**Národná koncepcia informatizácia verejnej správy**

**Strategická priorita 10 Kybernetická bezpečnosť**

# Úvod

[čo je informačná/kybernetická bezpečnosť a prečo ju potrebujeme, o čom bude tento dokument]

* existencia súčasnej spoločnosti v podstatnej miere závisí od spoľahlivého fungovania informačných a komunikačných technológií (IKT)[[1]](#footnote-1), ktoré sa používajú na spracovanie informácií vo všetkých oblastiach života spoločnosti; úplnosti, pravdivosti, aktuálnosti a dostupnosti informácií, ktoré sú pomocou IKT spracovávané a dostupnosti a dôveryhodnosti služieb, ktoré sú prostredníctvom nich poskytované,
* zaistenie dostatočnej úrovne kybernetickej (infraštruktúra) a informačnej bezpečnosti (obsah) je nutnou podmienkou informatizácie verejnej správy; t.j. aj nutnou podmienkou na dosiahnutie cieľov, ktoré si kladie NKIVS
* IKT sú rozsiahle, rozdielne a navzájom prepojené (závislé), údaje, ktoré sa prostredníctvo IKT spracovávajú sú rôznorodé tak z hľadiska obsahu, požiadaviek na ochranu, ako aj formátov; zodpovednosť za ich spracovanie a ochranu majú rôzne inštitúcie a požiadavky na spôsob spracovania a ochranu stanovuje viacero rôznych zákonov, a to nielen na slovenskej , ale aj európskej úrovni;
* vzhľadom na charakter IKT (rozšírenosť a vzájomná prepojenosť) si zaistenie kybernetickej a informačnej bezpečnosti vyžaduje spoluprácu všetkých zainteresovaných; štátnych inštitúcií, súkromných organizácií, občanov a keďže slovenský virtuálny priestor je súčasťou globálneho virtuálneho priestoru, aj spoluprácu na medzinárodnej úrovni

# Ciele dokumentu

[plus nejake „dislaimers“, ktorými sa rámcujeme / obmedzujeme; vymedzenie časti, ktorou sa budeme zaoberať, jej vzťahy s ostatnými časťami a predpoklady o bezpečnostnom okolí ISVS; možno vymedzenie sa voči ostatným prioritným oblastiam NKIVS]

* ISVS tvoria časť slovenského virtuálneho priestoru a preto bezpečnostné problémy existujúcich a budúcich ISVS nie je možné riešiť izolovane, abstrahujúc od ostatných systémov, patriacich do tohto priestoru;
* základným cieľom kybernetickej a informačnej bezpečnosti ISVS je zaistenie bezpečného a spoľahlivého fungovania ISVS tak, aby
  + orgány verejnej správy pracovali s aktuálnymi, úplnými a pravdivými informáciami a mohli prijímať kvalifikované rozhodnutia a poskytovať občanom kvalitné (elektronické) služby;
  + bola zabezpečená spoľahlivá obojstranná komunikácia občanov, podnikateľov, firiem, inštitúcií  s orgánmi VS, vrátane vzájomnej komunikácie orgánov VS,
  + bola zabezpečená primeraná ochrana spracovávaných údajov (dôvernosť, integrita, autentickosť, dostupnosť, súkromnosť, nepopretie autorstva, doručenia a i.) pri zachovaní primeranej ochrany súkromia občanov;
  + ochrana ISVS bola systematická, ekonomicky efektívna a dlhodobo udržateľná
  + spôsob ochrany ISVS bol v súlade s demokratickými princípmi.
* základnými cieľmi dokumentu sú
  + objasniť úlohu kybernetickej a informačnej bezpečnosti v informačnej spoločnosti,
  + definovať úlohy, ktoré štát potrebuje vyriešiť na to, aby zaistil primeranú úroveň bezpečnosti ISVS a ich bezpečnostného okolia;
  + vysvetliť jednotlivým kategóriám zainteresovaných, aké úlohy majú pri zaisťovaní primeranej úrovne ochrany slovenského virtuálneho priestoru vo všeobecnosti a ISVS zvlášť.
* zaistenie dostatočnej úrovne kybernetickej a informačnej bezpečnosti slovenského virtuálneho priestoru je náročná úloha, ktorú tento dokument nemôže riešiť v plnom rozsahu, ale rozoberie/analyzuje bezpečnostné požiadavky na subsystém/podpriestor ISVS a popíše požiadavky na bezpečnostné okolie/prostredie tohto podpriestoru. Menovite
  1. vymedzí rozsah problémov, ktoré bude potrebné riešiť na úrovni štátu;
  2. špecifikuje, čo je potrebné zaistiť v záujme zabezpečenia ISVS a úloh vyplývajúcich z NKIVS; t.j. stanoví ciele v oblasti kybernetickej a informačnej bezpečnosti pre verejnú správu;
  3. opíše aktuálny stav KB&IB v SR a navrhne postupnosť krokov potrebných na naplnenie stanovených cieľov
  4. navrhne dokumenty (a ich obsah), ktoré bude potrebné vypracovať;
  5. stručne rozoberie existujúcu relevantnú legislatívu, EU aj slovenskú, vrátane aktuálnych materiálov, o ktoré by sa bolo možné oprieť
  6. existujúce kompetencie a nepokryté oblasti,
  7. popíše spôsob správy tohto dokumentu
  8. Akčný plán?

