrovni zabezpečenou platformu pro komunikaci při řešení rozsáhlejších kybernetických bezpečnostních incidentů.	NBÚ/NCKB	Q4 2015

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Navyšovat technologické kapacity a schopnosti NCKB, potažmo GovCERT.CZ a v rovině personální neustále vzdělávat a školit zaměstnance tohoto pracoviště.	**C.6.01**	Průběžně vzdělávat a školit pracovníky NCKB v oblasti kybernetické bezpečnosti.	NBÚ/NCKB	průběžně
	C.6.02	Prostřednictvím zahraničních kurzů udržovat aktuální povědomí o trendech v kybernetické bezpečnosti a hrozbách, kterým ČR jako aktivní člen EU a NATO čelí.	NBÚ/NCKB	průběžně
	C.6.03	Navyšovat schopnosti GovCERT.CZ identifikovat povahu kybernetických bezpečnostních incidentů.	NBÚ/NCKB	od Q2 2016 průběžně
	C.6.04	Vybudovat a rozšiřovat detekční systém včasného varování GovCERT.CZ.	NBÚ/NCKB	Q3 2017
	C.6.05	Zavést v GovCERT.CZ nepřetržitý provoz pohotovostní služby k monitorování a řešení kybernetických bezpečnostních incidentů.	NBÚ/NCKB	Q1 2016
Důkladně a důvěryhodně zabezpečit prostředí pro skladování a práci s daty subjektů KII a VIS, které zřídí a bude spravovat stát.	**C.7.01**	Vytvořit a vládě předložit Národní strategii cloud computingu.	MV *ve spolupráci s:* MF NBÚ/NCKB	Q4 2015
	C.7.02	Vypracovat a vládě předložit projekt státního cloudu včetně datových uložišť a další potřebné podklady (finanční, bezpečnostní, organizační a technické nároky).	MV *ve spolupráci s:* MF NBÚ/NCKB	Q1 2016
	C.7.03	Zmapovat současný stav a případně vypracovat návrh legislativních změn s ohledem na vytvoření státního cloudu včetně datových uložišť.	MV *ve spolupráci s:* NBÚ/NCKB	Q1 2018

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Pravidelně provádět kontrolu, odhalování chyb a zranitelností v informačních systémech a sítích využívaných státem, založené na principu penetračních testů v KII a VIS.	**C.8.01**	Pomocí předem ohlášených pravidelných penetračních testů provádět u subjektů KII a VIS odhalování chyb a zranitelnosti v jejich informačních systémech a sítích.	NBÚ/NCKB	Q1 2017
Průběžně navyšovat technologické a organizační předpoklady k aktivnímu odvracení (potlačení) kybernetických útoků.	**C.9.01**	V rámci Vojenského zpravodajství vytvořit Národní centrum kybernetických sil (NCKS), které bude schopné provádět široké spektrum operací v kyberprostoru a aktivity nutné pro zajištění kybernetické obrany ČR. NCKS bude schopné provádět vojenské operace v kyberprostoru, a to jak na podporu zahraničních operací AČR v rámci NATO nebo EU, tak i v případě hybridního konfliktu za účelem obrany ČR.	VZ	od Q1 2016 průběžně
	C.9.02	Připravit projekt financování a budování NCKS.	VZ	Q4 2015
	C.9.03	Zajištění vhodných prostor a nábor personálu pro NCKS.	VZ	od Q4 2015 průběžně
	C.9.04	Vybudování kompletní technické infrastruktury pro NCKS.	VZ	od Q1 2016 průběžně
	C.9.05	Připravit návrh nutných legislativních změn pro potřeby plné funkčnosti NCKS.	VZ *ve spolupráci s:* NBÚ/NCKB BIS ÚZSI	Q3 2015

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Zvyšovat národní možnosti, schopnosti a kapacity v oblasti aktivní obrany a protiopatření proti kybernetickým útokům.	**C.10.01**	Plně zajišťovat kybernetickou obranu ČR skrze kooperaci NCKS, NCKB, národního CERT a ostatních pracovišť typu CERT/CSIRT.	VZ	Q1 2020
	C.10.02	Definovat soubor možných krizových situací a vytvářet krizové scénáře pro spolupráci, komunikaci a nasazení protiopatření v období krizových stavů.	NBÚ/NCKB *ve spolupráci s:* MO VZ	od Q3 2015 průběžně
	C.10.03	Provádět národní cvičení v oblasti komunikace, koordinace a spolupráce při zajišťování kybernetické obrany.	VZ *ve spolupráci s:* NBÚ/NCKB	od Q1 2017 průběžně
Vzdělávat specializované odborníky, kteří se zaměří na problematiku a možnosti aktivních protiopatření při zajišťování kybernetické bezpečnosti a obrany a na obecně ofenzivní pojetí kybernetické bezpečnosti.	**C.11.01**	Reflektovat v NCKB personální a znalostní nároky vyplývající z vývoje stavu kybernetické bezpečnosti ve světě a sdílet tyto své schopnosti a dovednosti s relevantními subjekty.	NBÚ/NCKB	průběžně
	C.11.02	Reflektovat v NCKS personální a znalostní nároky vyplývající z vývoje stavu kybernetické obrany ve světě.	VZ	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Zpracovat postup pro přechod mezi vyhlášeným stavem kybernetického nebezpečí dle zákona o kybernetické bezpečnosti a stavy dle ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR.	**C.12.01**	Zpracovat postup pro přechod mezi vyhlášeným stavem kybernetického nebezpečí dle zákona o kybernetické bezpečnosti a stavy dle ústavního zákona č. 110/1998 Sb., o bezpečnosti ČR.	NBÚ/NCKB *ve spolupráci s:* MV MZV MO VZ ÚV ČR	Q1 2016
	C.12.02	Vytvořit pracovní skupinu z odborníků na mezinárodní právo z řad MO, MZV, MV, zpravodajských služeb a NBÚ/NCKB ve věci opatření kybernetické bezpečnosti a kybernetické obrany v mezinárodním měřítku.	NBÚ/NCKB *ve spolupráci s:* MV MZV MO Zpravodajské služby	Q3 2015

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
D. Spolupráce se soukromým sektorem				
Pokračovat v navazování spolupráce se soukromým sektorem a navyšovat povědomí o práci a aktivitách NBÚ v oblasti kybernetické bezpečnosti.	**D.1.01**	Navazovat kontakty a spolupráci se soukromým sektorem, a navyšovat tak povědomí o práci a možnostech spolupráce s NCKB prostřednictvím pravidelných jednání a vzájemného sdílení informací.	NBÚ/NCKB	průběžně
	D.1.02	Spolu s poskytovateli služeb elektronických komunikací a s poskytovateli služeb informační společnosti pracovat na shodném přístupu, jak lépe internetovým uživatelům v ČR pomoci rozpoznat a chránit se před škodlivými aktivitami v jejich systémech.	NBÚ/NCKB	průběžně
Vytvořit v kooperaci se soukromými subjekty jednotné bezpečnostní normy, standardizovat spolupráci a stanovit povinnou úroveň zabezpečení pro subjekty KII.	**D.2.01**	Spolupracovat se soukromoprávními subjekty KII při vytváření požadavků na bezpečnostní normy a povinné úrovně zabezpečení pro subjekty KII.	NBÚ/NCKB	průběžně
	D.2.02	Podporovat rozvoj norem v oblasti kybernetické bezpečnosti prostřednictvím národních a mezinárodní standardizačních a certifikačních orgánů a institucí a podporovat jejich přijetí u soukromých subjektů.	NBÚ/NCKB	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Zajistit v kooperaci se soukromým sektorem kyberprostor poskytující spolehlivé prostředí pro sdílení informací, výzkum a vývoj a zajistit bezpečnou informační infrastrukturu stimulující podnikání soukromých subjektů v zájmu podpory konkurenceschopnosti všech podnikajících soukromých subjektů v ČR a chránící jejich investice.	**D.3.01**	Propagovat vysokou úroveň kybernetické bezpečnosti ve veřejných službách, a tím maximalizovat využívání systémů eGovernmentu ze strany soukromých organizací i široké veřejnosti.	MPO MV	průběžně
	D.3.02	Koordinovat přechod z protokolu IPv4 na IPv6 a informovat o bezpečnostních rizicích s tímto přechodem spjatých.	MPO *ve spolupráci s:* MV	průběžně
	D.3.03	Podporovat rozšiřování DNSSEC pro zabezpečení webových prezentací a pravidelně monitorovat stav implementace DNSSEC jak ve veřejné správě, tak v národní doméně.cz.	MPO	průběžně
Vzdělávat a provádět osvětu soukromého sektoru v oblasti kybernetické bezpečnosti. Soukromým subjektů tak poskytnout potřebné vedení, jak se správně chovat nejen při mimořádných situacích, respektive při kybernetických incidentech, ale i při každodenní činnosti.	**D.4.01**	Poskytovat poradenství a organizovat vzdělávací a osvětové aktivity pro subjekty soukromé sféry.	NBÚ/NCKB	průběžně
	D.4.02	Podporovat malé a středně velké podniky prostřednictvím informační kampaně ohledně kybernetické bezpečnosti úzce zaměřené na potřeby a jejich možnosti.	NBÚ/NCKB MPO	průběžně
Navyšovat důvěru mezi soukromým sektorem a státem, mimo jiné vytvořením platformy/systému na národní úrovni pro sdílení informací o hrozbách, incidentech a aktuálním ohrožení.	**D.5.01**	Vytvořit mezi NCKB a subjekty KII a VIS platformu na sdílení informací o kybernetických hrozbách a zranitelnostech.	NBÚ/NCKB	Q1 2016

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
E. Výzkum a vývoj / Spotřebitelská důvěra				
Podílet se na národních i evropských výzkumných projektech a aktivitách v oblasti kybernetické bezpečnosti.	**E.1.01**	Zmapovat současný stav VaV zabývajícího se kybernetickou bezpečností a technologiemi používanými v ČR.	NBÚ/NCKB *ve spolupráci s:* MV MO	Q1 2018
	E.1.02	Ve spolupráci s ostatními organizačními složkami státu vypracovat národní koncepci VaV v oblasti kybernetické bezpečnosti.	NBÚ/NCKB *ve spolupráci s:* MV MO Policie ČR TAČR Zpravodajské služby	Q3 2018
	E.1.03	Vypracovat a plnit plán výzkumných aktivit NBÚ v oblasti kybernetické bezpečnosti s ohledem na současné a budoucí potřeby státu.	NBÚ/NCKB *ve spolupráci s:* MO Zpravodajské služby	Q3 2017

