Junior centra excelence informační bezpečnosti v ČR

Koncepce JCE IB v ČR

Verze 13, 11.3.2020 Zpracoval: Jiří Sedláček, NSMC

1 Obsah

2 Preambule

Dále uvedený text je materiálem, jehož cílem je:

- definovat poslání junior center excelence (dále „JCE“),
- definovat přístupy JCE k zavedení informační bezpečnosti v organizaci typu střední škola,
- definovat přístupy JCE k výuce informační bezpečnosti,
- definovat postup jak se stát JCE,
- definovat organizační strukturu JCE.

Jedná se o koncepční materiál.

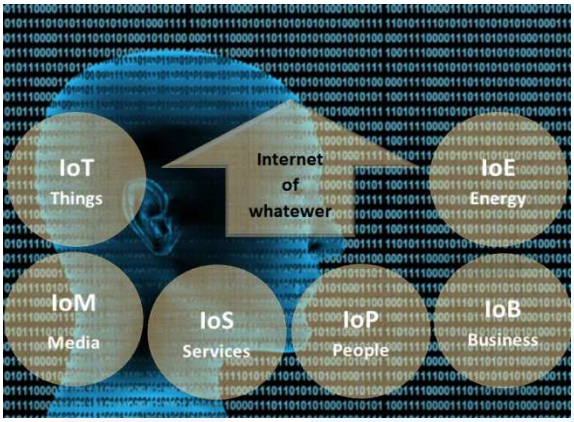
Excelentní centra jsou výjimečná, progresivní, jak s ohledem na přístup k výuce a evangelizaci informační bezpečnosti a s ohledem na implementaci bezpečnostních opatření v organizaci typu střední škola, tak i s ohledem na technické vybavení. Z důvodu rovnoměrného pokrytí celého území ČR těmito specializovanými středními školami uvažujeme jako optimální krajský model. Je rovněž nezbytné respektovat i ekonomické aspekty.

Excelentním centrem nemůže být každá střední škola. Každá střední škola ale může (právě i s pomocí excelentních center) vyučovat informační bezpečnost.

Každé JCE je startupem v rámci procesu rozvoje lidského kapitálu.

3 Předmluva

V dnešní dynamické době jsme stále častěji konfrontováni s pojmy IoT, IoS, IoP, …, průmysl 4.0, chytré domy, chytrá města, cloudové služby, eGovernment, ale také kyberválka, kyberzločin, kyberšikana, kyberšpionáž, kybersabotáž, atd. Závislost dnešní společnosti na elektronických technologiích je stále vyšší a vyšší, stejně tak jako rizika z toho plynoucí. Stále častěji je zmiňována otázka tzv. kontinuity činnosti organizace (Business Continuity), která je v úzké vazbě a provázanosti s ICT. V případě narušení funkce informační infrastruktury, informačních technologií, řídících systémů, průmyslových technologií, mohou být následky pro danou organizaci takového rozsahu, že řádově převyšují náklady na implementaci informační bezpečnosti. Pokud naše společnost nezmění přístup k této problematice, budou finanční ztráty narůstat. Základem pro změnu myšlení není nic jednoduššího, než vzdělávání. Změna přístupů a chování, která spadá pod bezpečnost lidských zdrojů, je naprosto klíčová. A to od řídících struktur až po řadové zaměstnance.



Události v nemocnici Benešov a v OKD ukazují, jak jsme na informačních technologiích závislí. Zároveň nám bylo nastaveno zrcadlo. Ukázalo se, jak je otázka informační a kybernetické bezpečnosti podceňována a nedostatečně řešena a jaké fatální dopady z toho plynou. Kde jsou péče a odpovědnost řádného hospodáře?

Dne 1.1.2015 vešel v účinnost **zákon** č. **181/2014 Sb**., **o kybernetické bezpečnosti** a o změně souvisejících zákonů (dále ZoKB), ve znění pozdějších předpisů. To je v naší legislativě významným milníkem, díky němuž se začal měnit přístup ke kybernetické bezpečnosti nejen z pohledu organizačních a technických opatření, ale i v právní rovině (povinné subjekty mají zákonnou povinnost řešit kybernetickou bezpečnost) a v oblasti vzdělávání a evangelizace. Počet povinných osob daný §3 ZoKB byl v roce 2017, po transpozici evropské směrnice NIS, rozšířen. Od 25.5.2018 je v účinnosti evropské nařízení o ochraně osobních údajů známé pod názvem GDPR.

Je zcela zjevné, že ruku v ruce s tímto vývojem musí jít i informační a kybernetická bezpečnost včetně edukace o čem tato problematika vlastně je. V ČR neexistují žádná organizace ani žádný občan, kterých by se vše výše uvedené netýkalo. Každá organizace řeší náklady, kvalitu a rozsah poskytovaných služeb, legislativní mantinely, ochranu svých zájmů a aktiv. Každý občan bude v osobním životě v kybernetickém prostoru dříve či později řešit komunikaci se státní správou a samosprávou (eGovernment), bezpečnost svou, zabezpečení svého majetku, bezpečnost svých blízkých. Budování bezpečnostního povědomí a znalostní základny je proto nezbytné už v prostředí středních škol.

Důvodem je nejen potřeba zajištění fungování (zapojení) občana v rozvinuté informační společnosti, případně příprava SŠ studentů na vyšší vzdělání, ale i potřeba uspokojení poptávky (výrazně převyšující nabídku) po středoškolských pracovnících/odbornících z této oblasti.

Abychom u naší populace dosáhli potřebné a nezbytné míry vzdělání v oblasti informační a kybernetické bezpečnosti, je vhodné, efektivní a přínosné jít cestou excelentních center, zaměřených na výuku informační a kybernetické bezpečnosti, která budou schopna zajistit jak kvalitní vzdělání pro své žáky, tak předávat znalosti (případně sdílet unikátní bezpečnostní technologie v centrech instalované) ostatním SŠ v rámci svého kraje. Tato excelentní centra potřebují pro plnění své funkce kvalifikovaný pedagogický sbor, potřebné technické prostředky a samozřejmě rovněž podporu zřizovatele a to nejen pouze v deklaratorní rovině. Financování je nutné zajistit jak na krajské, tak i republikové úrovni, případně z fondů EU.