# Adresáti dokumentu

* dokument je určený šiestim kategóriám čitateľov; spoločným cieľom pre každú kategóriu čitateľov je vysvetliť  podstatu a úlohu kybernetickej a informačnej bezpečnosti; pre jednotlivé kategórie potom špeciálne
  + vedúcim pracovníkom štátnych inštitúcií zabezpečujúcich, alebo sa podieľajúcich na zabezpečení ochrany slovenského virtuálneho priestoru prehľad úloh, ktoré v súvislosti so zabezpečením slovenského virtuálneho priestoru vo všeobecnosti a ISVS zvlášť je potrebné riešiť;
  + vedúcim pracovníkom štátnych inštitúcií, ktoré prevádzkujú ISVS má dokument vysvetliť význam zabezpečenia IB a KB systémov v pôsobnosti organizácie, ktorú riadia, povinnosti ktoré im vyplývajú z legislatívy a rámcovo čo pre to musia robiť.
  + pracovníkom štátnych inštitúcií, ktorí sú zodpovední za zaistenie ochrany ISVS: ako rozpracovať všeobecné úlohy vyplývajúce zo zákonov do systematického riešenia kybernetickej a informačnej bezpečnosti; kde nájsť na to potrebné podrobnejšie informácie a na ktoré štátne inštitúcie sa obrátiť v prípade problémov;
  + dodávateľom IKT, služieb pre štátne inštitúcie: požiadavky na ochranu ISVS a podmienky, ktoré musia dodávané IKT a služby spĺňať;
  + prevádzkovateľom systémov komunikujúcich s ISVS – podmienky, ktoré musia ich systémy spĺňať, aby ich bolo možné pripojiť k ISVS bez rizika kompromitácie ISVS;
  + používateľom ISVS a občanom pristupujúcim k ISVS základné zásady, ktoré musia dodržiavať pri využívaní elektronických služieb verejnej správy.

# Základné pojmy a označenia

[Formálne detaily (skratky, pojmy atď. - toho bude viac, dal by som to do príloh a na tomto mieste buď len základné pojmy a skratky a odkaz na prílohu)]

## Základné pojmy

Terminológia informačnej, resp. kybernetickej bezpečnosti sa ešte len vyvíja a neexistujú všeobecne akceptované definície ani mnohých základných pojmov (kybernetický priestor, kybernetická bezpečnosť). V tejto časti vysvetlíme základné pojmy nevyhnutné pre čítanie ďalšieho textu; stručný výkladový slovník základných pojmov je uvedený v prílohe XXX Terminológia

*[toto napíšeme nakoniec, keď budeme vedieť, aké pojmy sme v texte použili, zatiaľ skúsme robiť zoznam]*

* aktívum
* hrozba
* zraniteľnosť
* bezpečnostný incident
* útok
* informačná bezpečnosť
* kybernetický priestor
* kybernetická bezpečnosť
* opatrenie/protiopatrenie
* riziko

## Skratky

podobne ako s pojmami, keď bude hotový dokument, prejdeme cez neho a vyberieme všetky skratky. Ak ich bude veľa, dáme ich do prílohy, ak sa zmestíme na jednu stranu (do 40), môžeme ich dať do textu.

