

Koncepce junior center excellence informační bezpečnosti



JUNIOR CENTRUM EXCELENCE
INFORMAČNÍ BEZPEČNOSTI®

Autor koncepce a držitel ochranné známky č.: 407198

Ing. Jiří Sedláček

sedlacek.jiri@email.cz

+420 602129224

1 Tabulka řízeného dokumentu

Koncepce junior center excellence informační bezpečnosti

ŘÍZENÝ DOKUMENT	
Název dokumentu	Koncepce junior center excellence informační bezpečnosti
Klasifikace / stupeň důvěrnosti	Veřejné, TLP:CLEAR
Zpracoval	Ing. Jiří Sedláček
Aktuální verze	29
Datum zpracování	9.10.2026
Periodicita revize	1x ročně / v případě potřeby významné změny či doplnění
Distribuce	www.jc3.cz , na vyžádání e-mailem

1.1 Historie revizí

Verze	Datum	Autor	Popis změny
1	13.11.2026	Ing. Jiří Sedláček	První návrh dokumentu
2-28	25.2.2019	Ing. Jiří Sedláček	Doplňování dokumentu s ohledem na vývoj vzdělávacího systému a s ohledem na získané zkušenosti s aplikací koncepce na SŠ
29	11.9.2026	Ing. Jiří Sedláček	Úprava titulní strany, vytvoření tabulky řízeného dokumentu včetně jejího doplnění, úprava titulního obrázku (obrázek AI), úprava úvodní kapitoly a obrázku IoW, uvedení do souladu s novou KB legislativou po transpozici NIS2.

JC3IB[®]

JUNIOR CENTRUM EXCELENCE INFORMAČNÍ BEZPEČNOSTI



2 Obsah

1	Tabulka řízeného dokumentu	1
1.1	Historie revizí.....	1
3	Preambule	5
4	Předmluva	6
5	Východiska aneb, jak to začalo... ..	8
6	Současnost.....	9
7	Principy.....	10
8	Organizace JC3IB	13
9	Vize, ambice, poslání JC3IB	14
10	Pro úspěch Koncepce je nezbytné zajistit	15
11	Popis procesu vybudování JC3IB v daném kraji	16
11.1	Určení vhodné SŠ – kandidáta na JC3IB	17
11.2	Školení kybernetické bezpečnosti pedagogů a vedení školy	17
11.3	Stanovení směrů rozvoje (strategie rozvoje školy)	18
11.4	Vypracování studie proveditelnosti	19
11.5	Vypracování projektové dokumentace	19
11.6	Realizace.....	19
11.7	Posouzení souladu s Konceptí a poskytnutí licence pro užívání označení JC3IB	20
12	Implementace IB/KB v daném JC3IB	20
12.1	Síťová infrastruktura.....	20
12.2	Zvýšení úrovně fyzické bezpečnosti školy	21
12.3	Výkonná serverová infrastruktura pro provozní prostředí školy	21
12.4	Modernizované a nové prostory	21
12.5	Modernizace zařízení pro zajištění kontinuity činností, vysoké úrovně dostupnosti a řešení havarijních situací	21
12.6	Nástroje na zajištění zvýšené úrovně kybernetické bezpečnosti v provozním prostředí školy	21
13	Vybudování CYLAB JC3IB	23
13.1	Výkonná serverová infrastruktura pro CYLAB.....	23
13.2	Technologie CYLAB CyberRange.....	23
13.3	Sdílení znalostí, zkušeností a konfigurací v prostředí laboratoře	24