4 Východiska

♦ **Národní strategie kybernetické bezpečnosti (NSKB) české republiky na období let 2015 – 2020.**

„Český model vzdělávání a výchovy v oblasti kybernetické bezpečnosti **NEODPOVÍDÁ** v současné podobě aktuálním požadavkům a trendům. Z tohoto důvodu pak nedostatečně vzdělává a vychovává na základním a středním stupni žáky a také v nedostatečné míře nabízí vysokoškolské programy, které by vytvářely odborníky na kybernetickou bezpečnost. Poptávka po těchto odbornících je přitom vysoká."

♦ **Akční plán k NSKB 2015 – 2020.**

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.
- 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.**

- Povinnost organizace typu SŠ chránit informace, stanovená:
  - Platnou legislativou definující působnost subjektu -> rámec pro vymezení požadavků na informační bezpečnost.
  - Zřizovatelem (např. v JmK je to bezpečnostní politika Jihomoravského kraje z 09/2016).
- Péče řádného hospodáře a kontinuita byznysu.
- KAP krajů.
- Zastaralé ICT v prostředí SŠ a jejich nezbytná modernizace.
- ZoKB, GDPR a další související legislativa.

Z výše uvedeného je zřejmé, že výuka informační a kybernetické bezpečnosti není ve středním školství na úrovni odpovídající požadavkům rozvinuté informační společnosti, pracovního trhu, průmyslu, standardů a legislativy (jak evropské, tak i ČR) a rozmachu internetu. Školy musí plnit zákonnou povinnost - zajistit výuku studentů a současně musí chránit informace o studentech (zajištění dostupnosti, důvěrnosti a integrity), které jsou mnohdy charakteru zvláštní kategorie osobních údajů (viz např. dopady inkluze). Jsou povinny archivovat informace nezbytné k vystavení opisů studijních dokladů. Musí zajistit

dostupnost svých informačních systémů z internetu, ať už z důvodu administrace, či z důvodu přístupu rodičů studentů. Musí chránit sebe sama před studenty.

Lidský faktor je nejslabším článkem v oblasti IB/KB. Vliv elektronických technologií na fungování organizací a každodenní život obyvatel je výrazný (zatím stále podceňovaný). Každá organizace a každý občan jsou součástí kybernetického prostoru. Adekvátní reakce vzdělávacího systému je nezbytná a neodkladná.

ZoKB je velice dobře propracovaný, nicméně je závazný pouze pro tzv. „povinné osoby“, které jsou kategorizovány v §3. Pro ostatní právnické osoby ale může být ZoKB velice dobrým vodítkem, respektive jeho prováděcí **vyhláška** č. **82/2018** Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti - VyKB). Zpracování osobních údajů podléhá od 25.5.2018 (účinnost) evropskému nařízení známému pod zkratkou GDPR.

5 Principy

Při budování JCE je nezbytné brát zřetel na:

- **Systémový přístup**

Každá organizace sestává z lidí, procesů a technologií. Problematika IB/KB je proto řešena komplexně. Systémově je, s využitím této koncepce, řešena právě výuka informační bezpečnosti, včetně dalších služeb a poslání JCE.

- **Analytický přístup**

Než jsou přijímána rozhodnutí, je nezbytné danou problematiku podrobit analýze. Jedině tak je možné nasazovat vhodná a ekonomicky přijatelná řešení.

- **Měřitelnost**

IB/KB je postavena na měřitelnosti. Ať už z pohledu zavedených opatření, tak i z pohledu ekonomického - efektivity a účelnosti vynaložených nákladů.

- **Opakovatelnost, přenositelnost, kompatibilita**

Jak z pohledu času, tak z pohledu financování je vhodné použít řešení, které je principiálně přenositelné i na ostatní obdobné organizace. Jednotná koncepce budování laboratoří, jednotný přístup k informační bezpečnosti ve školách samotných, principiálně shodný systém výuky informační bezpečnosti (osnova dle NSMC) a plnění poslání JCE v rámci daného regionu v souladu s touto koncepcí, to vše je zárukou přenositelnosti takto vzniklého know-how.

- **Standardy**

Tak jako jsou jako norma přijaty v oblasti IB standardy (např. normy řady ISO27k), stejně tak je nutné tento přístup aplikovat na zvolená technická opatření. Není vhodné stavět bezpečnostní řešení majoritně na OpenSource platformách, kdy dvě implementace stejné technologie se po nějakém čase dostanou do podoby proprietárních nekompatibilních systémů.

- **Udržitelnost**

U OpenSource platforem není možné tento požadavek garantovat. Z tohoto pohledu je nasazení OpenSource produktů vnímáno jako nesystémové řešení použitelné pouze pro testovací a simulační účely, nikoli pro vzor implementace IB v reálné organizaci s ohledem na skutečnost, že takové neměřitelné řešení může být z pohledu IB samo hrozbou.

- **Racionalita**

Optimální přístup k řešení problematiky IB je postavený na racionálních rozhodnutích.

- **Dokumentovatelnost**

Veškeré kroky jsou v oblasti IB/KB dokumentovány.

- **Systematičnost**

Souvisí se systémovým přístupem. ISMS vnímáme jako celek složený z elementů - součástí s uplatněním vzájemných vazeb.