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Určit NBÚ jako hlavní kontaktní centrum v oblasti výzkumu v kybernetické bezpečnosti. NBÚ bude přispívat ke koordinaci výzkumných aktivit v této oblasti s cílem zabránit zdvojování výzkumných aktivit. Výzkum v oblasti kybernetické bezpečnosti se tak zaměří na opravdu podstatné problémy a převod výzkumných výsledků do praxe.	**E.2.01**	Vytvořit databázi výzkumných projektů v rámci kybernetické bezpečnosti a podávat z ní informace dalším subjektům.	NBÚ/NCKB	Q1 2019
	E.2.02	Zřídit pracovní skupinu zastoupenou všemi organizačními složkami státu zabývajícími se VaV v oblasti kybernetické bezpečnosti, tj. zejména NBÚ/NCKB, MV, MO, TAČR a zpravodajské služby.	NBÚ/NCKB *ve spolupráci s:* MV MO TAČR Zpravodajské služby	Q3 2017
Spolupracovat se soukromým a akademickým sektorem na vývoji a implementaci technologií využívaných státem k zajištění jejich maximálního zabezpečení a transparentnosti. Testovat a hodnotit míru zabezpečení používaných technologií.	**E.3.01**	Iniciovat a podílet se na realizaci výzkumných projektů s partnery ze soukromé sféry.	NBÚ/NCKB	průběžně
Spolupracovat s akademickou a soukromou sférou na výzkumných projektech (včetně primárního i experimentálního výzkumu) a aktivitách v technologické i společenskovědní oblasti, a to především na národní, evropské i mezinárodní transatlantické úrovni.	**E.4.01**	Spolupracovat s akademickou a soukromou sférou na výzkumných projektech, poskytovat jim potřebné informace a strategické vedení. Zapojit ČR a její akademickou i soukromou sféru do výzkumných programů (zahrnujících základní i aplikovaný výzkum a vývoj) na evropské i mezinárodní a transatlantické úrovni.	NBÚ/NCKB MŠMT	průběžně
	E.4.02	Podporovat a podílet se na publikační činnosti akademické sféry v oblasti kybernetické bezpečnosti.	NBÚ/NCKB	průběžně
Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec

F. Podpora vzdělávání, osvěta a rozvoj informační společnosti				
Navyšovat povědomí a gramotnost v otázkách kybernetické bezpečnosti jak u žáků a studentů základních a středních škol, tak i u široké veřejnosti, respektive koncových uživatelů, pomocí podpory iniciativ a osvětových kampaní, pořádáním konferencí pro veřejnost apod.	**F.1.01**	Podporovat iniciativy a osvětové kampaně, pořádat konference a workshopy pro veřejnost, respektive koncové uživatele.	NBÚ/NCKB *ve spolupráci s:* MPSV	průběžně
	F.1.02	Provozovat a kontinuálně aktualizovat portál GovCERT.CZ jako informační platformu pro veřejnost ohledně aktuálních bezpečnostních hrozeb, rizik, zranitelností a dalších aktivit NBÚ.	NBÚ/NCKB	průběžně
	F.1.03	Vytvořit e-learningovou platformu pro vzdělávání širší a odborné veřejnosti.	NBÚ/NCKB *ve spolupráci s:* MPSV	Q1 2016
Modernizovat stávající vzdělávací programy na základní a středoškolské úrovni a podporovat na vysokoškolské úrovni nové studijní programy, které budou přímo vzdělávat experty na kybernetickou bezpečnost.	**F.2.01**	Modernizovat rámcové vzdělávací programy na základní a středoškolské úrovni.	NBÚ/NCKB MŠMT	Q1 2017
	F.2.02	Připravit metodické pokyny a materiály usnadňující školám zapracování problematiky kybernetické bezpečnosti do školních vzdělávacích programů podle nových rámcových vzdělávacích programů.	NBÚ/NCKB MŠMT	Q1 2017
	F.2.03	Připravit dostatek metodických materiálů pro učitele, zajistit vzdělávání učitelů v této oblasti a připravit dostatek výchozích učebních materiálů pro žáky.	NBÚ/NCKB MŠMT	Q1 2017
	F.2.04	Vytvořit přehled vysokoškolských studijních programů v ČR i zahraničí zabývajících se kybernetickou bezpečnostní, průběžně jej aktualizovat a tento přehled v rámci propagace zveřejňovat.	NBÚ/NCKB	Q4 2015

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	F.2.05	Zvyšovat povědomí ohledně zodpovědného, bezpečného používání internetu, ICT a nových médií.	NBÚ/NCKB *ve spolupráci s:* MPSV	průběžně
	F.2.06	Podporovat u studentů rozvoj talentu v oblasti kybernetické bezpečnosti ve spolupráci s vysokými školami.	NBÚ/NCKB	průběžně
	F.2.07	Zprostředkovávat vysokoškolským studentům možnost stáže v oblasti kybernetické bezpečnosti v ČR i zahraničí.	NBÚ/NCKB MO	průběžně
	F.2.08	Spolupracovat na vytváření nových vysokoškolských studijních oborů v oblasti kybernetické bezpečnosti a kybernetické obrany a spolupracovat s univerzitami a vysokými školami při zavádění těchto nových oborů, tvorbě učebních plánů apod.	NBÚ/NCKB MO	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Vzdělávat a školit zaměstnance veřejné správy působící nejen v oblasti kybernetické bezpečnosti a informační kriminality.	**F.3.01**	Školit stávající zaměstnance veřejné správy v oblasti kybernetické bezpečnosti.	NBÚ/NCKB MPSV MV	Od Q4 2015 průběžně
	F.3.02	Školit manažery kybernetické bezpečnosti ve veřejné správě ve věci rozpoznávání, (např. detekování anomálií), hlášení kybernetických bezpečnostních incidentů a další spolupráce s NCKB.	NBÚ/NCKB MPSV	průběžně
	F.3.03	Institucionalizovat další vzdělávání prostřednictvím získávání osvědčení za absolvování vzdělávacích programů.	NBÚ/NCKB MPSV MV	průběžně
	F.3.04	Pomocí moderních výukových metod zvyšovat úroveň vzdělanosti v oblasti kybernetické bezpečnosti.	NBÚ/NCKB MPSV	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
G. Podpora rozvoje schopností PČR vyšetřovat a postihovat informační kriminalitu				
Posílit personálně jednotlivá policejní pracoviště informační kriminality.	**G.1.01**	Personálně posílit pracoviště informační kriminality Policejního prezidia ČR o systemizovaná služební místa a systemizovaná pracovní místa, která budou sanovat stávající krizový stav a dále nyní naplní nezbytný lidský potenciál pro plnění vyžadovaných a stanovených činností.	Policie ČR MV	do 2018
	G.1.02	Personálně posílit o systemizovaná služební místa, ÚOOZ SKPV, ÚOKFK SKPV a NPC SKPV s ohledem na vyšetřování návazné trestné činnosti související s informační kriminalitou, včetně oblasti boje s terorismem zasahujícím i prostředí informačních technologií.	Policie ČR MV	do 2018
	G.1.03	Personálně posílit jednotlivá regionální výkonná pracoviště SKPV určených pro informační kriminalitu o systemizovaná služební místa a systemizovaná služební místa v jednotlivých krajích. Tímto se sleduje reakce na lokální situaci v rámci regionálních součástí SKPV dle modelu respektujícího rozdělení na technický, operativní a procesní aspekt zastoupení na příslušném pracovišti informační kriminality, zajištěním dostatečné sanace stávajícího stavu, pokrytí vedení odborně náročného trestního řízení a zajištění akceschopnosti.	Policie ČR MV	do 2018

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	G.1.04	Personálně posílit infastrukturu regionálních znaleckých pracovišť PČR o systemizovaná služební místa. Kriminalistický ústav Praha v souvislosti s jeho republikovou působností posílit o systemizovaná služební místa, která budou sanovat stávající nesoulad poměru zajišťované činnosti a personálních kapacit.	Policie ČR MV	do 2018
	G.1.05	Personálně posílit ÚZČ SKPV v oblasti programování o systemizovaná služební místa, v oblasti technické správy systémů o systemizovaná služební místa, která budou zajišťovat přijímání, zpracování a vyřizování rostoucích požadavků a zejména objemu dat charakteru provozních a lokalizačních údajů sítě Internet.	Policie ČR MV	do 2018
	G.1.06	Personálně posílit o systemizovaná služební místa ÚSČ SKPV pro podporu speciálních činností v souvislosti s penetrací informačních technologií i do oblastí zajišťování úkonů souvisejících s vyšetřováním trestné činnosti	Policie ČR MV	do 2018
	G.1.07	Personálně posílit technologickou správu dat a informační podporu zabezpečovanou pracovišti informatiky a provozu informačních technologií.	Policie ČR MV	do 2018

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Modernizovat technologické vybavení odborných policejních pracovišť.	**G.2.01**	Nastavit povinnou a vynutitelnou minimální technologickou vybavenost všech pracovišť OIK SKPV a zajistit stanovenou techniku a technologie.	Policie ČR MV	do 2018
	G.2.02	Nastavit povinnou a vynutitelnou minimální technologickou vybavenost všech znaleckých pracovišť tzv. počítačové analýzy a zajistit stanovenou techniku a technologie.	Policie ČR MV	do 2018
	G.2.03	Společně plánovat jednotlivé nákupy pro výkonná pracoviště OIK a znalecká pracoviště počítačové analýzy s garancí vázanosti plánovaných prostředků v plánovaných rozpočtech pro další údobí.	Policie ČR MV	do 2018
	G.2.04	Postupně realizovat vzájemnou blízkost dislokací výkonných a znaleckých pracovišť SKPV na jednotlivých úrovních v závislosti na vývoji stávajících dislokací.	Policie ČR MV	do 2018
Zakotvit vazby přímé a rychlé spolupráce se zainteresovanými národními subjekty a ostatními bezpečnostními složkami pro oblast informační kriminality.	**G.3.01**	Vytvořit smluvní či obdobné vazby umožňující a garantující přímou a časově nejrychlejší spolupráci na prováděcí úrovni s bezpečnostními složkami BIS, ÚZSI a VZ a s prvky kritické infrastruktury, NCKB, GovCERT.CZ a národním CERT.	Policie ČR MV *ve spolupráci s:* Vojenská policie	Q3 2016

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Podpořit spolupráci se zahraničními subjekty v oblasti výměny informací k informační kriminalitě a v oblasti vzdělávání.	**G.4.01**	Spolupracovat se zahraničními subjekty v oblasti výměny informací k informační kriminalitě a v oblasti vzdělávání.	Policie ČR MV *Ve spolupráci s:* Vojenská policie	průběžně
Odborně vzdělávat a školit policejní specialisty.	**G.5.01**	Rozšířit kurzy kvalifikační přípravy o základní znalosti a dovednosti spojené s kriminalitou páchanou v prostředí informačních technologií a zavést elektronický nebo obdobně plošně nasaditelný systém průběžného vzdělávání.	Policie ČR MV	průběžně, do Q2 2017
	G.5.02	Rozšířit specializační kurzy pro policisty SKPV o vyšší znalosti a dovednosti spojené s kriminalitou páchanou v prostředí informačních technologií.	Policie ČR MV	průběžně, do Q2 2017
	G.5.03	Připravit odborné kurzy policejních specialistů na kriminalitu páchanou v prostředí informačních technologií.	Policie ČR MV	průběžně, do Q2 2017
	G.5.04	Vytvořit podmínky pro průběžné vzdělávání expertů PČR v oblasti informační kriminality v komerčním a akademickém prostředí.	Policie ČR MV	průběžně, do Q2 2017