14	Komunikace mezi JC3IB a zbytkem světa s využitím moderních videokonferenčních technologií.....	24
14.1	Komunikační infrastruktura (videokonferenční systém - VCF)	24
15	Sdílení znalostí a zkušeností mezi JC3IB.....	24
16	Stav JC3IB ke dni 9.10.2026.....	25
17	Použité zkratky	27
18	PŘÍLOHA Č. 1: ČASOVÁ OSA KANDIDÁTA NA JC3IB, SŠ IPF ČICHNOVA	28
18.1	Směry rozvoje kandidáta na JC3IB, SŠ IPF Čichnova	28
18.2	Možnosti kandidáta na JC3IB, SŠ IPF Čichnova	29
18.3	Efektivita projektu budování JC3IB na SŠ IPF Čichnova	29
18.4	CYLAB JC3IB	30
19	PŘÍLOHA Č. 2: KONCEPCE VÝUKY INFORMAČNÍ BEZPEČNOSTI NA VŠECH TYPECH SŠ V ČR.....	31
19.1	Jak zavést výuku IB/KB do všech SŠ.....	31
19.2	Level I. - Základ - KZ	31
19.3	Level II. - Střed - KICT.....	32
19.4	Level III. - Top - KJC3.....	32
19.5	Koncepce výuky IB - závěr	33
20	PŘÍLOHA Č. 3: PODPOROVATELÉ KONCEPCE	34
21	Příloha č. 4 Vzor licence JC3IB	35

3 Preamble

Dále uvedený text je materiálem, jehož cílem je:

- definovat poslání středoškolských junior center excellence informační bezpečnosti (dále „JC3IB“),
- definovat přístupy JC3IB k zavedení informační bezpečnosti v organizaci typu střední škola,
- definovat přístupy JC3IB k výuce informační bezpečnosti na středních školách,
- definovat postup, jak se stát JC3IB (od statutu kandidátské školy až po statut školy užívající označení JC3IB),
- definovat organizační strukturu JC3IB.

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 je uvažován jako optimální krajský model. Je rovněž nezbytné respektovat i neopominutelné ekonomické aspekty.

Excelentním centrem nemůže být každá střední škola.

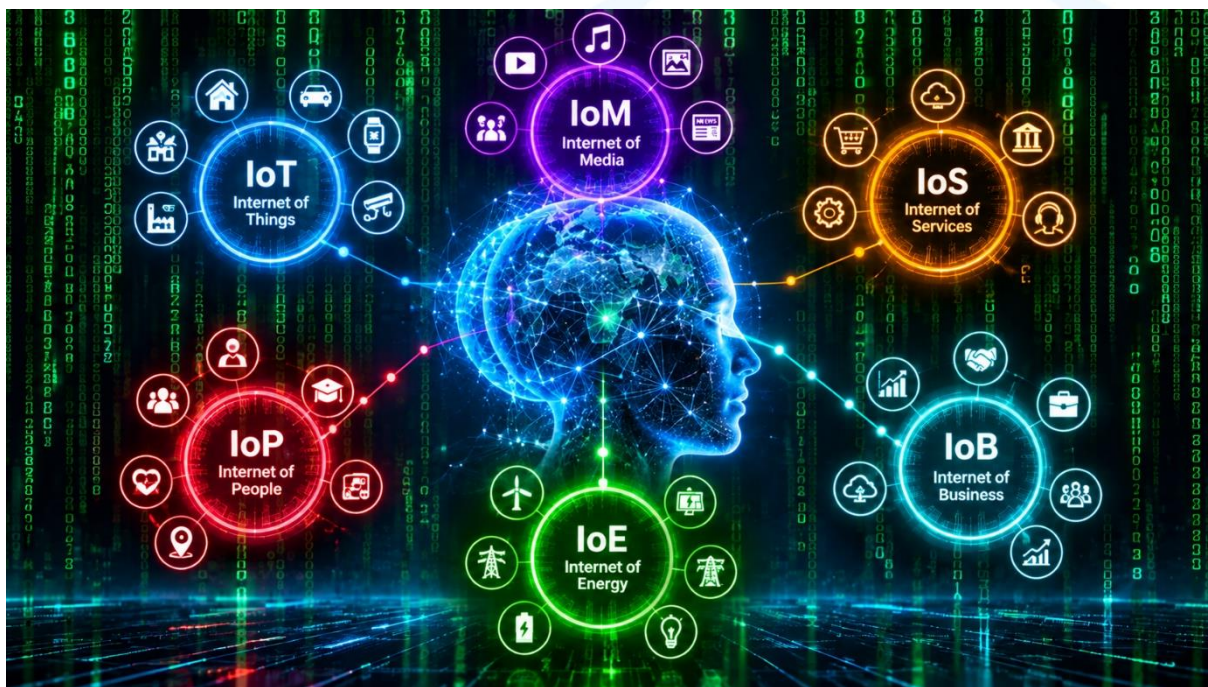
Každá střední škola ale může (právě i s pomocí excelentních center) vyučovat kvalitně a v dostatečné míře informační bezpečnost.