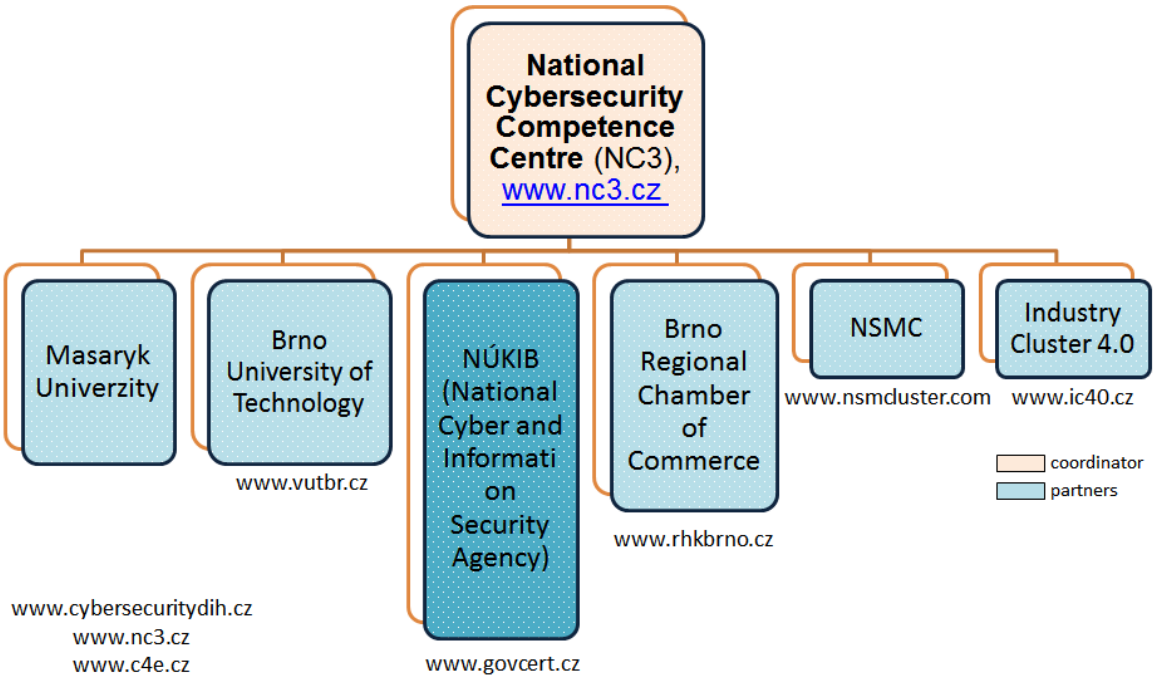
- **Metodičnost**

Veškeré zaváděné postupy v IB/KB jsou aplikovány na základě předem stanovených metodik.

Jako **etalon** JCE lze v ČR, jak v oblasti přístupu k implementaci informační a kybernetické bezpečnosti v organizaci typu střední škola, stejně tak i v oblasti výuky této problematiky, brát SŠ IPF Čichnova Brno. Tato škola je zatím, s ohledem na tuto koncepci, nejdále.

6 Organizace JCE

Excelentní centra jsou organizačně začleněna pod Masarykovu univerzitu v Brně, která je součástí CIH (Cybersecurity Innovation Hub). Jedná se o multidisciplinární prostředí pro výzkumné instituce, orgány veřejné moci, klastry, soukromé společnosti a ostatní subjekty působící v oblasti kybernetické bezpečnosti, zaměřené na spolupráci, sdílení informací, vzájemnou podporu, společný výzkum a implementaci inovací a špičkových technologií a řešení zajišťujících kybernetickou bezpečnost produktů, služeb a infrastruktur.



Tím je zaručeno zejména:

- systémový přístup,
- kompatibilita,
- odbornost,
- efektivní spolupráce s akademickou sférou (MU, VUT),
- propojení s gestorem v oblasti kybernetické bezpečnosti (NÚKIB),
- propojení se znalostní platformou v oblasti IB (NSMC), jenž je autorem této koncepce.

Střední školy, které budou mít/mají ambici stát se JCE, jsou určovány ve spolupráci s Asociací krajů (ať už se hlásí AK samy, nebo jsou ve spolupráci s AK určeny). Masarykova univerzita se spolu s NSMC podílí na definici jejich poslání a kompetencí, koordinuje jejich vzájemnou spolupráci a předávání zkušeností a podílí se na udržování a zvyšování jejich odbornosti, včetně certifikací. Systém certifikací bude jedním z efektivních nástrojů zajištění a udržení odborné úrovně JCE.

Jen Ti nejlepší mohou ČR pomáhat zvyšovat odbornou úroveň pracujících a zajišťovat tak nejen její konkurenceschopnost, ale i nezávislost.

7 Vize, ambice, poslání JCE

- Středoškolská centra excelence budou průkopníky pro zajištění výuky IB ve všech RVP.
- Výuka IB/KB pomůže zajistit podmínky pro hladce fungující informační společnost, občané získají potřebné návyky pro zodpovědné chování v kyberprostoru (Human Firewall), čímž bude významně redukována úspěšnost kybernetických útoků prostřednictvím lidského faktoru a občanům bude (díky nabytým znalostem) umožněn přístup k elektronickým službám rozvinuté informační společnosti.
- Zajištění potřebné expertní základny umožní lépe čelit nejnovějším kybernetickým hrozbám.
- ČR bude umožněno udržet dosavadní významné postavení v oblasti KB v celosvětovém měřítku, což přispěje k udržení její konkurenceschopnosti.
- Kritická informační infrastruktura, s úzkou vazbou na industriální systémy, bude efektivněji chráněna, kyberprostor ČR bude lépe zabezpečen, sociální a ekonomické zájmy budou lépe zajištěny.
- Vládní CERT podpoří vznik juniorních CSIRTů – JCSIRT na excelentních centrech v krajích.

Možnosti využití JCE:

- metodika implementace IB/KB a OOÚ v organizaci typu střední škola vycházeje z požadavků daných MŠMT, zřizovatelem, v rámci možností každé školy taktéž návodně z povinností dle ZoKB pro správce VIS (§3 písmeno e) a GDPR,
- evangelizace a vzdělávání IB/KB jak pro žáky, tak i pro veřejnost,
    - semináře,
    - uvědomovací akce,
    - konference,
    - videokonference,
    - kurzy, cvičení, školení, trénink,
- sdílení bezpečnostních technologií laboratoří JCE pro ostatní školy v rámci daného regionu (vynaložení potřebných finančních prostředků tak bude maximálně účelné a efektivní),
- v rámci laboratoře bude možné trénovat implementaci IB/KB a ochrany osobních údajů ve fiktivní organizaci (stanovení právní formy organizace, stanovení interního a externího kontextu, stanovení organizační struktury, vytvoření interní legislativy, identifikace aktiv, určení hranic ISMS v organizaci, aplikace adekvátních organizačních a technických opatření podložených analýzou rizik, zajištění kontinuity byznysu včetně stanovení DRP),
- spolupořádání soutěží k uvedené problematice,
- pořádání tabletop cvičení a bezpečnostních cvičení.