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
	G.5.05	Kapacitně posílit a rozšířit podmínky pro jazykové studium specialistů ve formě všeobecné jazykové přípravy, odborné jazykové přípravy a zdokonalovacích kurzů a souběžně zohlednit další nábory s preferencí jazykové vybavenosti.	Policie ČR MV	průběžně, do roku 2017
Vybudovat multidisciplinární akademické prostředí pro podporu rozvoje schopností PČR postihovat informační kriminalitu.	**G.6.01**	Vybudovat multidisciplinární formalizované akademické prostředí rozvoje schopnosti bezpečnostních složek a zejména PČR postihovat informační kriminalitu a řešit s tím spojené bezpečnostní, standardizační, normotvorné, výzkumné a další provázané potřeby.	Policie ČR MV	průběžně do roku 2018

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
H. Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce) Účast na tvorbě a implementaci evropských a mezinárodních pravidel				
Na základě systematického přístupu, tj. vzhledem k existujícím právním předpisům, vytvářet v oblasti kybernetické bezpečnosti srozumitelné, efektivní a proporcionální právní předpisy.	**H.1.01**	Vytvářet v oblasti kybernetické bezpečnosti srozumitelné, efektivní a proporcionální zákonné a podzákonné právo.	NBÚ/NCKB *ve spolupráci s:* MZV	průběžně
	H.1.02	Analyzovat nezbytné zákonné regulace pro účinné zajištění kybernetické bezpečnosti v ČR.	NBÚ/NCKB *ve spolupráci s:* MZV	průběžně
Aktivně se účastnit tvorby a implementace evropských a mezinárodních pravidel.	**H.2.01**	Kontinuálně se podílet na vývoji a implementaci evropského a mezinárodního právního rámce a pravidel v oblasti kybernetické bezpečnosti.	NBÚ/NCKB MZV	průběžně
	H.2.02	Účastnit se diskuzí nad pojetím a významem konceptů kybernetické bezpečnosti a kybernetické obrany.	NBÚ/NCKB MZV MO MV Zpravodajské služby	průběžně

Hlavní cíle	Kód	Úkoly	Odpovědný subjekt	Časový rámec
Provádět jak kontinuální analýzu efektivity účinné právní úpravy a jejího souladu s aktuálními poznatky z dotčených technických a společenskovědních oborů, tak i průběžné provádění změn a doplňování tak, aby právní úprava odpovídala aktuálním požadavkům bezpečné informační společnosti.	**H.3.01**	Na základě průběžné analýzy efektivity účinné právní úpravy a jejího souladu s aktuálními poznatky z dotčených technických a společenskovědních oborů provádět příslušné změny a doplňování.	NBÚ/NCKB	průběžně
	H.3.02	Nastavovat povinnou úroveň zabezpečení pro subjekty KII pomocí aktualizace zákonného a podzákonného práva.	NBÚ/NCKB	průběžně
	H.3.03	Provést revizi a vytvořit návrh legislativních změn vybraných paragrafů trestního zákoníku a zákona o elektronických komunikacích, které by zefektivnily vyšetřování a postihování informační kriminality a reflektovaly aktuální situaci v problematice informační kriminality.	MV Policie ČR ČTÚ *ve spolupráci s:* Zpravodajské služby	Q1 2016
Podporovat vzdělávání v problematice kybernetické bezpečnosti v rámci justičních orgánů (tj. státních zástupců nebo soudců).	**H.4.01**	Pomocí vzdělávání soudců a státních zástupců ohledně kybernetické problematiky zajistit ukládání a vymáhání přiměřených sankcí v trestněprávních sporech, které zahrnují kybernetickou problematiku.	NBÚ/NCKB MS MV Policie ČR	průběžně

PŘÍLOHA P III: DOTAZNÍK VÝZKUMU POCITU BEZPEČÍ OBČANŮ MORAVSKOSLEZSKÉHO KRAJE

Příloha 3 Dotazník pocitu bezpečí

1. Považujete Moravskoslezský kraj za bezpečný kraj?

a) rozhodně ano b) spíše ano c) nevím d) spíše ne e) rozhodně ne

2. Existuje místo (či místa) v Moravskoslezském kraji, která považujete za nebezpečná?

a) ano b) ne c) nevím

3. Pokud takové místo (či místa) existují, která to jsou a proč? Prosím, vypište je:

……

4. Považujete obec, v níž žijete, za bezpečnou?

a) rozhodně ano b) spíše ano c) nevím d) spíše ne e) rozhodně ne

5. Existuje místo (či místa) ve vaší obci, která považujete za nebezpečná?

a) ano b) ne c) nevím

6. Pokud takové místo (či místa) existují, která to jsou a proč? Prosím, vypište je:

……

7. Je ve vaší obci místo, které lze vnímat jako sociálně vyloučenou lokalitu?

a) ano b) ne c) nevím

8. Pokud takovou lokalitu (lokality) znáte, které to jsou? Prosím, vypište je:

……

9. Uveďte, proč toto místo (tato místa) za sociálně vyloučenou lokalitu považujete. V této otázce můžete označit více odpovědí.

a) místo je prostorově vyloučené

b) jde o místo s vysokou koncentrací obyvatel jiného etnika

c) jde o místo s vysokou koncentrací nezaměstnaných osob

d) jde o místo s vysokou koncentrací osob závislých na návykových látkách

e) jde o místo se zhoršenou kvalitou bydlení

f) jde o místo se zhoršenou kvalitou životního prostředí

g) jiný důvod – uveďte jaký: ……

10. Které skupiny obyvatel považujete za nejsnadnější oběti trestné činnosti? V této otázce můžete označit více odpovědí.

a) děti
b) mladiství
c) ženy
d) osoby bez přístřeší
e) lidé se zdravotním handicapem
f) etnické menšiny
g) cizinci
h) jiné osoby – uveďte jaké:……
i) náboženské menšiny
j) jiné minoritní skupiny
k) senioři

11. Které skupiny obyvatel považujete za nejčastější pachatele trestné činnosti?

V této otázce můžete označit více odpovědí.

a) děti a mladiství
b) bezdomovci
c) alkoholici
d) fotbaloví fanoušci
e) etnické menšiny
f) podnikatelé
g) ekon. dobře zajištění lidé
h) extremisté
i) drogově závislí
j) sociálně vyloučené osoby
k) agresivní řidiči
l) náboženské menšiny
m) úředníci
t) gambleři
n) již někdy trestané os./recidivisté
o) cizinci
p) lidé s duševním onemocněním
q) politici (veřejní činitelé)
r) organizované zločinecké skup.
s) osoby s nedostatečným příjmem
u) jiné osoby – uveďte jaké:…….

12. Zhodnoťte míru vlivu vybraných oblastí a jevů na existenci kriminality. Ke každému pojmu přiřaďte křížek k vybranému hodnocení. Význam bodů: 1 = maximální vliv, 5 = žádný vliv, 6 = nevím nebo nechci odpovídat.

	1	2	3	4	5	6
Úroveň školství						
Úroveň zdravotnictví						
Sociální a ekonomická situace						
Nezaměstnanost						

Legislativa						
Vývoj politické situace						
Úroveň životního prostředí						
Přistěhovalectví						
Jiný jev – vypište jaký:……						

13. Vyjádřete svou míru obavy z vybraných druhů protiprávního jednání (protiprávní jednání zahrnuje zejména přestupky, trestné činy, správní a jiné delikty). Ke každému pojmu přiřaďte křížek k vybranému hodnocení. Význam bodů: 1 = maximální strach, 5 = žádná obava, 6 = nevím nebo nechci odpovídat.

	1	2	3	4	5	6
Krádež						
Loupež						
Vandalismus						
Rušení nočního klidu						
Stalking (pronásledování)						
Šikanování						
Přepadení						
Sexuální obtěžování						
Pohlavní zneužívání						
Znásilnění						
Podvod						
Neoprávněné nakládání s osobními údaji (zneužití osobních dat)						
Ublížení na zdraví						

Vražda						
Vydírání						
Korupce						
Domácí násilí						
Nekalý podomní prodej a veřejné prodejní						
Jiné protiprávní jednání – vypište jaké: ……						

14. Stal/a jste se někdy obětí trestné činnosti?

a) ano b) ne c) nepamatuji se

15. Pokud ano, uveďte prosím, o jakou trestnou činnost či protiprávní jednání se jednalo? V této otázce můžete označit více odpovědí.

a) krádež do 5 000 Kč
b) krádež nad 5 001 Kč výše
c) vandalismus
d) stalking (pronásledování)
e) šikanování
f) domácí násilí
g) přepadení
h) sexuální obtěžování
i) pohlavní zneužívání
j) znásilnění
k) neoprávněné nakládání s os. údaji
l) jiné protiprávní jednání – uveďte jaké:
m) podvod
n) ublížení na zdraví
o) vydírání
p) korupce

……

16. Pokud jste se již někdy stal/a obětí trestné činnosti, na koho jste se obrátil/a s žádostí o pomoc? Pokud jste se obětí trestné činnosti ještě nestal/a, prosím označte, na koho byste se v takovém případě obrátil/a. V této otázce můžete označit více odpovědí.

a) na nikoho – pomůžu si sám/a
b) na rodinu a příbuzné
c) na přátele/známé
d) na městskou policii
e) na Policii ČR
f) na lékaře
g) na právníka
h) na Státní zastupitelství
i) na soud
j) na obecní úřad
k) na pojišťovnu
l) jiná varianta – uveďte:

……..

17. V případě, že jste se již někdy stal/a obětí trestné činnosti a něčí pomoci jste využil/a, byla tato pomoc efektivní? Uveďte také důvod proč ano nebo proč ne.

a) ano b) ne c) nevím/nepamatuji se

Důvod:……

18. Bylo v blízkosti Vašeho bydliště již někdy spácháno nějaké protiprávní jednání?

a) ano b) ne c) nevím

19. Bylo v rámci Vaší rodiny, přátel či známých již někdy spácháno nějaké protiprávní jednání?

a) ano b) ne c) nevím

20. Zhodnoťte práci institucí/subjektů, které se na zajištění bezpečnosti občanů podílejí. Ke každému pojmu přiřaďte křížek k vybranému hodnocení. Význam bodů: 1 = výborná, 5 = zcela nedostačující, 6 = nevím nebo nechci odpovídat.

	1	2	3	4	5	6
Městská policie						
Úroveň zdravotnictví						
Sociální a ekonomická situace						
Policie ČR						
Státní zastupitelství						
Soudy						
Armáda ČR						
Bezpečnostní agentury						
Hasičské sbory						
Jiný subjekt – vypište jaký: ……						

21. Uveďte, které činnosti či aktivity podle Vašeho názoru spadají pod prevenci kriminality. Odpovědi vypište:

……

22. Myslíte si, že jsou ve vaší obci realizována nějaká preventivní opatření proti kriminalitě?

a) ano b) ne c) nevím

23. Pokud ano, jaká opatření to jsou? Odpovědi vypište:

……

24. Jaká preventivní opatření proti kriminalitě Vám ve vaší obci chybí, a proč? Odpovědi vypište:

……

25. Zhodnoťte efektivitu níže uvedených opatření k prevenci kriminality v obci. Ke každému pojmu přiřaďte křížek k vybranému hodnocení. Význam bodů: 1 = výborná, 5 = zcela nedostačující, 6 = nevím nebo nechci odpovídat.