Každé JC3IB je startupem v rámci zajištění procesu rozvoje lidského kapitálu.

4 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 kyberválna, 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, řídicích systémů, průmyslových technologií, mohou být následky pro danou organizaci takového rozsahu, že řádově převyšují náklady na implementaci informační a kybernetické bezpečnosti. Pokud naše společnost nezmění přístup k této problematice, budou finanční ztráty narůstat. Základem pro změnu myšlení není nic jednoduššího než vzdělávání. Změna bezpečnostního povědomí a chování, která spadá pod bezpečnost lidských zdrojů, je naprosto klíčová. A to od řídicích struktur až po řádové zaměstnance.

Medializované kybernetické bezpečnostní incidenty 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 (ZoKB) a o změně souvisejících zákonů, ve znění pozdějších předpisů. To byl v naší legislativě významný milník, 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.

Od roku 2025 je díky transpozici evropské směrnice NIS2 opět novelizována kyberbezpečnostní legislativa ČR.

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.

5 Východiska aneb, jak to začalo...

◆ 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.“



Koncepci podporuje i NÚKIB

◆ Akční plán k NSKB na období let 2021 – 2025

Podpora Koncepce JC3IB viz část Kvalitní systém vzdělávání (strana 16), kód 92.

◆ 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.**

6 Současnost

Povinnost organizace typu SŠ chránit informace je stanovena jak zákony ČR, které jsou určujícími pro její činnost, tak i zákony upravujícími ochranu osobních údajů, osobnostní práva a zákony z oblasti trestní odpovědnosti. SŠ jsou také řízeny pokyny zřizovatele.

Dále je dobré také zmínit:

- Principy péče řádného hospodáře, včetně zajištění kontinuity činností.
- KAP krajů.

Školy musí plnit zákonnou povinnost - zajistit výuku studentů a současně musí chránit informace, a to nejen o studentech (zajištění důvěrnosti, integrity, dostupnosti informací a dat. Jsou povinny archivovat informace nezbytné k vystavení opisů studijních dokladů. Musí zajistit dostupnost relevantních informací z internetu (např. pro rodiče studentů). Musí chránit sebe sama před hrozbami z kybernetického prostoru.

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.

KB legislativa je velice dobře propracovaná, nicméně je závazná pouze pro tzv. „povinné osoby“. Pro organizace, které nejsou povinnými osobami z pohledu KB legislativy lze jako vodítka pro ochranu informací a zajištění kontinuity činností použít Minimální bezpečnostní standard NÚKIB (dále jen „MBS“) – viz použité zkratky níže. Zpracování osobních údajů podléhá od 25.5.2018 (účinnost) evropskému nařízení známému pod zkratkou GDPR.



7 Principy

Při budování JC3IB 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 JC3IB.

- **Analytický přístup**

Než jsou přijímána rozhodnutí, je nezbytné podrobit danou problematiku 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, efektivita**

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 JC3IB v rámci daného regionu v souladu s touto koncepcí, to vše je zárukou přenositelnosti takto vzniklého know-how, včetně zajištění vysoké efektivity, jako nezanedbatelného ekonomického hlediska.