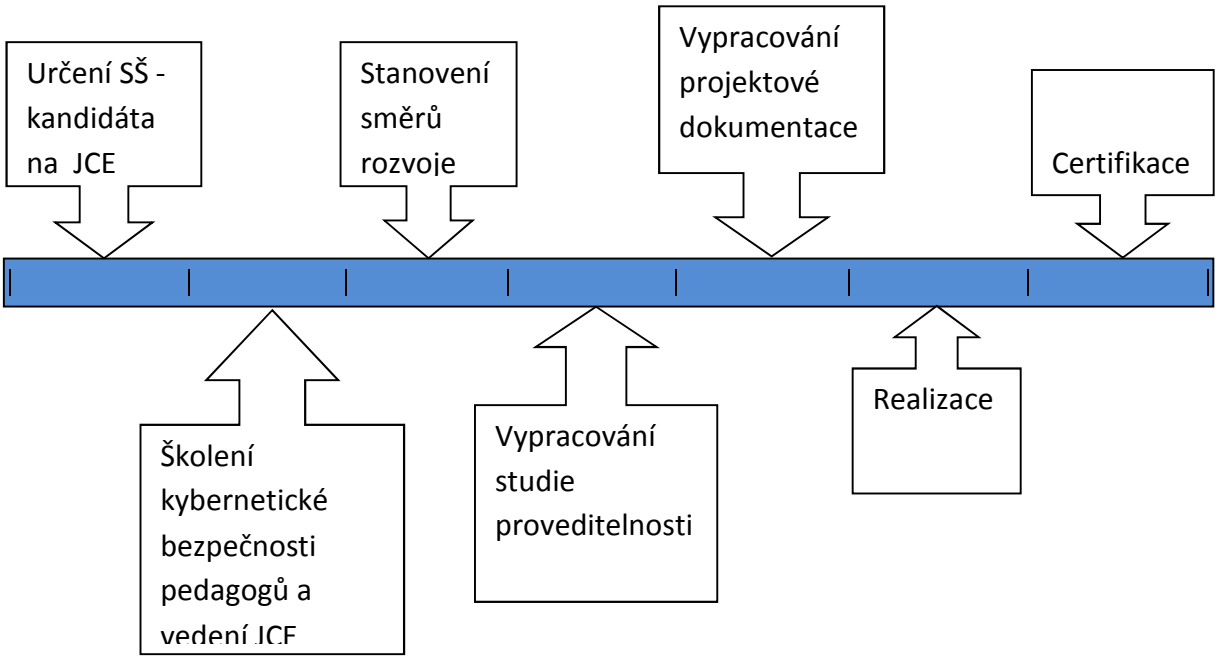
Naší ambicí je vybudování jednoho excelentního centra pro výuku informační bezpečnosti v každém kraji. Naší vizí je navyšovat počet těchto excelentních center v souladu s možnostmi a rozvojem daného regionu.

8 Pro úspěch koncepce je nezbytné zajistit

- Záštitu národní autoritou v oblasti KB – NÚKIB (NÚKIB koncepci JCE podporuje).
- Vzdělané vedení zapojených excelentních škol a vzdělaný pedagogický sbor,
    - výuka ředitelů a pedagogů v rámci DVPP – akreditované kurzy MŠMT (NSMC - číslo akreditace: MSMT- 8135/2019-1-357).
- Revitalizované/modernizované ICT excelentních center.
- Zbudované kybernetické laboratoře s orientací na standardy tak jak je tomu v reálném životě (žáci nebudou odtrženi od praxe, bude garantována udržitelnost projektů).
- Potřebné finanční prostředky pro výše uvedené ve spolupráci se zřizovateli.
- Spolupracující vysoké školy (MU, VUT, ČVUT, ÚTB…).
- Spolupracující organizace zabývající se IB/KB (NSMC).

Pokud se tato koncepce začne uplatňovat jako podklad pro projekty budování JCSIRT, bude vytvořena podrobná implementační projektová mapa.

9 Popis procesu vybudování JCE v daném kraji



Jak je z obrázku zřejmé, proces vybudování JCE se děje postupnými kroky:

- Určení kandidáta na JCE.
- Školení vedení školy a pedagogického sboru.
- Stanovení směrů rozvoje školy.
- Vypracování studie proveditelnosti.
- Vypracování projektové dokumentace.
- Realizace projektu.
- Certifikace.

Každý jednotlivý krok bude popsán dále.

9.1 Určení vhodné SŠ – kandidáta na JCE

Koncepce JCE je postavena na krajském modelu, kdy je nejen z finančních důvodů uvažována v každém kraji jedna excelentní střední škola, která bude schopna naplnit myšlenku JCE pro informační bezpečnost.

Tento model byl představen na zasedání Asociace krajů ČR, komise pro vzdělávání, dne 5.9.2019, v rámci prezentačního bloku NÚKIB, panem Jiřím Sedláčkem z NSMC (autor této koncepce). AK ČR přislíbila této koncepci podporu a do zápisu z jednání komise byl zaznamenán úkol vytipování škol ve všech krajích ČR. Samozřejmě je brán zřetel na to, když se nějaká SŠ s ambicí stát se JCE IB přihlásí sama.

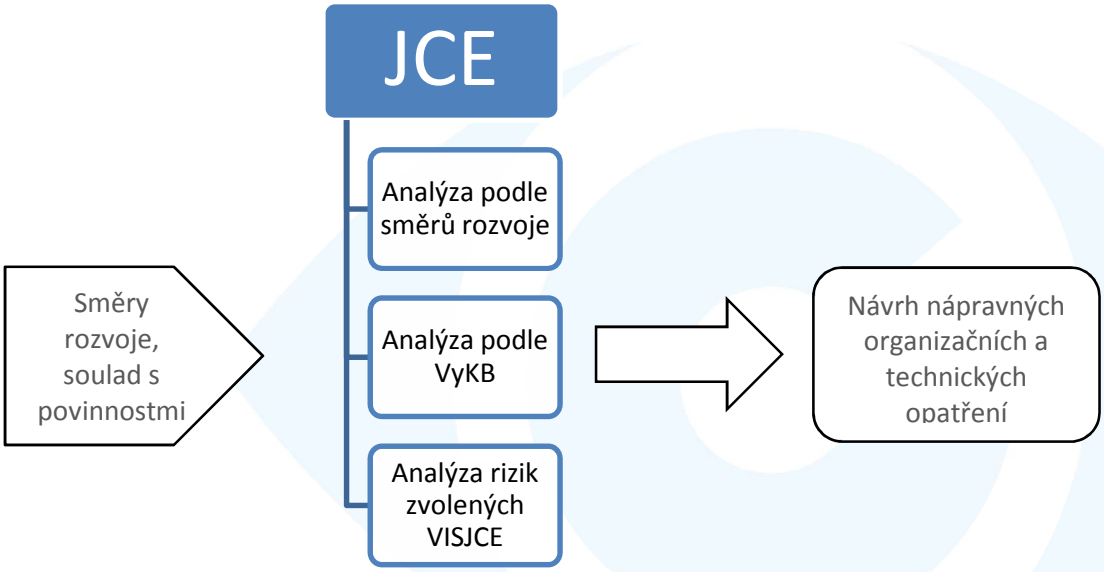
9.2 Školení kybernetické bezpečnosti pedagogů a vedení školy

Vedení JCE a pedagogický sbor musejí být uvedeni do problematiky informační a kybernetické bezpečnosti. Důvodem je budování bezpečnostního povědomí a zavádění bezpečnostní kultury, na což je nutné brát zřetel v každé organizaci, zejména pak v excelentních centrech, která mají být vzorem pro ostatní SŠ. Bezpečnost lidských zdrojů je řešena jak ve standardu ISO 27001, tak i ve vyhlášce o kybernetické bezpečnosti.