	1	2	3	4	5	6
Kamerový systém						
Bezpečnostní stojany na kola						
Mříže, ploty, bezpečnostní dveře apod.						
Pulty centralizované ochrany napojené na hlídací agentury						
Asistenti prevence kriminality						
Informační kampaň (letáky, v TV, v dopravních prostředcích)						
Vzdělávání a přednášky						
Pouliční osvětlení						
Přítomnost policie v ulicích						
Podpora práce neziskových org. pracujících s rizikovými skupinami						
Poradenství						

Léčebné a resocializační programy						
Sportovní aktivity						
Terénní sociální práce						
Alternativní tresty						
Radary na měření rychlosti, zpomalovací prahy na silnicích						
Jiné opatření – vypište jaké: ……						

26. Označte, které služby sociální prevence znáte (resp. víte, že existují). V této otázce můžete označit více odpovědí.

a) intervenční centra

b) telefonická krizová pomoc

c) kontaktní centra

d) azylové domy

e) domy na půl cesty

f) nízkoprahová denní centra

g) nízkoprahová zařízení pro děti a mládež

h) noclehárny

i) služby následné péče

j) sociálně aktivizační služby (SAS) pro rodiny s dětmi

k) terapeutické komunity

l) terénní programy

m) krizová pomoc

n) sociální rehabilitace

o) jiné služby – uveďte jaké:……

p) žádnou z uvedených služeb neznám

27. Používáte sami nějaká opatření pro zvýšení vlastní bezpečnosti a ochraně majetku?

a) ano b) ne c) nevím

28. Pokud ano, označte, které opatření využíváte. V této otázce můžete označit více odpovědí.

a) důsledné zamykání bytu/domu

b) nenosím u sebe téměř žádnou hotovost

c) mám cennosti a peníze uložené v bance

h) mám u bytu/domu kamerový systém

i) mám na oknech bytu/domu mříže

j) nevpouštím domů cizí osoby

d) pozdě večer nevycházím z bytu/domu k) mám trezor

e) mám střelnou zbraň l) mám psa či jiné hlídací zvíře

f) mám pepřový sprej nebo paralyzér m) mám alarm v autě

g) absolvoval/a jsem kurz sebeobrany n) mám zabezpečovací zařízení domu

o) jiné opatření – uveďte jaké:……

Identifikační otázky:

1. Jaké je Vaše pohlaví?

a) muž b) žena

2. Kolik je Vám let? Prosím, vypište: …….

3. Jaké je Vaše nejvyšší dosažené vzdělání?

a) bez vzdělání c) vyučen e) SŠ bez maturity g) VŠ

b) ZŠ d) VOŠ f) SŠ s maturitou h) postgraduální

4. Jaký je Váš rodinný stav?

a) svobodný/á b) ženatý/vdaná c) rozvedený/á d) vdovec/vdova

e) registrované partnerství

5. Ve které obci bydlíte? Prosím, vypište její název a zařazení do okresu či ORP (pokud nevíte, nemusíte bližší zařazení obce pod okres či ORP uvádět).

……..

6. Jaký je Váš ekonomický status?

a) student/studentka/připravuji se na budoucí povolání

b) matka/otec na mateřské/rodičovské dovolené

c) zaměstnanec d) nezaměstnaný/á

e) živnostník/OSVČ/podnikatel f) žena/muž v domácnosti

g) důchodce/důchodkyně

h) jiná profese – uveďte jaká:……

PŘÍLOHA P IV: METODIKA PRO TVORBU STRATEGICKÝCH DOKUMENTŮ PREVENCE KRIMINALITY A VÍCELETÝCH BEZPEČNOTNÍCH ANALÝZ

Příloha 4 Metodika prevence kriminality

A. Bezpečnostní analýza na úrovni obce či regionu

1. Bezpečnostní analýza na úrovni obce:

- **analýza protiprávních činů (přečiny, zločiny, přestupky)** = vývojové trendy trestné činnosti (analýzu kriminality) a přestupků,
- **sociální analýza (**vybrané ukazatele, které souvisí s vývojem kriminálně rizikových jevů = nezaměstnanost, sociální dávky odrážející míru chudoby**)**
- **institucionální analýza** (subjekty, které působí preventivně a ovlivňují úroveň veřejného pořádku a bezpečnosti).

Předpokladem analýzy kriminality je průběžné vyhodnocování statistik sledovaných typů trestné činnosti a využití podnětů Policie ČR ke zpracování návrhů preventivních opatření; je třeba také sledovat a reagovat na sociálně - demografické ukazatele a posuzovat provázanost činností jednotlivých institucí, míru vzájemné informovanosti a kvalitu spolupráce.

Bezpečnostní analýza bude obsahovat minimálně následující údaje o přečinech, zločinech a přestupcích, všechny za území obce (správní obvod v případě obcí s rozšířenou působností):

- trestné činy minimálně za minulé 2 roky (ideálně déle a sledovat trendy/vývoj), meziroční srovnání a index na 10 tisíc obyvatel*, včetně meziroční změny v indexu, trestná činnost bude uvedena ve struktuře:

Kriminalita (přečiny i zločiny)

Rok	Celkem	Násilná	Mravnostní	Majetková

***** index se spočítá: (počet trestných činů / počet obyvatel obce, správního obvodu ORP, okresu či kraje) x 10 000

Pachatelé

Rok	Věk 0-14 let	15 -17 let	18 a více let	Recidivisté

Oběti

Rok	Děti (0-18 let)	Ženy	Osoby starší 65ti let

- **Data o vybraných druzích přestupků -** pro účely analýzy je nezbytné shromáždit a analyzovat data o následujících druzích přestupků:
  - proti veřejnému pořádku,
  - proti občanskému soužití,
  - proti majetku,
  - přestupky na úseku ochrany před alkoholismem a jinými toxikomaniemi,
  - přestupky proti obecně závazným vyhláškám v oblasti bezpečnosti a veřejného pořádku.

Data o všech uvedených přestupcích dodají obci subjekty, v jejichž kompetenci je řízení o jednotlivých druzích přestupků, tj. obce s rozšířenou působností (včetně dat z městských policií), obce a Policie ČR. Údaje budou uspořádány do tabulky podle jednotlivých druhů přestupků, a to za území (nebo správní obvod) obce.

	počet obyvatel		**přestupky – abs. počet**			**index na 10 tis. obyv.**			
druh	k 31.12. 201y*	změna proti roku 201x*	rok 201x	**k 31.12. 201y**	změna 1x-1y	rok 201x	**rok 201y**	změna 1x-1y (index)	změna 1x-1y (%)
Proti veřejnému pořádku									
Proti občanskému soužití									
Proti majetku									
na úseku ochrany před alkoholismem a jinými toxikomaniemi									
přestupky proti obecně závazným vyhláškám v oblasti bezpečnosti a veřejného pořádku									

*rok x = např. 2014, rok y = např. 2015

Sociálně-demografická část analýzy bude obsahovat minimálně:

- počet nezaměstnaných za rok x, y, meziroční srovnání a index na 10 tisíc obyvatel
- počet vyplacených sociálních dávek závislých na výši příjmu na území obce respektive ve správním obvodu okresu či ORP (dávky hmotné nouze: příspěvek na živobytí, doplatek na bydlení, mimořádná okamžitá pomoc; dávky státní sociální podpory: sociální příplatek, příspěvek na bydlení) za rok x, y, meziroční srovnání a index na 1 tisíc obyvatel,

- existence sociálně vyloučených lokalit na území obce – uvést název lokality, její stručný popis a odhadovaný počet obyvatel, včetně jejich národnostního složení,
- další rizikové sociální faktory.

Institucionální analýza

Cílem institucionální analýzy je získat přehled a provést vyhodnocení dosavadních aktivit orgánů státní správy, samosprávy, nestátních neziskových organizací a dalších institucí působících v oblasti sociální a situační prevence[1] s důrazem na prevenci sekundární a terciární[2]. Důležité je také posoudit míru jejich vzájemné informovanosti, kvalitu spolupráce a vytipování duplicitních, neefektivních, případně chybějících aktivit a služeb. Při zpracování institucionální analýzy lze využít všechny dostupné strategické, koncepční a přehledové materiály, které jsou, byť i jen částečně obsahově průnikové s oblastí prevence kriminality (může se jednat např. o plány rozvoje města, komunitní plány, přehledy zařízení a služeb různých resortů apod.).

Standardně by analýza měla obsahovat informace o následujících konkrétních institucích (subjektech, zařízeních, službách):

- v rámci referátu sociálních věcí: OSPOD, sociální kurátoři, sociální asistenti, protidrogový koordinátor a romský poradce,
- výchovné ústavy, ústavy sociální péče, věznice, pedagogicko-psychologické poradny, střediska výchovné péče, azylové domy, domy na půl cesty, poradny AT, kontaktní centra, noclehárny pro osoby bez přístřeší, DDM, komunitní centra, občanské poradny, poradny pro rodinu, stacionáře, nízkoprahová centra, streetwork, linky důvěry a případně další subjekty a zařízení,
- podrobný přehled aktivit nestátních neziskových a charitativních organizací, které působí v oblasti sociální prevence, zejména pokud je jejich činnost zaměřena na problémové a rizikové cílové skupiny, nebo poskytují pomoc obětem trestné činnosti,
- informace o činnosti PMS[3],
- stručný přehled nabídky zájmové a sportovní činnosti pro děti i dospělé ve městě, informace o školách a školních klubech a o sportovních nebo jiných zájmových klubech a zařízeních.

---

[1]/ Jedná se v podstatě o audit subjektů, činností a služeb v této oblasti, při jehož zpracování je možné s výhodou využít podkladů pro komunitní plány měst.

[2]/ Sekundární prevence je zaměřena na rizikové skupiny osob, u nichž je zvýšená pravděpodobnost, že se stanou pachateli nebo oběťmi trestné činnosti (specializovaná sociální péče), na sociálně patologické jevy (např. vandalismus, šikana, záškoláctví, rasové konflikty apod.) a na příčiny kriminogenních situací (dlouhodobá nezaměstnanost, chudoba apod.). Terciární prevence se soustřeďuje na kriminálně narušené jedince a na prokriminální sociální prostředí.

[3]/ Zvláště uvést střediska PMS se specializovaným oddělením pro mládež.

Součástí institucionální analýzy by mělo být rovněž zhodnocení spolupráce všech zainteresovaných subjektů v systému intervence a následné péče o delikventní nebo delikvencí ohrožené děti a mládež (příslušné komise MÚ nebo magistrátu, Policie ČR, MP, soudy, PMS, PPP nebo další specializovaná zařízení, NNO). **Podstatnou informací je, zda existuje komise, pracovní skupina apod. pro prevenci, pokud ne, musí být založena podle doporučení OBPPK MV.**

Syntéza poznatků s návrhy řešení a komentář k bezpečnostní analýze

Doporučujeme zpracovat stručný komentář a interpretaci statistických výstupů, které budou obsahovat označení nejvíce problémových lokalit a hlavních bezpečnostních problémů vyplývajících z údajů o přečinech a zločinech, přestupcích, jejich pachatelích a obětech i o jejich teritoriálním rozložení. Obecné výstupy naznačené v tabulkách je možné a žádoucí dále konkretizovat a zajistit si tak argumenty pro zvolenou podobu Žádosti obce/kraje na konkrétní rok.