- **Standardy/Kompatibilita**

Tak jako jsou jako norma přijaty v oblasti informační bezpečnosti standardy (např. normy řady ISO27k nebo metodika a doporučení bezpečnostních autorit členských států EU), stejně tak je nutné tento přístup aplikovat na zvolená technická opatření. Není vhodné stavět bezpečnostní opatření majoritně na technologických platformách nebo řešeních, které nemají garantovanou určitou míru podpory přímo od výrobce nebo důvěryhodného dodavatele. Takovými problematickými technologiemi jsou například řešení od krátce vzniklých Startupů nebo technologie OpenSource platform **bez existující dlouhodobější podpory výrobce takové platformy**, který nabízí i služby komerční podpory.

- **Soulad s praxí**

V laboratoři je kladen důraz na standardy – viz předchozí bod. Jedním z možných využití technologií laboratoře je i praktická aplikace organizačních a technických opatření ve fiktivní firmě. Technická opatření jsou pak aplikována dle vyhlášky o kybernetické bezpečnosti, na vyhlášce vyhovujících technologiích, či podle MBS. Tedy přesně tak, jako je tomu **v reálném světě**. Je to něco podobného, jako když škola produkuje své absolventy, specialisty na obrábění, **vyučuje v praktické výuce své žáky na moderních obráběcích strojích**. **Samozřejmě to lze aplikovat i tím způsobem, že žákům ukáží moderní obráběcí stroje na fotkách, videích, či v rámci exkurze a v dílnách jim pak rozdám ruční vrtačky a pilníky...** Jistě ale uznáte, že tato na první pohled levná metoda patrně **nezajistí vysoce kvalifikované odborníky**.

- **Udržitelnost**

Jak bylo řečeno výše, problematickými jsou například řešení od krátce vzniklých Startupů nebo technologie OpenSource platformem bez existující dlouhodobější podpory výrobce takové platformy, protože u těchto platform není možné předem předvídat a garantovat míru udržitelnosti. Z tohoto pohledu je nasazení takto definovaných platform vnímáno jako nesystémové řešení použitelné pouze pro testovací, simulační nebo vývojové účely, nikoli ale pro vzor implementace informační nebo kybernetické bezpečnosti v reálné organizaci s ohledem na skutečnost, že takové neměřitelné řešení může být z pohledu informační nebo kybernetické bezpečnosti samo hrozbou díky nemožnosti reagovat na nově objevivší se hrozby.

- **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.

Pro tuto Konceptci je uvažován **regionální princip**. V jednom regionu bude zřizovatel financovat/spolufinancovat vybudování laboratoře v jedné excelentní škole. Tato zvolená škola ale umožní sdílení „své“ laboratoře všem zájemcům ze středních škol z regionu (jak prezenčně, tak hlavně vzdáleně). **Laboratoř tedy bude využita v maximální možné míře, čímž bude zajištěno efektivní využití vložených finančních prostředků. Tento přístup povede v konečném důsledku k úspoře finančních prostředků v rámci regionu.**

Je efektivnější vybudovat jednu špičkovou laboratoř (jenž bude sdílena v rámci regionu), než vybudovat a zafinancovat (n) levnějších laboratoří ve školách, které budou v rámci regionu vyučovat IB/KB.

Jako vzor budování JC3IB lze v ČR, jak v oblasti přístupu k implementaci informační a kybernetické bezpečnosti v organizaci typu střední škola, stejně tak i v oblasti výuky a evangelizace této problematiky, brát kandidáty na JC3IB:

- Střední průmyslová škola a Střední odborná škola, Dvůr Králové nad Labem (<https://sposdk.cz/>)
- Střední průmyslová škola, Česká Lípa (<https://sps-cl.cz>)
- SOŠ INFORMATIKY A SPOJŮ A SOU KOLÍN (<https://soskolin.cz>)
- Střední škola informatiky, poštovníctví a finančnictví Brno (<https://www.cichnovabrno.cz/>)

Ucházet o licenci JC3IB se může i škola, která nebude zřizovatelem podpořena v otázce vybudování laboratoře. Takováto škola může plnit všechny ostatní principy Konceptce, s využitím laboratoře jiné školy, která dostala od zřizovatele přednost.