Takováto školení realizují v ČR různé organizace. NSMC má vlastní kurz kybernetické bezpečnosti: Kybernetická bezpečnost pro pedagogické pracovníky a management středních škol. *Vzdělávací program byl akreditován MŠMT v rámci systému dalšího vzdělávání pedagogických pracovníků (DVPP) pod č.j.: MSMT-8135/2019-1-357.*

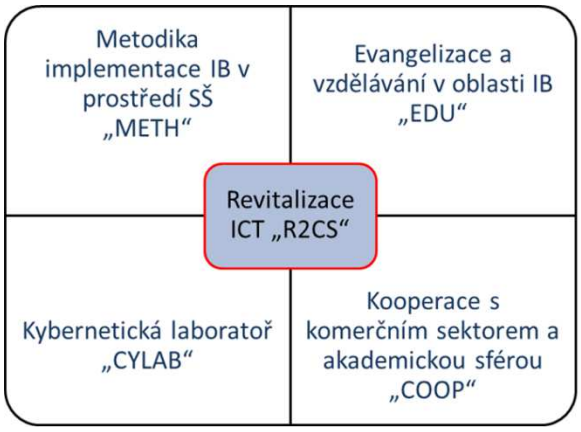
9.3 Stanovení směrů rozvoje

Stanovení směrů rozvoje školy je klíčové. Na základě toho si škola ujasní své přístupy k implementaci informační bezpečnosti v produkčním prostředí, k výuce informační bezpečnosti a k její evangelizaci mimo školu, k vybudování laboratoře a ke spolupráci jak s ostatními JCE, SŠ, tak i s VŠ a ostatními subjekty.



Klíčovými parametry pro směry rozvoje jsou:

- **R2C –** Ready to Cybersecurity – uvedení školy do stavu, který jí umožní implementovat informační bezpečnost (organizační a technická opatření).
- **METH** - Metodika implementace IB v prostředí SŠ.
- **EDU** - Evangelizace a vzdělávání v oblasti IB.
- **CYLAB** – Kybernetická laboratoř.
- **COOP** – Kooperace s ostatními JCE, akademickou sférou, komerčním sektorem a ostatními organizacemi.



Excelence spočívá nejen ve výuce daného předmětu s využitím moderních technologií, ale i v přístupu k informační bezpečnosti ve škole samé, v předávání a sdílení znalostí, scénářů a zkušeností a sdílení techniky prostřednictvím vzdáleného přístupu nejen mezi JCE, ale i mimo ně v rámci regionu.

9.4 Vypracování studie proveditelnosti

Po stanovení směrů rozvoje má kandidát na JCE dostatek informací pro specifikaci poptávky na vypracování studie proveditelnosti.

Studie proveditelnosti řeší zejména:

- Organizační a technická opatření pro produkční prostředí školy a technické vybavení CYLAB, v souladu s vytyčenými směry rozvoje.
    - GAP analýza podle směrů rozvoje.
    - GAP analýza podle VyKB (VyKB je pouze metodickým vodítkem, organizace typu škola není povinnou osobou z pohledu ZoKB).
    - Analýza rizik VISJCE (určených IS školy jako primárních aktiv a zpracování analýzy rizik pro tyto IS).

Studie proveditelnosti stanovuje rozsah organizačních a technických opatření v produkčním prostředí školy a požadavky na vybavení CYLAB, včetně stanovení hrubé cenové kalkulace.

Studie proveditelnosti je informačním zdrojem pro sestavení zadávacího řízení na vypracování projektové dokumentace.

9.5 Vypracování projektové dokumentace

Na základě zpracované studie proveditelnosti je nutné vypracovat projektovou dokumentaci včetně výkazů výměr (podrobné položkové rozpočty).

Projektová dokumentace je finálním projektovým materiálem pro realizaci projektu JCE.

9.6 Realizace

Na základě vypracované detailní projektové dokumentace je zadán požadavek na VŘ pro realizaci.

9.7 Certifikace

Certifikace JCE je finálním krokem k získání statutu JCE. V rámci certifikace bude posuzováno naplnění principů dle této koncepce, přístupy k implementaci informační bezpečnosti v organizaci typu SŠ, k výuce informační bezpečnosti a její evangelizaci, k předávání znalostí a zkušeností, k plnění funkce JCE v rámci regionu.

Certifikační mechanismus zpracovává NSMC ve spolupráci s MU, i s ohledem na podněty v rámci EU.

Certifikace JCE je finálním krokem k získání statutu JCE.

10 Definice přístupu k implementaci IB/KB v daném JCE

Z vytyčených směrů rozvoje JCE vyplývají požadavky na technické zajištění infrastruktury organizace.

Technickým zajištěním je myšleno:

- síťová infrastruktura,
- zvýšení úrovně fyzické bezpečnosti školy,
- výkonná serverová infrastruktura pro provozní prostředí školy,
- výkonná serverová infrastruktura pro CYLAB,
- modernizované, případně nové prostory pro CYLAB,
- komunikační infrastruktura (videokonferenční systém),
- modernizace zařízení pro zajištění kontinuity, vysoké úrovně dostupnosti a řešení havarijních situací,
- nástroje na zajištění zvýšené úrovně kybernetické bezpečnosti.