- **identifikace problémů** a/nebo rizik, které je nutné řešit,
- **způsob řešení a identifikace subjektů**, které se budou na realizaci plánu (způsobech řešení) podílet,
- **integrace navrhovaných opatření** k řešení identifikovaných problémů a/nebo rizik do celkového (komplexního) řešení nebo odstranění problému/rizika,
- **finanční zajištění** navrhovaných opatření,
- **vymezení aktivit** (dílčích projektů),
- **způsob měření efektivity dopadů** jednotlivých opatření, aktivit a projektů,
- **rozdělení odpovědností** za realizaci plánu.

2. Bezpečnostní analýza na úrovni kraje

Analýza obsahuje zejména:

- Data o kriminalitě
- Data o nezaměstnanosti a sociálních dávkách
- Případná další relevantní data
- Analýzu všech uvedených dat

Data o kriminalitě

- Za dodání údajů o kriminalitě odpovídá Policie ČR – krajské ředitelství Policie ČR (pracovník odpovědný za prevenci kriminality KŘ P ČR)
- Policie ČR (dále jen „P ČR“) provede také základní analýzu dat – popíše strukturu trestné činnosti (přečinů i zločinů), pachatelů a teritoriální rozložení kriminality podle jednotlivých obvodních (místních) oddělení P ČR,

- analýza může být při respektování struktury kraj →územní odbor→obvod zpracována mnohem detailněji, dále uvedené výstupy jsou považovány za základní (povinné),
- krajem se vždy rozumí VÚSC (nikoliv „policejní kraj“),
- důležitým krokem ve zpracování analýz kriminality je zajistit porovnatelnost (indexaci) sledovaných kriterií na nižší úrovni než jsou okresy, tzn. na úrovni obvodních (místních) oddělení P ČR,
- nezbytnými údaji pro analýzu na úrovni obvodních (místních) oddělení P ČR jsou počty obyvatel žijících v územní působnosti těchto oddělení, které zpracuje a dodá pracovníkovi odpovědnému za prevenci kriminality KŘ P ČR manažer prevence kriminality kraje (VÚSC),
- návod pro postup při zjišťování počtu obyvatel v působnosti jednotlivých obvodních (místních) oddělení P ČR:
  - z webové stránky ČSÚ www.czso.cz/csu/redakce.nsf/i/regiony_mesta_obce_souhrn se lze dostat k seznamům obcí v kraji s uvedeným počtem jejich obyvatel. Seznamy lokalit zahrnutých do působnosti jednotlivých OO P ČR nejsou však shodné se seznamem obcí uvedeným ve statistickém přehledu ČSÚ, protože zahrnují jak obce samosprávné (s vlastním obecním úřadem), tak i další lokality (osady, samoty), které jsou však vždy registrovány jako „části obce“ některé z obcí v seznamu ČSÚ uvedených. Obyvatelé „částí obcí“ jsou již započítáni ve statistikách obcí, ke kterým přísluší → tzn. pro zjištění počtu obyvatel v působnosti konkrétního OO PČR stačí sečíst počty obyvatel obcí uvedených ve statistice ČSÚ[4],
  - sestavení pořadí zatíženosti obvodních (místních) oddělení policie provede na základě indexace P ČR[5].

Statistické výstupy ke kriminalitě od P ČR[6]

Úroveň kraje (VÚSC)

Celková kriminalita

Tabulka č. 1: sestavení pořadí zatíženosti v krajích v roce 201y v porovnání s rokem 201x

	počet obyvatel			**celková TČ – abs. Počet**			**index na 10 tis. obyv.**			
kraj	k 31.12. 201y	změna proti roku 201x	rok 201x	**k 31.12. 201y**	změna 1x-1y	rok 201x	**rok 201y**	změna 1x-1y (index)	změna 1x-1y (%)	**pořadí dle indexu 201y**
čr										
PHA										
STČ										

[4] Zda se jedná o část obce a k jaké samosprávné obci přísluší lze ověřit na stránce ČSÚ „části obcí“, adresa - http://www.czso.cz/cz/cisla/1/13/130704/data/castiob2004.xls.
[5] Index = přepočet na 10000 obyvatel= počet TČ / počet obyvatel v působnosti OO PČR x 10000.
[6] Údaje ke kriminalitě do úrovně jednotlivých obvodních (místních) oddělení P ČR poskytne všem krajům odbor prevence kriminality, a to po 20. lednu následujícího roku po roku, za který jsou požadovány, jakmile budou k dispozici.

JČ										
PL										
KV										
ÚST										
LB										
KH										
PA										
VY										
JM										
OL										
MS										
ZL										

Pozn.: *Tuto tabulku na vyžádání zpracuje a dodá manažerům prevence kriminality krajů odbor prevence kriminality MV.*

- *Pokud bude kraj v Koncepci řešit z hlediska prevence kriminality specifické oblasti (domácí násilí, stalking, extremismus, apod.), musí být uvedena také data o trestné činnosti v daných oblastech.*

Tabulka č. 2: vývoj kriminality ČR a kraje (VÚSC) v letech 2012 – 2015 – celková kriminalita

evidovaná celková TČ- abs. počet **meziroční odchylky v %**

kraj	2012	2013	2014	2015	12-13	13-14	14-15	**12 – 15****
ČR								
PHA								
STČ								
JČ								
PL								
KV								
ÚST								
LB								
KH								
PA								
VY								
JM								
OL								
MS								
ZL								

* Data budou k dispozici po 15. lednu 2016, poskytne je na vyžádání odbor prevence kriminality MV.

** Porovnání situace v roce 2012 a v roce 2015.

Pozn.:

- *Obdobné meziroční porovnání míry kriminality a porovnání let 2012 a 2015 může být provedeno na indexovaných údajích vztažených k počtu obyvatel.*
- *Tuto tabulku zpracuje a dodá manažerům prevence kriminality krajů odbor prevence kriminality MV.*

Tabulka č. 3: Skladba kriminality v kraji YZ – porovnání s ČR za rok 201z* (základ, tj. 100% = celková kriminalita)

	ČR – počet	ČR - %	kraj – počet	kraj - %	odchylka (%) kraj – ČR
celková TČ		100		100	
z toho:					
majetková					
násilná + mravnostní					
ostatní kriminalita[7]					
zbývající kriminalita[8]					
hospodářská					

Pozn.: *Tuto tabulku na vyžádání zpracuje a dodá manažerům prevence kriminality krajů odbor prevence kriminality MV.*

Skladba kriminality v kraji YZ – graf

(zde je možné doplnit grafickou podobu Tabulky č. 3 – koláč, sloupečky)

* rok 201z = 2015, v kontextu s roky 201x = 2012 a 201y = 2014

Tabulka č. 4: Skladba násilné kriminality v kraji YZ – porovnání s ČR za rok 201z (základ, tj. 100% = násilná kriminalita[9])

	ČR – počet	ČR - %	kraj – počet	kraj - %	odchylka (%) kraj – ČR
násilná		100		100	
z toho:					
loupeže					
úmyslné ublížení na zdraví					
nebezpečné vyhrožování					
vydírání					

[7]/ Zahrnuje mimo jiné trestné činy výtržnictví, překupnictví, maření výkonu úředního rozhodnutí, sprejerství, výroba jedů.

[8]/ Zahrnuje mimo jiné TČ padělání a pozměňování peněz, opilství + návyk látky, zanedbání povinné výživy, nedbalostní dopravní nehody, ostatní TČ.

[9]/ Tabulka zahrnuje pouze statisticky nejvýznamnější násilné trestné činy evidované v ČR v řádech nad 1 tisíc. Mezi v tabulce nezařazené významnější TČ této skupiny s četností v ČR v řádu stovek patří např. násilí na veřejných činitelích a policistech, omezovaní a zbavení osobní svobody, týrání svěřené osoby, neoprávněné zasahování do práv a další.

porušování dom. svobody					

Pozn.: *Tuto tabulku na vyžádání zpracuje a dodá manažerům prevence kriminality krajů odbor prevence kriminality MV.*

Skladba násilné kriminality v kraji – graf

(zde je možné doplnit grafickou podobu Tabulky č. 4 – koláč, sloupečky)

Tabulka č. 5: Skladba majetkové kriminality v kraji YZ – porovnání s ČR za rok 201z (základ, tj. 100% = majetková kriminalita)

	ČR – počet	ČR - %	kraj – počet	kraj - %	odchylka (%) kraj – ČR
majetková celkem		100		100	
z toho:					
krádeže vloupáním					
krádeže prosté					
ostatní[10]					

Pozn.: *Tuto tabulku na vyžádání zpracuje a dodá manažerům prevence kriminality krajů odbor prevence kriminality MV.*

Skladba majetkové kriminality v kraji YZ – graf (zde je možné doplnit grafickou podobu Tabulky č. 5 – koláč, sloupečky)

Tabulka č. 6: Skladba krádeží prostých v kraji YZ – porovnání s ČR za rok 201z (základ, tj. 100% = krádeže prosté[11])

	ČR – počet	ČR - %	kraj – počet	kraj - %	odchylka (%) kraj – ČR
krádeže prosté celkem		100		100	
z toho:					
kapesní					
jiné na objektech					
motorová vozidla dvoustopá					
věci z aut					
součástky z aut					
jízdní kola					
krádeže v bytech					
v jiných objektech					
ostatní					

[8]/ Zahrnuje TČ podvod, zpronevěru, zatajení cizí věci, poškozování a neoprávněné užívání cizí věci a ostatní TČ.

[11]/ Tabulka zahrnuje jen statisticky nejvýznamnější trestné činy ze skupiny krádeží prostých, v ČR evidovaných v řádu minimálně 1 tisíc.

Pozn.: *Tuto tabulku na vyžádání zpracuje a dodá manažerům prevence kriminality krajů odbor prevence kriminality MV.*

Skladba krádeží prostých v kraji YZ – graf (zde je možné doplnit grafickou podobu Tabulky č. 6 – koláč, sloupečky)

Tabulka č. 7: Skladba krádeží vloupáním v kraji YZ – porovnání s ČR za rok 201z (základ, tj. 100% = krádeže vloupáním[12])

	ČR – počet	ČR - %	kraj – počet	kraj - %	odchylka (%) kraj – ČR
krádeže vloupáním		100		100	
z toho:					
do obchodů					
do restaurací a hostinců					
do bytů					
do chat					
do rodinných domků					

Pozn.: *Tuto tabulku na vyžádání zpracuje a dodá manažerům prevence kriminality krajů odbor prevence kriminality MV.*

(zde je možné doplnit grafickou podobu Tabulky č. 7 – koláč, sloupečky)

Tabulka č. 8: TČ výtržnictví a sprejerství – ze skupiny „ostatní TČ" v kraji YZ – porovnání s ČR za rok 201z (základ, tj. 100% = „ostatní TČ")[13]

	ČR – počet	ČR - %	kraj – počet	kraj - %	odchylka (%) kraj – ČR
ostatní TČ celkem		100		100	
z toho:					
výtržnictví					
sprejerství					

Pozn.: *Tuto tabulku na vyžádání zpracuje a dodá manažerům prevence kriminality krajů odbor prevence kriminality MV.*

Struktura pachatelů

Tabulka č. 9: stíháno, vyšetřováno osob v roce 201z – **ČR**

trestná činnost	celkem osob	nezletilí (do14 let)	tj. %	mladiství (15 – 17)	tj %	recidivisté	tj.%
násilná							
mravnostní							
krádeže vloupáním							

[12] Zahrnuje jen statisticky nejvýznamnější trestné činy ze skupiny krádeží vloupáním, v ČR evidovaných v řádu minimálně 1 tisíc.