Mít vlastní laboratoř není podmínkou nutnou pro splnění principů a cílů této Konceptce a pro posouzení a následné případné propůjčení licence JC3IB.

8 Organizace JC3IB

Excelentní centra by měla spolupracovat s akademickou sférou. Kde to není možné, může být spolupráce navázána s Masarykovou univerzitou 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,
- propojení s gestorem v oblasti kybernetické bezpečnosti (NÚKIB),
- propojení se znalostní platformou v oblasti IB (NSMC).

Střední školy, které budou mít/mají ambici stát se JC3IB, jsou určovány ve spolupráci zřizovatelů s Asociací krajů (ať už se hlásí AK samy, nebo jsou ve spolupráci s AK určeny). Autor Koncepte definuje jejich poslání a kompetence, koordinuje jejich vzájemnou spolupráci a předávání zkušeností a podílí se na udržování a zvyšování jejich odbornosti, včetně posouzení souladu s Konceptí. Právě posouzení souladu s Konceptí bude jedním z efektivních nástrojů zajištění a udržení odborné úrovně/kvality JC3IB.

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

9 Vize, ambice, poslání JC3IB

- Středoškolská centra excellence 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 JC3IB:

- metodika implementace IB/KB a OOÚ v organizaci typu střední škola vycházejí z požadavků daných MŠMT, zřizovatelem, v rámci možností každé školy taktéž z MBS NÚKIB a GDPR,
- evangelizace a vzdělávání IB/KB jak pro žáky, tak i pro veřejnost,
 - semináře, workshopy,
 - uvědomovací akce,
 - konference,
 - videokonference,
 - kurzy, cvičení, školení, trénink,
- sdílení bezpečnostních technologií laboratoří JC3IB 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.
- posílení vazby a spolupráce s akademickou sférou

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

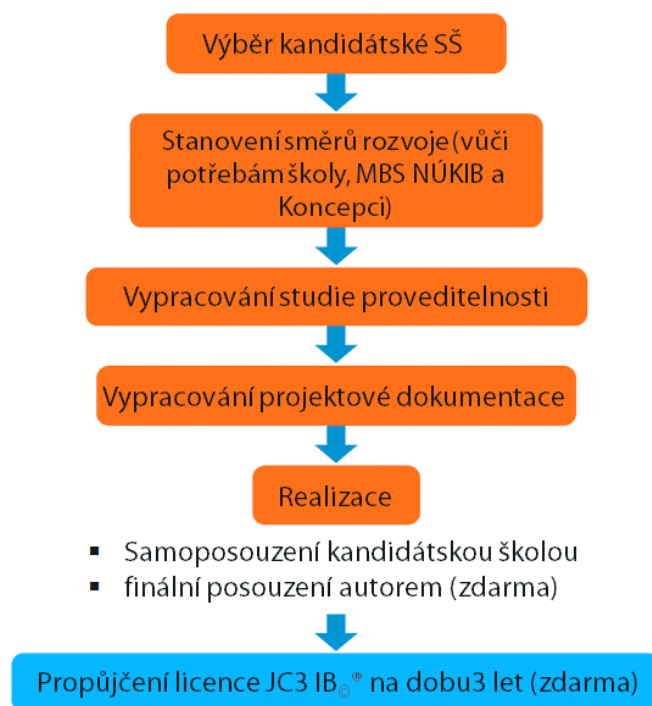
10 Pro úspěch Koncepce je nezbytné zajistit

- Záštitu národní autoritou v oblasti KB – NÚKIB (NÚKIB Koncepti JC3IB podporuje – viz AP k NSKB ČR na léta 2021-2025).
- Podporu vedení kandidátských škol a podporu zřizovatelů těchto škol.
- Vzdělané vedení kandidátských či již licencovaných škol a vzdělaný pedagogický sbor.
- Revitalizované/modernizované ICT excelentních center.
- Zavedený SŘBI u 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.