Velice dobrým doplňkovým vodítkem je např. materiál NÚKIB: BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 3.0
https://www.govcert.cz/download/doporuceni/NUKIB_doporuceni_admin_3.0_barva.pdf

10.1 Síťová infrastruktura

- dostatečně dimenzované páteřní propoje, s ohledem na zajištění provozní spolehlivosti a dostatečné přenosové rychlosti,
- spolehlivé/nechybující metalické kabelové rozvody,
- oddělení prostředí CYLAB od provozního prostředí školy,
- zajištění dostupnosti VISJCE (u kterých je to vyžadováno) z internetu,
- zajištění dostupnosti CYLAB z internetu odděleným komunikačním kanálem,
- zajištění dostatečné přenosové rychlosti u internet konektivity,
- zajištění dostatečného pokrytí prostor školy bezdrátovou technologií (dle potřeb školy),
- zajištění dostatečného počtu portů výkonnými aktivními prvky s centrálním managementem,
- vystavení web portálů školy dostupných z internetu do odděleného segmentu,
- zajištění oddělení skupin uživatelů, případně technologií segmentací provozního prostředí školy.

10.2 Zvýšení úrovně fyzické bezpečnosti školy

- zajištění fyzické bezpečnosti na úrovni perimetru školy,
- zajištění fyzické bezpečnosti serverovny.

10.3 Výkonná serverová infrastruktura pro provozní prostředí školy

- síťová infrastruktura provozního prostředí školy ve formě konvergované infrastruktury umožňující konfiguraci dle potřeb školy,
- možnost přístupu do provozního prostředí školy pomocí VPN z internetu,
- zajištění optimálních provozních podmínek, kybernetické a fyzické bezpečnosti,
- zajištění odpovídající serverové infrastruktury provozního prostředí školy formou virtuálního prostředí a bezpečnostních technologií zajišťujících business continuity.

10.4 Modernizované a nové prostory

- zajištění vhodných prostor pro umístění technologií pro provozní prostředí školy,
- zajištění prostor pro CYLAB – modrý, červený, bílý tým,
- zajištění prostor pro technologii CYLAB,
- zajištění prostor pro komunikační videokonferenční systém.

10.5 Modernizace zařízení pro zajištění kontinuity, vysoké úrovně dostupnosti a řešení havarijních situací

- zajištění zálohování dat metodou disk2disk2tape (D2D2T) s možností archivace,
- zajištění zálohování důležitých technických aktiv stanovených VISJCE využitím redundance v návrhu řešení a zajištěním náhradních technických aktiv v určeném čase,
- zajištění spolehlivé a dostatečné zálohy napájení technologií v serverovně,
- zajištění viceokruhového napájení serverovny,
- zajištění optimálních provozních podmínek v serverovně.

10.6 Nástroje na zajištění zvýšené úrovně kybernetické bezpečnosti v produkčním prostředí školy

- Zajištění řízení přístupu do sítě,

- zajištění monitoringu datových toků,
- zajištění antivirových prostředků,
- zajištění auditu privilegovaných uživatelů,
- zajištění log managementu,
- zajištění oddělení provozního prostředí školy od internetu, CYLAB a technologických řídících systémů,
- zajištění možnosti odpojení kompromitovaného zařízení od sítě,

Etalon v duchu této koncepce, JCE Čichnova, má nezanedbatelnou výhodu v napojení na KOC JMK (Security Operations Center – Kybernetické Operační Centrum zřizovatele). S tímto napojením získala JCE Čichnova technické řešení Log Management a analýzu stavu kybernetické bezpečnosti ze strany KOC v reálném čase (SIEM, procesy, vyškolení pracovníci KOC). Tím byla zajištěna vysoká úspora v řádu MIO Kč.

11 Definice přístupu k vybudování kybernetické laboratoře JCE

11.1 Výkonná serverová infrastruktura pro CYLAB

- fyzicky oddělená síťová infrastruktura CYLAB od ostatního provozního prostředí školy;
- síťová infrastruktura CYLAB ve formě konvergované infrastruktury umožňující jednoduše realizovat variabilní konfigurace prostředí pro zajištění scénářů kybernetických bezpečnostních cvičení,
- možnost přístupu do CYLAB pomocí VPN z provozního prostředí školy a internetu,
- 3 zvukově a technicky oddělené místnosti, aby byly zajištěny vhodné podmínky pro realizaci výuky formou kybernetického cvičení 3 týmů (červení – útočníci, modří – obránci, bílí – podpůrný tým),
- prostory pro obránce a útočníky by měly být dimenzovány každá pro min 10 osob, místnost pro podpůrný tým v rozsahu cca 2 osob,
- prostory by při výuce měly zajistit optimální prostředí jak v letním, tak i v zimním období při jejich plném osazení plánovaným počtem osob,
- zajištění nábytku umožňujícího operativní změnu dispozice jeho uspořádání,
- zajištění koncových bezdiskových stanic pro připojení hráčů a podpůrného týmu k tréninkové infrastruktuře CYLAB,
- zajištění odpovídající serverové infrastruktury CYLAB formou variabilního virtuálního prostředí a implementace bezpečnostních technologií k zajištění cvičebních bezpečnostních scénářů.

11.2 Sdílení znalostí, zkušeností a konfigurací v prostředí laboratoře

U CYLAB je nezbytné klást vysoký důraz na kompatibilitu technických prostředků mezi JCE vzájemně z důvodu zajištění možnosti sdílení scénářů cvičení a konfigurací infrastruktur. Tím je zajištěna možnost předávání know how mezi školami.

12 Komunikace mezi JCE a zbytkem světa s využitím moderních videokonferenčních technologií

12.1 Komunikační infrastruktura (videokonferenční systém - VCF)

- zajištění kvalitní konektivity pro VCF,
- zajištění VCF sestavy kompatibilní s JCE Čichnova,
  - HW zařízení,
  - protokoly H.323, SIP, platforma Lync,
  - možný počet spojení minimálně 1+3.

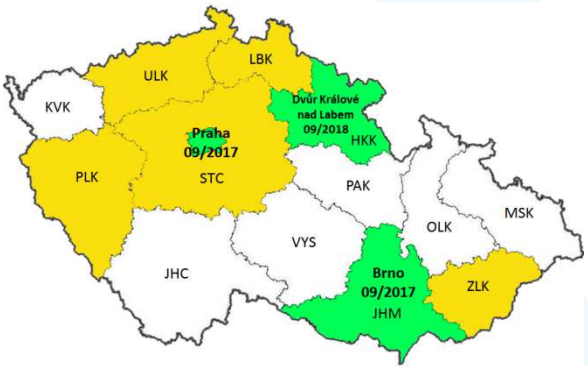
13 Sdílení znalostí a zkušeností mezi JCE

Pro sdílení znalostí, zkušeností a know how mezi JCE je nezbytné zajistit:

- Zachování co nejvyšší míry kompatibility technologií v CYLAB,
- zachování co nejvyšší míry kompatibility technologií VCF,
- sdílení znalostí a zkušeností na pravidelných workshopech (optimálně čtvrtletně),
- spolupráci na konfiguracích v CYLAB, herních scénářích, výukových a metodických materiálech.