[13] Ze skupiny „ostatní TČ" je, z úhlu pohledu prevence kriminality, doporučeno sledování trestných činů výtržnictví a sprejerství.

krádeže prosté								
ostatní								
zbývající								
hospodářská								
celková TČ								

***Pozn**.: Tuto tabulku na vyžádání zpracuje a dodá manažerům prevence kriminality krajů odbor prevence kriminality MV.*

Tabulka č. 10: stíháno, vyšetřováno osob v roce 201z – kraj YZ

trestná činnost	celkem osob	nezletilí (do 14 let)	tj. %	rozdíl % k ČR	mladiství (15 – 17)	tj %	rozdíl % k ČR	recidivisté	tj.%	rozdíl % k ČR
násilná										
mravnostní										
krádeže vloupáním										
krádeže prosté										
ostatní										
zbývající										
hospodářská										
celková TČ										

***Pozn.:** Tuto tabulku na vyžádání zpracuje a dodá manažerům prevence kriminality krajů odbor prevence kriminality MV.*

Jako další výstupy na úrovni kraje se s využitím ESSK doporučuje zpracovat přehled kriminality na osobách dle věku a s využitím „Zprávy o situaci v oblasti veřejného pořádku a vnitřní bezpečnosti na území České republiky“[14] zpracovat mezikrajové srovnání struktury pachatelů a srovnání v oblasti extremismu (viz Zpráva o projevech extremismu na území ČR - http://www.mvcr.cz/clanek/bezpecnostni-hrozby-337414.aspx?q=Y2hudW09NA%3d%3d)

<u>Úroveň okresů (územní odbory P ČR)</u>

Všechna data dodá krajům příslušné krajské ředitelství policie ČR.

[14]/ http://www.mvcr.cz/dokument/index.html

Tabulka č. 11: Zatíženost územních odborů P ČR dle vybraných kriterií v územní působnosti kraje (VÚSC) za rok 201z. Pořadí je dle indexů.

		celková trestná činnost			násilná+mravnostní		
okres	počet obyvatel	absolutní počet	index	pořadí	absolutní počet	index	pořadí

		krádeže vloupáním			krádeže prosté		
okres	počet obyvatel	absolutní počet	index	pořadí	absolutní počet	index	pořadí

Pořadí územních odborů v zatíženosti dle indexu nápadu TČ v kraji YZ za rok 201z:

<u>celková kriminalita násilná + mravnostní krádeže vloupáním krádeže prosté</u>

1.
2.
3.
4.
5.

Tabulka č. 12: Stíháno, vyšetřováno osob (celkem, recidivisté, děti + mladiství) za rok 201z

		Celkem			recidivisté			děti + mladiství		
okres	počet obyv.	abs.	Index	pořadí	abs.	Index	pořadí	abs.	Index	pořadí

<u>Úroveň obvodních (místních) oddělení P ČR</u>

Zjištění počtu obyvatel v působnosti jednotlivých obvodních (místních) oddělení P ČR

Okres: (pro každý okres bude zvláštní tabulka)

Obvodní (míst-	obce v působnosti	součet počtu	komentář, poznámky, informace

ní) oddělení / typ (I-IV)	(název / počet obyvatel)	obyvatel v obcích	(stručný popis charakteru území a základní údaje o demografické struktuře obyvatelstva)[15].

Sestavení pořadí zatíženosti obvodních (místních) oddělení P ČR dle vybraných ukazatelů v okrese Okres: (pro každý okres bude zvláštní tabulka)

		celková TČ			násilná + mravnostní		
obvodní (místní) oddělení	počet obyvatel	absolutní počet	index	pořadí	absolutní počet	index	pořadí

		krádeže prosté			krádeže vloupáním		
obvodní (místní) oddělení	počet obyvatel	absolutní počet	index	pořadí	absolutní počet	index	pořadí

Pořadí obvodních (místních) oddělení v zatíženosti dle indexu nápadu TČ v okrese:

celková kriminalita násilná + mravnostní krádeže vloupáním krádeže prosté

1.
2.
3.
4.
5.

Sestupně sestavené pořadí zatíženosti všech obvodních (místních) oddělení dle indexu nápadu celkové TČ za rok 201y v kraji (VÚSC)

1.

---

[15]/ Např. sezónnost, rekreační oblasti, koncentrace pracovních sil ze zahraničí apod.

2.
3.
4.
5.
6.……

Komentář ke statistickým údajům

Na tomto místě doporučujeme zpracovat stručný komentář a interpretaci statistických výstupů, které budou obsahovat označení nejvíce problémových lokalit a hlavních bezpečnostních problémů vyplývajících ze zkušeností P ČR.

Komentář zpracuje územní odbor P ČR na základě zpráv:
1/ vedoucích OO (MO) umístěných v první třetině sestavených pořadí OO (MO) v rámci okresu, a to v kterémkoliv ze sledovaných ukazatelů.
2/ vedoucích odborů obecné kriminality (OOK) SKPV příslušného OŘ P ČR zejména k činnosti oddělení 1 (násilí), 2 (vloupání byty a objekty), 3 (krádeže prosté), 7 (kapsy), 8 (motorová vozidla).

Sociálně demografická analýza kraje[16]

Analýza, která je zaměřena především na kriminálně rizikové skupiny, musí obsahovat nejméně následující základní údaje:

Obyvatelstvo – základní údaje
Počet obyvatel, hustota a charakter osídlení, podíl mužů a žen, průměrný věk, podíl obyvatel v produktivním věku, počet dětí a mladistvých a jejich podíl na celkové skladbě obyvatel, mladí dospělí, počet osob nad 60 let, migrační trendy, národnostní složení, ekonomika-porovnání podílu tvorby HDP na obyvatele s ostatními kraji.

Struktura vzdělanostní úrovně obyvatelstva:

procentní podíly u ekonomicky aktivní populace:

	celkem	muži	ženy	ČR celkem	ČR muži	ČR ženy
základní vzdělání						
vyučení						
středoškolské						
vysokoškolské						

Data o dalších rizikových faktorech

Počet **nezaměstnaných** (zdroj dat je Úřad práce ČR) za rok 201y přepočtený na 10 000 obyvatel.
Nezaměstnanost - mezikrajové srovnání[17] :

[16]/ Při zpracování sociálně demografické i institucionální analýzy je možné navrženou strukturu obměnit a rozsah materiálu rozšířit, předkládaný materiál má doporučující a přehledový charakter.

Další ukazatele nezaměstnanosti[18]:

	kraj	ČR
Podíl nezaměstnaných mladších 30 let (%)		
Průměrný věk nezaměstnaných		
Podíl nezaměstnaných déle než rok		
Podíl nezaměstnaných se zákl. vzdělá-ním		
Podíl nezam. vyučenců bez maturity		

Počet **vyplacených sociálních dávek závislých na výši příjmu** za rok 201y přepočtený na 1 000 obyvatel (zdroj – tabulka MPSV[19])

Územní srovnání – vybrané ukazatele podle okresů a v obcích s rozšířenou působností
Výčet obcí a počty obyvatel, počet obcí se statutem města, hustota osídlení, věková a vzdělanostní struktura obyvatelstva (průměrný věk, rozvodovost), migrace, nezaměstnanost[20], sociální dávky závislé na výši příjmu apod.

Výskyt sociálně vyloučených lokalit
V důsledku různých sociálních a ekonomických činitelů dochází ve většině měst ke vzniku menšinových komunit (sociálně a kulturně znevýhodněných skupin obyvatelstva), ve kterých je výskyt sociálně negativních jevů mnohem vyšší než v majoritní společnosti. Pokud dojde ke kumulaci těchto komunit, zvyšuje se výrazně riziko zintenzivnění problémů, jejichž jsou nositeli nebo dalších, nově vznikajících specifických problémů (např. xenofobní prostředí apod.).
Sociálně vyloučené lokality jsou uvedeny v Mapě sociálně vyloučených nebo sociálním vyloučením ohrožených romských lokalit v ČR na adrese http://www.esfcr.cz/mapa/index-2.html.

Stanovení map „rizikových lokalit“
Rizikové jsou lokality (území, obcí, správní obvody obcí s rozšířenou působností), ve kterých je:

- nejvyšší hodnota indexu kriminality
- nejvyšší hodnota indexu nezaměstnanosti
- nejvyšší hodnota indexu vyplacených sociálních dávek závislých na výši příjmu
- výskyt sociálně vyloučených lokalit

Kraj sestaví pořadí obcí a správních obvodů obcí s rozšířenou působností podle výše uvedených kritérií. Za rizikové jsou považovány ty lokality, které dosahují hodnot

---

[17]/ Zdroj statistiky ČSÚ – mezikrajová srovnání, údaje za daný rok.
[18]/ Doporučuje se rozdělit ukazatele podle pohlaví.
[19] Údaje jsou vedeny za úřady obcí s rozšířenou působností, na vyžádání budou poskytnuty z MPSV prostřednictvím odboru bezpečnostní politiky a prevence kriminality MV.
[20]/ Případně i další ukazatele a informace vypovídající o sociální situaci a demografické struktuře v územní působnosti kraje; statistické výstupy interpretovat komentářem.

nad republikovým průměrem (u kvantifikovaných kritérií – kriminalita, nezaměstnanost, vyplacené sociální dávky) a ty, ve kterých je sociálně vyloučená lokalita.
Počet rizikových lokalit v kraji se odvíjí od splnění uvedených podmínek.

Institucionální analýza

Cílem institucionální analýzy je získat přehled a provést vyhodnocení dosavadních aktivit orgánů státní správy, samosprávy, nestátních neziskových organizací a dalších institucí působících v oblasti prevence kriminality[21] na území kraje, s důrazem na prevenci na sekundární a terciární[22] úrovni. Důležité je zhodnocení dostupnosti služeb, které reagují na specifické psychosociální, zdravotní a kulturně-sociální handicapy určitých skupin obyvatel kraje a vytipování aktivit a služeb chybějících. K tomu je třeba provést audit institucí působících ve jmenovaných oblastech jak na území celého kraje nebo jeho velké části, tak v jednotlivých městech i obcích. Při zpracování institucionální analýzy lze využít všechny dostupné strategické, koncepční a přehledové materiály, které jsou, byť i jen částečně obsahově průnikové s oblastí prevence kriminality (může se jednat např. o plány rozvoje, komunitní plány, přehledy zařízení a služeb různých resortů apod.).
Standardně by analýza měla obsahovat informace o existenci a působnosti následujících konkrétních institucí (subjektů, zařízení, služeb) **na úrovni kraje a na úrovni správních obvodů obcí s rozšířenou působností:** referáty sociálních věcí a jejich součásti: SPOD[23], kurátoři pro mládež, sociální kurátoři, sociální asistenti, protidrogový koordinátor a romský poradce,

- výchovné ústavy, ústavy sociální péče, věznice, pedagogicko-psychologické poradny, střediska výchovné péče, azylové domy, domy na půl cesty, poradny AT, protidrogová zařízení, noclehárny pro osoby bez přístřeší, nízkoprahová a komunitní centra, linky důvěry, občanské poradny, stacionáře a případně další subjekty a zařízení,
- střediska včasné intervence,
- střediska PMS[24],
- subjekty poskytující pomoc obětem trestné činnosti,
- přehled aktivit obecně prospěšných společností, nestátních neziskových a charitativních organizací, které působí v oblasti sociální prevence, zejména pokud je jejich činnost zaměřena na problémové a rizikové cílové skupiny,

---

[21]/ Jedná se v podstatě o audit subjektů, činností a služeb v této oblasti, při jehož zpracování je možné s výhodou využít podkladů pro komunitní plány krajů a měst.
[22]/ **Sekundární prevence** je zaměřena na rizikové skupiny osob, u nichž je zvýšená pravděpodobnost, že se stanou pachateli nebo oběťmi trestné činnosti (specializovaná sociální péče), na sociálně patologické jevy (např. vandalismus, šikana, záškoláctví, povalečství, rasové konflikty apod.) a na příčiny kriminogenních situací (dlouhodobá nezaměstnanost, sociální chudoba apod.). **Terciární prevence** se pak soustřeďuje na kriminálně narušené jedince a na prokriminální sociální prostředí.