* ISVS informačné systémy verejnej správy
* IKT – informačné a komunikačné technológie
* GDPR
* NIS

# Súčasná situácia

[Obsah

* *aspoň stručne globálna situácia v IB/KB vo svete, posledné veľké bezpečnostné incidenty, aktivity EU, NATO*
* *tu by som rád videl komplexnejšiu analýzu, ale na tú nemáme čas; môžeme ísť na vysokoúrovňový popis, aby politici videli rozsah problematiky a aby sme v návrhu implementácie mohli požadovať napr. správy o stave IB/KB a mali zdôvodnenie pre navrhované riešenia). Zároveň úvod k ďalším častiam tejto kapitoly*
* *legislatíva, kompetencie, činnosť existujúcich štátnych orgánov,*
* *Videná zvonku (ITU index, atd) ako krajina, regulácia / EU požiadavky*
* *Videná zvonku v oblasti IS VS*
* *Videná interne / fakty csirt.sk pre IS VS*
* *PEST (uvidíme)]*
* charakteristika slovenského virtuálneho priestoru (odhad počtu systémov: štát, súkromný sektor, občania, pripojenie na Internet, špeciálne siete a systémy) – toto zároveň charakterizuje rozsah problému, ktorý potrebujeme riešiť
* legislatíva a kompetencie za IB/KB (do prílohy, v dokumente len stručná charakteristika)
  + utajované skutočnosti
  + telekomunikačný zákon
  + ISVS
  + výnos MF o štandardoch
  + kritická infraštruktúra
  + slobodný prístup k informáciám
  + e-Government
  + dôveryhodné služby
  + trestný zákon a trestný poriadok
  + iné zákony
* EÚ Nariadenia a Direktívy
  + eIDAS
  + Direktíva NIS
  + Nariadenie o ochrane (osobných) údajov GDPR
  + kritická infraštruktúra
  + počítačová kriminalita
  + iné
* štátne inštitúcie so zodpovednosťou súvisiacou s IB/KB – prehľad (prípadne spojiť s legislatívou a kompetenciami)
  + utajované skutočnosti a elektronický podpis – NBÚ
  + osobné údaje – Úrad na ochranu osobných údajov
  + Internet
  + telekomunikačné siete
  + špeciálne siete (Govnet)
  + kritická informačná infraštruktúra
  + národný kybernetický priestor – MO?
  + spravodajstvo a tajné služby?
* ľudské zdroje – koľko máme odborníkov (stačia odhady) (bezpečnostní manažéri, technickí správcovia, forenzní analytici, lektori, výskumníci, kryptológovia, penetrační testeri, právnici, prípadne ďalšie špecializácie)
  + v štátnej sfére
  + školy a akadémia
  + firmy
  + iní
* firmy a organizácie zamerané na IB/KB
  + organizácia, čo vie robiť dobre, koľko má na to ľudí (audit, vzdelávanie, bezpečnostné projekty, analýzy rizík, penetračné testovanie, forenzná analýza, právne aspekty – vyšetrovanie a stíhanie počítačovej kriminality, autorské práva, počítačové právo a i. )
* informácie o stave IB/KB na Slovensku
  + prieskumy stavu oficiálne
  + počítačový zločin – existujú štatistiky?
  + aktivity zamerané na zlepšenie (vzdelávanie, konferencie, vládne dokumenty, súkromné iniciatívy,...)
* ak nie je dosť informácií, pripravíme si prieskum - osnova – správy BSI, pozrieť aj správy USA
* špeciálne – bezpečnostné aspekty informatizácie – pozrieť sa na ostatné materiály a zistiť, aké sú bezpečnostné predpoklady ich naplnenia, resp. u existujúcich zákonov – aké bezpečnostné dôsledky z nich vyplývajú (zákon o e-Gov)
* zhodnotenie stavu IB/KB na Slovensku

Terminológia informačnej resp. kybernetickej bezpečnosti sa dynamicky vyvíja a mnohé, dokonca aj základné pojmy, nie sú v medzinárodnej terminológii jednoznačne definované. Slovenská terminológia sa vyvíja živelne a zväčša preberá anglické termíny, v najlepšom prípade ich prekladatelia poslovenčujú alebo prekladajú. Tento dokument vychádza z výkladového slovníka pojmov informačnej bezpečnosti MF SR.