Řídící roli zde má MU Brno z pohledu certifikační autority, metodika a koordinátora.

14 Stav JCE ke dni 30.1.2020



Legenda:

JCE – SŠ, v transformačním procesu

JCE – další vytipované SŠ

Ve spolupráci s NSMC (NSMC je autorem osnovy vzdělávacího programu KB na SŠ) probíhá výuka IB/KB na těchto středních školách v ČR:

- SŠ IPF Čichnova Brno (od roku 2017),
- SPŠ Smíchovská Praha (od roku 2017),
- SŠ IS Dvůr Králové nad Labem (od roku 2018).

V oblasti technických opatření a vybavení laboratoří však nejsou tyto školy na stejné úrovni. Spojujícím elementem je však ambice a schopnost vyučovat informační a kybernetickou bezpečnost a být lídrem v této oblasti v regionu.

Tyto výše uvedené SŠ mají výraznou zásluhu v oblasti výuky a evangelizace IB/KB v ČR.

15 Použité zkratky

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
IB	Informační bezpečnost
IS	Informační systém
JCE	Junior Centrum Excelence
KB	Kybernetická bezpečnost
KICT	Kategorie ICT
KJCE	Kategorie Junior Centrum Excelence
KZ	Kategorie základní
NSKB	Národní strategie kybernetické bezpečnosti
VISJCE	Významný informační systém JCE. V rámci koncepce máme na mysli IS, které jsou pro plnění poslání organizace typu SŠ klíčové. Název VIS, převzatý ze ZoKB §2 je zde uveden pouze pro inspiraci. **Organizace typu SŠ nespadá pod ZoKB.**
VyKB	Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).
ZoKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, ve znění pozdějších předpisů (zákon o kybernetické bezpečnosti).

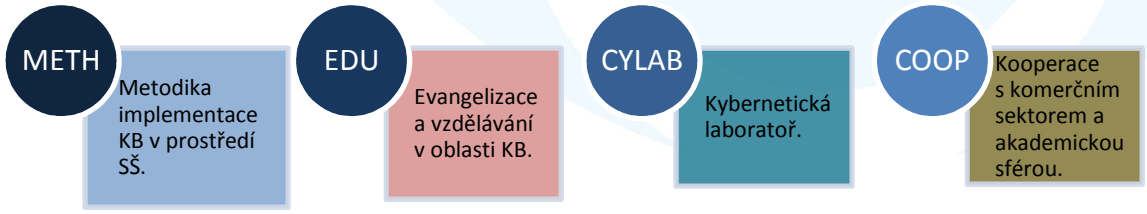
PŘÍLOHY

16 Příloha č. 1: JCE Čichnova – etalon v souladu s touto koncepcí

Popis procesu

16.1 Směry rozvoje JCE Čichnova

Směry rozvoje na obrázku znázorněné vedou k cíli - k vybudování JCE.



16.2 Využití JCE Čichnova

JCE Čichnova má tyto kompetence, schopnosti a možnosti:

- Zpracování metodiky výuky IB/KB na SŠ.
- Výuka užití standardních bezpečnostních technologií, umístěných v laboratoři školy.

    - Jak v rámci školy, tak i pro ostatní školy v rámci JMK (vzdáleně).
    - Uvažují se pouze standardy ať už z důvodu jejich měřitelnosti, z důvodu povinné udržitelnosti projektu a stejně tak i z důvodu snahy o zajištění maximálního souladu výuky na SŠ s praxí (tzn. zamezení odtržení studia od praxe).
- Vytvoření fiktivní organizace a implementace IB a KB v této organizaci v souladu se zákonnými požadavky a standardy.
- Kybernetická bezpečnostní cvičení, tabletop cvičení a soutěže.
- Forenzní analýza.
- Sdílení znalostí a zkušeností s ostatními SŠ a s akademickou sférou.
- Mentoring základních škol.
- Edukace a evangelizace IB/KB (studenti, veřejnost).
- Vybudování JSOC (Junior SOC).
- Ustavení JCSIRT týmu (Junior CSIRT).

16.3 Efektivita projektu JCE Čichnova

Efektivita projektu JCE Čichnova je zajištěna:

- Bezpečnostní technologie navržené pro provozní prostředí školy jsou pouze nezbytné a potřebné pro zajištění nejnutnější elementární úrovně informační bezpečnosti v organizaci typu SŠ a jsou pořízeny s přihlédnutím k možnostem regionu (nezanedbatelnou výhodou je napojení školy do KOC JMK - Security Operations Center JMK, včetně dodání Log Management v rámci tohoto napojení).
- Důraz na efektivní administraci navržených provozních technologií a technologií laboratoře z důvodu využití pouze pracovníků školy bez nutnosti vzniku nových pracovních pozic, pro něž škola nedisponuje dostatečnými finančními prostředky.
- Po ukončení projektu budou technologie laboratoře školy vzdáleně zpřístupněny i ostatním SŠ v rámci JMK.
- Projekt JCE Čichnova je etalonem pro vznik JCE na krajské úrovni v ČR v souladu s touto Koncepcí juniorních center excelence v oblasti informační bezpečnosti v ČR. Tato škola je etalonem pro:
    - Vybudování JCE na SŠ v ostatních krajích.
    - Aplikaci IB v prostředí SŠ – splnění zákonných povinností.
    - Výuku IB/KB na SŠ pro všechny typy RVP.
- Scénáře ve škole vytvořené budou k dispozici (v duchu této koncepce) ostatním JCE. Jedná se nejen o popis scénářů, ale rovněž o konfigurace setů ve virtuálním prostředí laboratoře. V případě zachování principu kompatibility budou takto vzniklé konfigurace přenositelné mezi JCE vzájemně.
- Všechny činnosti a úkony vedoucí ke startu/prosazení pilotního projektu výuky KB v ČR (na SŠ Čichnova a SPŠ Smíchovská) činěné zástupci obou SŠ a NSMC nestály daňové poplatníky ČR ani korunu.

- Vypracování této koncepce nestálo daňové poplatníky ČR ani korunu.
- Po ukončení projektu JCE Čichnova budou minimalizovány možné případné budoucí sankce škole za (byť neúmyslné) porušení zákonných povinností při ochraně informací např. za porušení povinností správce z pohledu ochrany osobních údajů – GDPR.