[23] Sociálně-právní ochrana dětí.
[24]/ Zvlášť uvést střediska PMS se specializovaným oddělením pro mládež.

- nejvýznamnější organizace v kraji, které poskytují možnosti zájmové nebo sportovní činnosti nejvíce dětem a mládeži v kraji,
- městské policie a jejich preventivní aktivity,
- PIS P ČR,
- komise + pracovní skupiny prevence kriminality ve městech a obcích kraje,
- soukromé bezpečnostní agentury a firmy specializované na zabezpečovací techniku.

Informace o sociologických výzkumech, šetřeních, anketách apod., týkajících se oblasti prevence kriminality, které byly provedeny na území kraje

Obsahově zahrnující tematické okruhy např. pocit bezpečí občanů, spokojenost s prací státní či městské policie, informovanost veřejnosti o projektech prevence kriminality, postoje k zavádění nebo rozšiřování městského kamerového dohlížecího systému (dále jen „MKDS“) – vysvětlit zkratku, informace o expertních šetřeních atd.

Přehled preventivních projektů a výše finančních prostředků vynaložených na jejich realizaci v městech a obcích na území kraje

Jako zdroj údajů je možné využít databázi realizovaných projektů v rámci Programu prevence kriminality na místní úrovni z let 1996 až 2015.

B. Metodika přípravy strategického dokumentu prevence kriminality obce, kraje

1. Příprava plánu prevence kriminality obce

V souladu s vládou schválenou[25] Strategií prevence kriminality v České republice na léta 2016 až 2020 (dále jen „Strategie“) **je systém prevence kriminality založen na třech úrovních – republikové, krajské a lokální (obecní).** Jednotlivé úrovně se liší svým teritoriálním vymezením, typem realizátorů, mírou kompetencí klíčových partnerů, postupy při zpracování analýz, zpracováním rozdílných koncepčních materiálů a způsoby vyhodnocování své činnosti. Liší se také nároky na personální obsazení a na míru zapojení a odpovědnosti zúčastněných subjektů.

Lokální úroveň tvoří síť všech obcí v ČR, které za splnění dále stanovených podmínek mají možnost v období let 2016 až 2020 předkládat prostřednictvím místně příslušného krajského úřadu **Žádosti o dotace** v oblasti prevence kriminality na realizaci **projektů prevence kriminality obce (dále jen „Žádost“).**

[25] Usnesení č. xxx ze dne xx. ledna 2016.

Tato metodika je závazná pro všechny obce, které se budou v rámci Programu uchá-zet o státní účelovou dotaci na projekty prevence kriminality.

Strategický dokument prevence kriminality obce

Kriminálně rizikové, kriminální a protiprávní jevy jsou, podle dlouhodobých studií a zkušeností, zpravidla kumulovány do větších měst a městských aglomerací. Stále více se ale objevují v malých městech či obcích o několika stech obyvatelích. Týká se to zejmé-na specifických jevů nebo kumulace jevů (např. protiprávní jednání nepřizpůsobivých osob, které je důsledkem jejich sestěhování do jednoho objektu, do prostoru malé obce, apod.). Stále obtížněji lze určit, v jak velké obci či městě se uvedené jevy objeví. O to těžší je řešení situace, pokud se takový jev či jejich kumulace objeví v malém městě či obci, které zpravidla nedisponují lidskými ani finančními zdroji, často ani potřebným know-how. Protože je více než nutné zasahovat proti kriminálně-rizikovým, kriminálním a proti-právním jevům pokud možno včas, efektivně a preventivně, jeví de jako nezbytné v rozumné míře podporovat vybrané druhy aktivit také pomocí dotační podpory. Ze shora uvedených důvodů není současně možné omezit okruh obcí (oprávněných žadatelů) po-čtem obyvatel. Strategie prevence kriminality v České republice na léta 2016 až 2020 (dále jen Strategie“) vytyčuje, v souladu s výše uvedeným a dosavadními zkušenostmi v oblasti dotační podpory projektů měst a obcí v prevenci kriminality, nová pravidla na další období dotační podpory. O dotační podporu se může ucházeti každá obec v ČR, a to bez ohledu na počet obyvatel.

Obec, která identifikuje na svém území problém nebo riziko z oblasti veřejného pořádku (jak na úrovni přestupků, tak kriminality), postupuje při jejich řešení/odstranění standard-ně, za použití nástrojů, které jí dává právní řád ČR, s využitím aparátu vlastního úřadu, obecní policie (pokud je zřízena), v úzké spolupráci s místně příslušnými útvary Poli-cie ČR (obvodní/místní oddělení, územní odbor), orgány justice, dalšími subjekty veřejné správy (např. hasičský záchranný sbor, hygienická stanice, finanční úřad), neziskovým sektorem a občany obce.

Pokud se obec rozhodne pro řešení/odstranění výše uvedených problémů a/nebo rizik také pomocí projektů prevence kriminality, musí tento krok tvořit součást, či nadstavbu ne-bo doplnění standardních kroků a postupů výše uvedených. Současně musí problém či riziko, které bude v Žádosti řešeno, odpovídat prioritám a cílům obsaženým ve Strategii. Plán prevence kriminality obce, který je základním předpokladem předložení žádosti o státní účelovou dotaci, musí tedy popisovat komplexní řešení vytipovaného problému, a nemůže být pouze jednorázovým izolovaným opatřením.

Projektové řešení bezpečnostních problémů je spíše nadstavbou činností v této oblas-ti. Základní ambicí je, aby příslušné subjekty a instituce vykonávaly své kompetence důsledně, ve vzájemné spolupráci a v rámci svých rozpočtů.

Doporučený postup k přípravě strategického dokumentu prevence kriminality obce

Při přípravě obec respektuje všechny následující doporučené postupy.

Strategický dokument prevence kriminality obce je obecněji pojatý dokument popisující problémy identifikované v rámci bezpečnostního auditu (analýzy) obce (viz předchozí ka-

pitola) a navrhující jejich řešení, včetně všech potřebných zdrojů (organizační, personální, finanční), a to minimálně na dobu 2 po sobě jdoucích let. K popisu může obec také pro doplnění využít již hotové dokumenty jako je např. komunitní plán rozvoje, integrovaný plán rozvoje města, koordinační dohody mezi samosprávou a Policií ČR dle § 16 zákona o Policii ČR, výstupy lokálního partnerství při spolupráci s Agenturou pro sociální začleňování apod.

Doporučuje se, aby strategický dokument využíval a kombinoval aktivity z oblasti situační i sociální prevence a informování občanů o možnostech ochrany před trestnou činností. Dílčí opatření/ projekty jsou zaměřeny na řešení identifikovaných problémů. Může se jednat např. o komplexní řešení problému určené rizikové lokality obce, řešení konkrétních problémů nebo rizik v oblasti výskytu kriminálního chování apod. Důležitou podmínkou pro uskutečňování uvedeného strategického dokumentu a pro jeho trvání a udržitelnost jsou finanční prostředky, které je vhodné sdružovat. Vedle obecních i krajských finančních zdrojů a finančních prostředků na rozvoj prevence kriminality z kapitoly Ministerstva vnitra je možné získávat další prostředky z grantů státních i nestátních a z fondů EU. Do plánu je vhodné zapojit vedle orgánů samosprávy, státní správy, policie a nestátních neziskových organizací, zástupce podnikatelského sektoru, mimo jiné i jako potenciální sponzory některých aktivit, i občany samotné.

Organizační a personální zabezpečení strategického dokumentu

Podmínkou pro úspěšné sestavení strategického dokumentu je zejména:

- **existence pracovní skupiny prevence kriminality**, ve které jsou zastoupeni pracovníci, kteří se problematikou bezpečnosti, veřejného pořádku a sociálně patologickými jevy profesionálně zabývají[26],

- **pověření** pracovníka zodpovědného za prevenci kriminality ve městě – **manažera prevence kriminality**[27].

Manažer a pracovní skupina odpovídají za přípravu, realizaci a hodnocení realizaci plánu. Hlavním partnerem pro orgány samosprávy je Policie ČR, která odpovídá za zpracování podrobných analýz trestné činnosti, formulaci a iniciaci návrhů řešení identifikovaných problémů a zpracovávání stanovisek k předkládaným projektům z oblasti situační prevence. Zástupci Policie ČR jsou členy pracovní skupiny (komise).

---

[26] Doporučuje se následující složení pracovní skupiny: zástupce vedení města odpovědný za bezpečnost a prevenci, manažer prevence kriminality města, zástupci sociálního, školského, bezpečnostního odboru (oddělení), romský poradce, zástupce městské policie, zástupce Probační a mediační služby ČR, zástupci Policie ČR (PIS Policie ČR a další dle potřeby) a další podle místních podmínek (např. NNO a církevní organizace). Při řešení zásadních problémů, přípravě programu a při zpracování koncepce se doporučuje zapojit do práce skupiny manažera prevence kriminality kraje a koordinátora prevence kriminality krajské správy Policie ČR.

[27] Manažer je zároveň kontaktní osobou pro odbor bezpečnostní politiky a prevence kriminality MV, Policii ČR a pro manažera prevence kriminality příslušného KÚ.

Schválení strategického dokumentu
Konečnou verzi schvaluje rada nebo zastupitelstvo obce. Tím se mu dostane závaznosti a může být financován z rozpočtu obce, vyhodnocován a kontrolován**.**

2. Tvorba strategického dokumentu prevence kriminality kraje

Zpracování strategického dokumentu prevence kriminality krajů na léta 2012 až 2016 (dále jen „Koncepce“) je jednou z podmínek realizace programů prevence kriminality krajů obsažených ve Strategii prevence kriminality v České republice.
Jestli budou kraje na rok 2016 požadovat státní účelovou dotaci z Programu prevence kriminality MV, musí mít zpracovanou Koncepci.
Koncepce popíše krajská a regionální specifika v oblasti prevence kriminality, a to s využitím „tvrdých dat“ o kriminalitě, nezaměstnanosti a počtu vyplacených sociálních dávek) a „měkkých dat“ (socio-demo analýza a podobně). Podkladem pro zpracování Koncepce jsou také údaje o sociálně vyloučených lokalitách (dále jen „vyloučené lokality) Cílem Koncepce je:

- Popsat území kraje z hlediska výskytu kriminality
- Popsat území kraje z hlediska výskytu vyloučených lokalit
- Popsat území kraje z hlediska dalších rizikových faktorů (počet nezaměstnaných a počet vyplacených sociálních dávek závislých na výši příjmů), které mohou mít vliv na výskyt delikventní činnosti
- Stanovit „rizikové lokality“ na základě všech výše uvedených faktorů
- Poskytnout podklady obcím k plánování vlastních preventivních aktivit
- Vymezit „krajskou roli“ v oblasti prevence kriminality
- Definovat politiku kraje v oblasti prevence kriminality na uvedené období
- Stanovit oblasti priorit a poskytnout tím vodítko subjektům v území kraje pro jejich činnost

Následující text je doporučením odboru prevence kriminality Ministerstva vnitra k procesu zpracovávání vlastních Koncepcí. Každý zpracovatel si může podle svého uvážení, místních podmínek, identifikovaných problémů, potřeb a požadavků tento doporučený minimální standard dále rozšířit o místně vnímaná rizika kriminality.