# **Problémové oblasti**

(z toho predchádzajúceho)

# Priority

smerovanie podľa nkivs

# Ciele (návrh PS)

– riešenie problémov / priorít v strednodobom horizonte + stručná SWOT tohto riešenia (high level uroveň)

# Kritické faktory úspechu

(vrátane všetkých relevantných predpokladov

# Návrh implementácie –

1. *governance / regulácia (uprava vynosu) všeobecnejšie – legislatíva, kompetencie, miesto ISVS v slovenskom virtuálnom priestore, ochrana ISVS v kontexte ochrany celého slovenského virtuálneho priestoru*
2. *Návrh implementácie – procesy*
3. *Návrh implementácie – štandardy*
4. *Návrh implementácia – ľudia*
5. *Návrh implementácie – kultúra / vzdelávanie*
6. *Návrh implementácie – odporúčania pre SORO*

## národná/štátna úroveň

* čo treba upratať v legislatíve a kompetenciách, zdôraznenie nepokrytých oblastí
* vybudovanie centrálnych odborných kapacít (na začiatku budú asi virtuálne, viazané na štátnu inštitúciu (NBU, ÚV?) poskytujúcou organizačné a finančné zabezpečenie a s nejakým koordinačným orgánom), ktoré budú plniť (bude treba začať postupne a potom sa uvidí, či je rozumné sústreďovať ich a ak áno, ktoré)
  1. metodické a koncepčné úlohy
  2. tvorba legislatívy, sledovanie európskej a slovenskej pripravovanej legislatívy (opravy, koordinácia – ale na to potrebujeme garanta s dostatočnou autoritou, aby to dokázal presadiť)
  3. štandardizácia v oblasti IB/KB – medzinárodná (výber medzinárodných štandardov, ktoré budú zaradené do STN a podpora ich prebratia/prekladu; tvorba domácich štandardov)
  4. bezpečnostné štandardy pre ISVS a odporúčané pre ostatných
  5. certifikácia a akreditácia systémov, nezávislý audit a testovanie
  6. terminológia
  7. vlastný výskum v kľúčových oblastiach
  8. stimulácia a koordinácia výskumu v IB/KB (účasť na tvorbe programov, činnosti grantových agentúr a pod.)
  9. klasifikácia informácie a systémov (metodika klasifikácie a kritériá pre klasifikáciu, možno kategorizácia = stanovenie typov informácie)
  10. požiadavky na základnú úroveň ochrany (analógia Grundschutz BSI) a ich udržiavanie (sledovanie vývoja hrozieb, objavovania zraniteľností, posudzovanie nových systémov a technológií)
  11. sledovanie úrovne IB/KB na Slovensku (raz za dva roky prieskum stavu IB a predloženie do Vlády s návrhom opatrení)
  12. kontrola, testovanie a audit bezpečnosti ISVS (tieto funkcie budú primárne musieť plniť aj štátne orgány v okruhu svojej pôsobnosti, ale v prípade vážnych problémov by takéto funkcie mal kvôli nezávislej kontrole mať možnosť vykonávať aj centrálny orgán)
  13. znalostné štandardy (aké znalosti a zručnosti v IB/KB potrebujeme, koľko akých ľudí) požiadavky na vzdelávanie (akreditácia programov), možno vzdelávanie vybraných skupín ľudí (kvôli spätnej väzbe a overovaniu metodiky)
  14. podpora vzdelávania v IB/KB na vzdelávacích inštitúciách (technická IB/KB, manažérska, právnici, vyšetrovatelia)
  15. cvičenia v IB/KB (účasť na medzinárodných, organizácia národných cvičení)
  16. zastupovanie SR v odborných orgánoch (pracovných skupinách) EÚ, NATO a iných organizácií a využívanie (použiteľných) informácií (semináre);
* centrálne operačné kapacity na riešenie globálnych bezpečnostných incidentov a rozsiahlych útokov na slovenský virtuálny priestor (monitoring slovenského virtuálneho priestoru a jeho častí; identifikácia príznakov útokov a organizácia obrany – armáda? a CSIRTy);
* budovanie globálneho obranného systému slovenského virtuálneho priestoru
* vytváranie/zvyšovanie bezpečnostného povedomia používateľov
* budovanie odborných kapacít na zabezpečenie existujúcich systémov (rutinná prevádzka) (príloha 8.9)