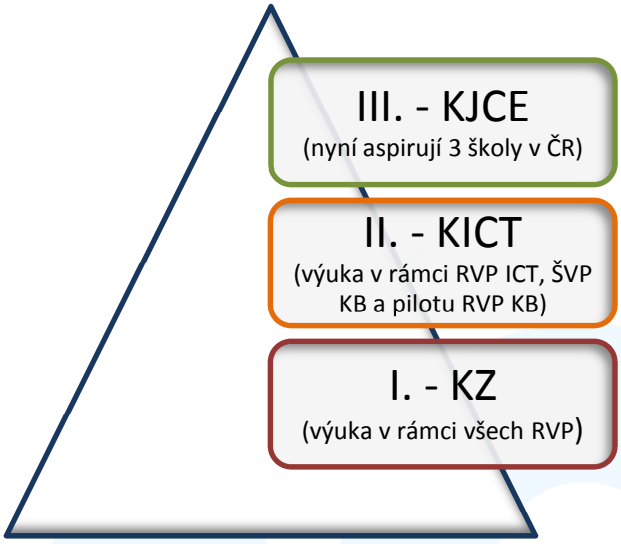
17 PŘÍLOHA Č. 2: KONCEPCE VÝUKY INFORMAČNÍ BEZPEČNOSTI NA VŠECH TYPECH SŠ V ČR

Naší ambicí je zajistit výuku informační bezpečnosti - **plošně** - na všech typech SŠ ve všech RVP v ČR. **Jedině tak bude možné naplnit cíl daný NSKB - zajištění vzdělaného občana pro fungování v rozvinuté informační společnosti.**

17.1 Jak zavést výuku IB/KB do všech SŠ

V rámci naší analýzy byly identifikovány 3 typy vzdělávacích programů IB pro SŠ v ČR:

I. **Kategorie základní** (KZ).
II. **Kategorie ICT** (KICT).
III. **Kategorie JCE** (KJCE).



17.2 Level I. - Základ - KZ

Uvažujeme výuku pro všechny typy RVP, tedy pro:

- RVP, které s ICT nesouvisí,
- RVP 18 – 20 – M/01 Informační technologie,
- ŠVP KB, případně RVP KB v pilotním ověřování.

Předpokládáme, že tato kategorie pokryje výuku IB/KB na všech školách, které nejsou více na tuto problematiku zaměřeny (specializovány) a dále na školách, které již vyučují RVP 18 – 20 – M/01 Informační technologie, ŠVP KB, případně RVP KB v pilotním ověřování.

Informační a kybernetickou bezpečnost uvažujeme vyučovat v základním rozsahu. Výuka je koncipována především se zaměřením na pokročilou evangelizaci, aby byli studenti **dostatečně připraveni na fungování v rozvinuté informační společnosti**.

Rozvinutá informační společnost je přímo závislá na občanech, kteří jsou schopni v ní fungovat. Desítky procent občanů ČR neví, co si představit pod pojmem „datová schránka“.

V rámci výuky pro KZ jsou uvažovány oblasti:

- Úvod do IB.
- Kybernetický prostor I.
- Sociální inženýrství.
- Právo v oblasti IB I.

17.3 Level II. - Střed - KICT

Uvažujeme výuku pro:

- RVP 18 – 20 – M/01 Informační technologie,
- ŠVP KB, případně RVP KB v pilotním ověřování.

Předpokládáme, že tato kategorie pokryje výuku IB/KB na všech školách, které již vyučují RVP 18 – 20 – M/01 Informační technologie, ŠVP KB, případně RVP KB v pilotním ověřování.

Informační a kybernetickou bezpečnost uvažujeme vyučovat ve středním rozsahu v návaznosti na základní rozsah. Školy jsou vybaveny učebnami ICT a mají tedy předpoklady pro výuku informační a kybernetické bezpečnosti nejen v teoretické, ale i v praktické rovině. Technická opatření je možné v počítačových učebnách implementovat a procvičovat dle možností dané školy.

V rámci výuky pro KICT jsou uvažovány oblasti:

- Informační bezpečnost v organizaci I.

17.4 Level III. - Top - KJCE

Uvažujeme výuku pro:

- ŠVP KB, případně RVP KB v pilotním ověřování.

Předpokládáme, že tato kategorie pokryje výuku IB/KB na všech školách, které již vyučují ŠVP KB, případně RVP KB v pilotním ověřování.

Informační a kybernetickou bezpečnost uvažujeme vyučovat v návaznosti na střední a základní rozsah. Zvolené školy jsou excelentními centry s výukou informační bezpečnosti a aspirující na vytvoření JCSIRT. Technické zázemí škol umožňuje i pokročilou praktickou výuku s možností procvičování vybraných technických opatření dle možností dané školy. Tyto školy mají roli lídra v oblasti IB v kraji.

V rámci výuky pro KJCE jsou uvažovány oblasti:

- Strategická analýza v organizaci.
- Integrovaná bezpečnost (IB, KB, OOÚ).
- Kybernetický prostor II.
- Právo v oblasti IB II.

- Standardy v oblasti IB.
- IB v organizaci II.

17.5 Koncepce výuky IB - závěr

Jak je z výše uvedeného zřejmé, úrovně I. – III. na sebe navazují. Tento model umožňuje výuku IB/KB na každé SŠ pro každý studijní obor na této SŠ (může nastat situace, že na jednu školu budou aplikovány všechny 3 výše uvedené kategorie). Výuka IB/KB tedy nebude nadále doménou pouze pro školy se specializovanými studijními obory, jak tomu bylo doposud.

Navržený model plošné výuky IB/KB lze aplikovat bez vyvolání okamžitých změn v systému RVP, který je sám o sobě **zastaralý, překonaný, dlouhodobě neudržitelný a vyžadující systémové změny, což je s ohledem na současnou situaci otázkou v řádu let.**

Je třeba podotknout, že NSMC ve spolupráci s MU Brno disponují znalostmi, zkušenostmi, kompetencemi a know-how pro vytvoření učebnic a dalších studijních materiálů pro výuku IB, jak je uvedeno výše. Jediné, co nám momentálně chybí, jsou dostatečné finanční prostředky. Poslední námi podaný projekt (předložen ve spolupráci s JCE Čichnova) nebyl schválen.