Východiska
Koncepce je navržena na základě:

- analýzy kriminality (skutky, pachatelé, oběti);
- sociodemografických údajů;
- institucionální analýzy;
- analýzy názorů a postojů občanů (např. výzkumy pocitu bezpečí, viktimologické výzkumy);
- analýzy možných zdrojů financování preventivních aktivit (ROP, dotační tituly ústředních orgánů státní správy, vlastní krajské dotační možnosti, dotační politika samospráv);

- doporučení expertů (např. komise prevence kriminality kraje, pracovní skupiny, pracovní skupiny měst, poznatky obecní policie a P ČR, PMS);
- zkušeností kraje s realizací preventivních aktivit (např. v rámci Programu prevence kriminality na místní úrovni – Partnerství, zkušeností měst z realizace preventivních programů);
- doporučení a analýz poskytnutých v rámci tzv. Lokálního partnerství s Agenturou pro sociální začleňování v romských lokalitách
- zahraničních zkušeností (např. z dokumentů OSN nebo EUCPN).

Stanovení priorit[28]

Priority lze stanovit dle:

- Priorit a Specifických cílů Strategie prevence kriminality v České republice na léta 2016 až 2020
- cílových skupin, na které je zaměřena (pachatelé protiprávního jednání, oběti, rizikoví jedinci v postavení potenciálních pachatelů nebo obětí),
- trestných činů a jiných typů delikventních chování,
- hlediska působnosti (je možné, že budou definovány okruhy problémů přesahujících kompetence kraje, které mohou být postoupeny např. Ministerstvu vnitra a Republikovému výboru pro prevenci kriminality k hledání systémového republikového řešení),
- územního rozložení trestné činnosti,
- kompetencí (kraje a obcí a dalších subjektů zabývajících se bezpečnostní situací),
- legislativy (zákonné nebo podzákonné vymezení preventivních opatření kriminality, legislativní akty kraje a obcí upravujících místní podmínky bezpečnosti a veřejného pořádku),
- systémových a organizačních priorit (např. zajištění rozdělní státní účelové dotace na projekty prevence kriminality, fungování Komise prevence kriminality kraje, iniciování pracovních skupin kraje a obcí).

Stanovení hlavních a dílčích problémů a návrhy na jejich řešení

Z hlediska časového je třeba stanovit, že se jedná o řešení:

- **Dlouhodobá**

Reagují na definované obecné problémy a hlavní priority. Budou řešeny v horizontu trvání celé Koncepce, tj. do roku 2020 nebo s přesahem do dalšího období.

- **Krátkodobá** (akční plán, seznam úkolů)

---

[28]/ Jednou z metod stanovení priorit, hlavních a dílčích problémů k řešení může být SWOT analýza, pomocí které lze identifikovat:

- silné stránky (vnitřní potenciál a nástroje, které lze využít),
- slabé stránky (vnitřní slabá místa, na jejichž odstranění se lze zaměřit),
- příležitosti (vnější faktory, které můžeme využít pro dosažení cílů),
- hrozby (vnější faktory, které znesnadňují dosažení cílů a je žádoucí je překonat).

Reagují na definované dílčí problémy. Budou obsahem každoročního hodnocení, které město bude předkládat Radě nebo Zastupitelstvu a zasílat pro informaci na Ministerstvo vnitra.

Návrhy řešení zahrnují:

- nástroje a podmínky pro dosažení cílů,
- gesce za jejich plnění,
- termíny plnění,
- forma očekávaných výstupů,
- použité metody a postupy,
- popis konkrétních aktivit,
- zajištění financování.

Způsob vyhodnocování

Součástí Koncepce budou indikátory úspěšnosti (kritéria efektivity), které určí způsob rozpoznání dosažení cílů a priorit (zcela, částečně nebo vůbec). V průběhu naplňování priorit a cílů Koncepce je vhodné si stanovit postupné cíle a hodnotit jejich dosažení k určitému datu.

Doporučuje se také nastavit systém a termíny předkládání každoročních hodnotících zpráv o plnění Koncepce orgánům kraje (samosprávné orgány, odborné komise, odbory krajského úřadu).

V kontextu s národní Strategií prevence kriminality v České republice na léta 2016 až 2020 by každá Koncepce měla obsahovat nástroje k měření efektivity dopadů aktivit a vynaložených prostředků.

Cílem vyhodnocování Koncepce je sestavení závěrečné zprávy, ve které kraj konstatuje, zda naplnil stanovené cíle, co a jak se změnilo, co se podařilo/nepodařilo a proč. Taková závěrečná zpráva opřená o fakta a čísla bude východiskem pro zpracování dalšího strategického materiálu kraje v oblasti prevence kriminality.

Aktéři a jejich role

Na základě institucionální analýzy nebo SWOT analýzy budou definováni klíčoví partneři a další aktéři v oblasti prevence kriminality a sociálně patologických jevů a zvyšování bezpečí občanů. Popis může obsahovat:

- postavení manažera prevence kriminality v rámci krajského úřadu a jeho kompetence,
- kompetence dalších partnerů a subjektů (zákonné, výkonné),
- jejich silné a slabé stránky (co lze využít již nyní, v čem potřebují podporu),
- formu zapojení do naplňování Koncepce,
- způsob koordinace jejich aktivit, prezentace výsledků, zapojení na úrovni krajské.

Dlouhodobé řešení oblasti prevence kriminality na úrovni kraje

Je také potřebné formulovat postup dalšího směřování kraje v oblasti prevence kriminality a bezpečí občanů po ukončení platnosti Koncepce prevence kriminality kraje na léta 2012

až 2015, současně s tím, že vláda přijala novou Strategii prevence kriminality České republiky na léta 2016 až 2020. Znamená to odpovědět na otázky, zda kraj bude nadále:

- pokračovat v práci odborné víceoborové komise nebo pracovní skupiny prevence kriminality,
- zpracovávat další koncepční materiály,
- podporovat činnost manažera prevence kriminality;
- koordinovat preventivní aktivity,
- vyčleňovat finanční prostředky na preventivní aktivity.

C. Způsoby a kritéria stanovování míry rizikovosti území ve vztahu k prevenci kriminality.

Ve vztahu k prevenci kriminality stanovila Strategie prevence kriminality v České republice na léta 2016 až 2020 základní způsoby a kritéria stanovování míry rizikovosti území ČR. Pro oblast prevence kriminality je použito několik málo indikátorů

Jsou sledovány 3 základní úrovně území (lokalit):

- kraje (vyšší územně samosprávné celky)
- okresy (územní jednotky)

V rámci těchto území jsou sledovány následující indikátory rizikovosti:

a) **trestná činnost** (přečiny i zločiny) v daném území k 31. 12. předchozího kalendářního roku

b) **počty nezaměstnaných** k 31. 12. předchozího kalendářního roku

c) **počty vyplacených sociálních dávek závislých na výši příjmu**[29] k 31. 12. předchozího kalendářního roku („dávky, které lze charakterizovat jako dávky související s chudobou“).

Odbor bezpečnostní politiky a prevence kriminality MV zpracuje každoročně tabulku rizikovosti všech 3 úrovní území[30] v rámci České republiky. Úroveň okresů se kryje s územními odbory Policie ČR (případně jejich městskými ředitelstvími) a je jich celkem 77[31].

[29] Počty vyplacených testovaných dávek státní sociální podpory a hmotné nouze (jedná se o počty řádně vyplacených dávek - tj. bez doplatků, přeplatků a vratek - v roce 201x) podle území (trvalá adresy osoby). Počty příjemců nejsou sledovány, pouze jsou odvozeny z počtu přiznaných dávek za daný měsíc bez ohledu na okamžik následné výplaty.

[30] Jedná se o bývalé okresy včetně hl. m. Prahy. Pro zjednodušení se bude v textu dále používat název „okres“.

[31] Jedinou výjimkou je územní odbor Policie ČR Praha venkov - jih, který v tabulce č. 1 uveden není. Tabulka obsahuje územní odbory Praha venkov - západ a Praha venkov - východ. Kriminalita v ÚO PČR Praha venkov -jih byla mezi ně rozdělena podle příslušnosti obcí s rozšířenou působností.

Výsledky jsou přepočteny (indexovány) na 10 tisíc obyvatel (respektive 1 000 obyvatel u sociálních dávek) a rizikovost území je řazena od nejzatíženější[32] po nejméně rizikovou. Jednotlivé kraje, včetně okresů spadajících do jejich území, jsou v tabulce barevně odlišeny. Krajské úřady obdrží od odboru prevence kriminality MV každoročně tyto tabulky v dostatečném předstihu.

Území, která budou mít **vyšší index rizikovosti než je průměr České republiky v daném roce**, budou prohlášena za **riziková.** Ostatní území nejsou považována za riziková.

Cílem zvoleného postupu je zaměřit pozornost Ministerstva vnitra, dalších členů Republikového výboru a především krajů **na nejrizikovější místa v rámci ČR**, zlepšovat bezpečnostní situaci a nastavovat preventivní opatření v místech, kde je potřebnost statisticky prokázána.

D. Rekapitulace

Předkládaná metodika předkládá doporučení k přípravě bezpečnostních analýz obce a kraje, k přípravě koncepčních materiálů obcí či krajů v oblasti prevence kriminality a současně stanovuje základní indikátory, jejichž pomocí bude pro účely prevence kriminality stanovována rizikovost území ČR.

Pro doplnění doporučujeme nastudování materiálu vydaného Institutem pro kriminologii a sociální prevenci – „**Příručka pro bezpečnostní audit na místní úrovni. Kompendium mezinárodní praxe**“ (http://www.ok.cz/iksp/publikace.html, publikace roku 2008, část prameny).

[32] Tam, kde je zatíženost vysoká, je vhodné v preventivních programech kombinovat sociální, situační a behaviorální opatření. V hl. m. Praze, která je sice v souhrnu až na 73 místě ze 77 územních celků, ale v počtu registrovaných trestných na místě prvním, se doporučují opatření situačního charakteru – koncipovaných ve spolupráci Policie ČR, Magistrátu hl. m. Prahy, obvodních úřadů a městské policie. I v tomto případě je nutné zpracovat (PČR a MěP) detailní analýzu výskytu kriminality na území města, a to v souvislosti s výskytem bazarů a zastaváren, nepřehledných a snadno únikových míst, tzn. podmínek, které páchání trestné činnosti a zisku z ní, usnadňují.