## CSIRT

* zmapovanie potrieb verejnej správy v oblasti podpory pri riešení bezpečnostných incidentov (Koľko a akých útvarov CSIRT bude treba v optimálnom prípade, čo je nutné minimum,. kde by mali byť zriadené a postup pri ich budovaní)
* podpora existujúcich útvarov CSIRT
* využívanie existujúcich útvarov CSIRT na prípravu odborníkov pre nové útvary CSIRT
* dohoda o spolupráci
* podpora pri medzinárodnom etablovaní nových útvarov
* vytvorenie cvičného akademického útvaru CSIRT (SANET, vysoké školy, ale najmä príprava ľudí pre prax)

## Ministerstvá a im na roveň postavené štátne orgány

* inštitúcie zodpovedné za rezort alebo oblasť
* ustanovenie človeka zodpovedného za IB/KB – bezpečnostný manažér rezortu
* týchto ľudí budeme asi musieť vyškoliť,  pripraviť im návrh postupu a poskytovať minimálne metodickú, ale asi aj odbornú pomoc (výnimiek nebude veľa)
* bezpečnostný manažér (s prípadnou pomocou externých odborníkov) zabezpečí zmapovanie stavu IB/KB v rezorte (kritické informačné systémy)
* stručná koncepcia (čo rezort v IB/KB potrebuje) a postup, ako to dosiahnuť
* ale súčasne s koncepčnými a analytickými prácami presadzovanie štandardizovaných riešení

## Štátne inštitúcie (stredná a nižšia úroveň)

* inštitúcie zodpovedajúce za ISVS alebo prevádzkujúce ISVS
* na podnet/príkaz nadriadeného orgánu zriadenie funkcie bezpečnostného manažéra
* vyškolenie bezpečnostného manažéra (uvidíme, koľko ich treba, môžeme poskytnúť metodické materiály, pri zvládnuteľnom počte ich aj školiť centrálne)
* jednoduchý bezpečnostný projekt organizácie, bezpečnostná politika
* školenia zamestnancov
* podobne ako v prípade ministerstiev súčasne s koncepčnými a analytickými prácami presadzovanie štandardizovaných riešení

## Špeciálne systémy a aplikácie

* pozrieť sa či neexistujú ISVS, pre ktoré nestačí uplatnenie štandardných postupov z častí 7.3 a 7.4
  + kritická informačná infraštruktúra – štátna, súkromná, iná (Direktíva NIS)
  + systémy súvisiace s e-Gov (ÚPVS, referenčné registre, systémy pre manažment identity)
  + utajované skutočnosti
  + osobné údaje
* majú inštitúcie prevádzkujúce takéto ISVS dostatočne kvalifikovaných ľudí?
* ak nie,
  + vyškoliť ľudí
  + spraviť analýzu rizík
  + bezpečnostné projekty na špeciálne systémy
  + zavedenie ISVS
  + správa rizík, priebežné monitorovanie a nezávislý audit
* ak áno, bezpečnostný projekt a ostatné si spravia sami (stačí skontrolovať)
* povinná certifikácia a akreditácia (kto to bude robiť?)

## Systémy ktoré nie sú ISVS

* pre tie, ktoré nie sú pripojené k ISVS majú bezpečnostné štandardy a baseline ochrana len charakter odporúčaní
* systémy, ktoré komunikujú s ISVS musia spĺňať podmienky na pripojenie, aby neohrozili ISVS

# Ďalšie kroky (úlohy)

# Prílohy

## Zoznam skratiek

* spravíme po napísaní dokumentu

## Malý výkladový slovník

* máme hotový

## Stav legislatívy

* prehľad relevantných zákonov, bezpečnostné požiadavky na ochranu ISVS, ktoré z nich vyplývajú, porovnanie
* prehľad právnych aktov EÚ, z ktorých vyplývajú požiadavky na ochranu ISVS

## Klasifikácia informácie a systémov

* FIPS 199 a FIPS 200, máme spracovaný
* chýba zoznam typov informácie, ktoré je potrebné rozlišovať
* možno by bolo dobré spraviť zoznam typov systémov, aby sme si vedeli predstaviť, na čo sa budú všeobecné požiadavky aplikovať a či to je relevantné

## Minimálne požiadavky na ochranu ISVS (Baseline)

* nemecký alebo americký model, alebo ich skúsime skombinovať?

## Bezpečnosť v priebehu životného cyklu ISVS

* len stručne – kto a čo má v jednotlivých fázach životného cyklu spraviť, ale nezachádzať do detailov. Podrobnejší popis by mal byť v metodických materiáloch, pozri NIST SP 800.

## Bezpečnostný projekt systému

* ostaneme pri systéme, alebo pripustíme škálovanie bezpečnostného projektu (od systému až po organizáciu)?
* zahrnieme správu rizík pod bezpečnostný projekt, alebo do projektu dáme len analýzu rizík?
* postup podľa ISO/IEC 15408, resp. ISO/IEC 27005

## Riadenie informačnej bezpečnosti v organizácii

* ISO/IEC 27001, 27002, tiež BSI Standards
* význam a popis ISMS, zavádzanie ISMS však rozhodne nerobiť podľa ISO/IEC 27003

## Zoznam bezpečnostných rolí a kvalifikačné požiadavky na jednotlivé roly

* máme

## Systém vzdelávania v IB/KB

* existuje Vládou schválený materiál, ktorý sa podarilo realizovať len čiastočne, nevyrábajme ďalší, ale skúsme rozbehnúť prípravu kvalifikovaných ľudí v čo najkratšom čase:
* stanovme priority – akých ľudí štátny sektor akútne potrebuje
* máme definované znalostné štandardy;
* máme podrobné sylaby a učebné texty;
* zrevidujme existujúce materiály a doplňme ich (analýza použiteľnosti materiálov zo vzdelávacieho  projektu MF SR je hotová)
* spravme inventarizáciu vzdelávacích kapacít (v prvom rade ľudí, až potom inštitúcií)
* pripravme a spustime pilotný projekt na vyškolenie týchto ľudí (úvodné školenia, praktické vzdelávanie, cyklické celoživotné vzdelávanie)
* vyhodnoťme pilotný projekt (resp., ak to chceme skrátiť, vychádzajme z poznatkov zo vzdelávacieho projektu MF SR) – obsah, formy, témy, ktoré by bolo treba doplniť, výber ľudí, metodika vzdelávania, skúšky, certifikát
* identifikujme inštitúcie, ktoré by sa dali použiť ako školiace pracoviská, ponúknime im metodickú (technickú a materiálnu?) pomoc, zorganizujeme školenia lektorov, prípadne stáže vo fungujúcich inštitúciách
* vysoké školy (TU Žilina, UPJŠ a TU Košice)
* špeciálne vysoké školy a vzdelávacie inštitúcie (Liptovský Mikuláš, Policajná akadémia Bratislava, Justičná akadémia (?) Bratislava)
* formy
* rozšírenie obsahu existujúcich študijných programov o IB/KB, resp. doplnenie výberovej výučby
* plné vzdelávanie podľa študijných programov vypracovaných centrálne
* spustíme vzdelávanie v školiacich pracoviskách

1. asi by sme mali zdôrazniť, že ide o IKT, ktoré vznikli spojením počítačov, telekomunikačných sietí a masovokomunikačných prostriedkov, pretože pori nich existujú aj tradičné IKT; IKT, ktoré spôsobili informačnú revolúciu sa vyznačujú automatizovaným spracovaním digitálne kódovanej informácie. Možné označenie by bolo digitálne IKT [↑](#footnote-ref-1)