11 Popis procesu vybudování JC3IB v daném kraji



Jak je z obrázku zřejmé, proces vybudování JC3IB se děje postupnými kroky:

- Určení kandidáta na JC3IB.
- Školení vedení školy a pedagogického sboru včetně stanovení směrů rozvoje školy.
- (Volitelně vypracování Věcného záměru budování JC3IB.)
- Vypracování studie proveditelnosti.
- Vypracování projektové dokumentace.
- Realizace projektu.
- Posouzení souladu s Konceptí (soulad je oprávněn posoudit pouze autor této Koncepce).
- Propůjčení licence JC3IB na dobu tří let.

Každý jednotlivý krok procesu bude popsán dále.

11.1 Určení vhodné SŠ – kandidáta na JC3IB

Koncepce JC3IB je postavena na krajském modelu, kdy je nejen z finančních důvodů uvažována v každém kraji minimálně jedna excelentní střední škola, která bude schopna naplnit myšlenku (požadavky) JC3IB.

Tento model byl představen na zasedání Asociace krajů ČR, komise pro vzdělávání, dne 5.9.2019, v rámci prezentačního bloku NÚKIB, panem Jiřím Sedláčkem (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 JC3IB přihlásí zřizovateli sama.

11.2 Školení kybernetické bezpečnosti pedagogů a vedení školy

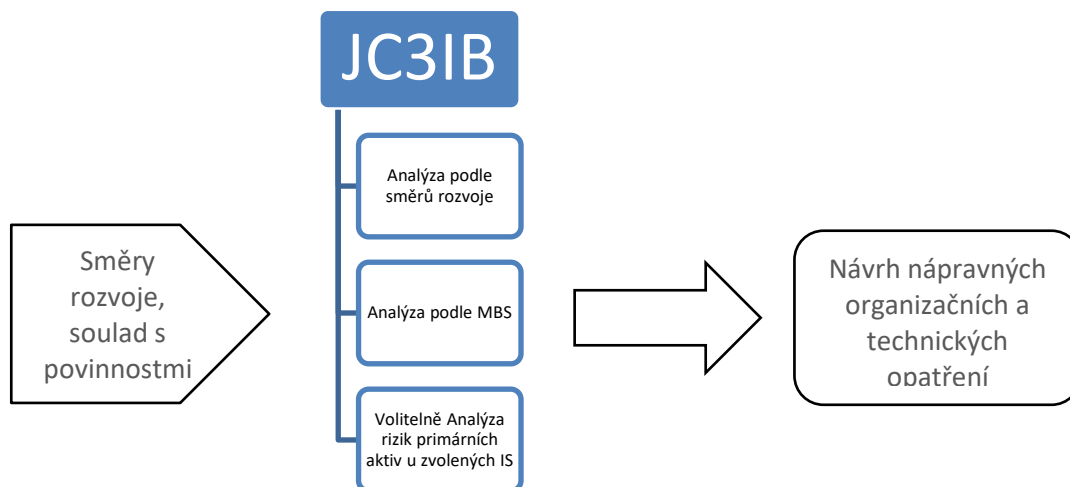
Vedení JC3IB a pedagogický sbor musejí být uvedeni do problematiky informační a kybernetické bezpečnosti. Důvodem je budování bezpečnostního povědomí a zavádění bezpečnostní kultury, na což je nutné brát zřetel v každé organizaci, zejména pak v excelentních centrech, která mají být vzorem pro ostatní SŠ. Bezpečnost lidských zdrojů je řešena jak ve standardu ISO/IEC 27001, tak i ve vyhlášce o kybernetické bezpečnosti a v MBS NÚKIB.

Takováto školení realizují v ČR různé organizace, včetně autora této Koncepce.

V případě realizace školení autorem budou posluchači seznámeni i s touto Koncepcí.

11.3 Stanovení směrů rozvoje (strategie rozvoje školy)

Stanovení směrů rozvoje školy je klíčové. Na základě toho si škola ujasní své přístupy

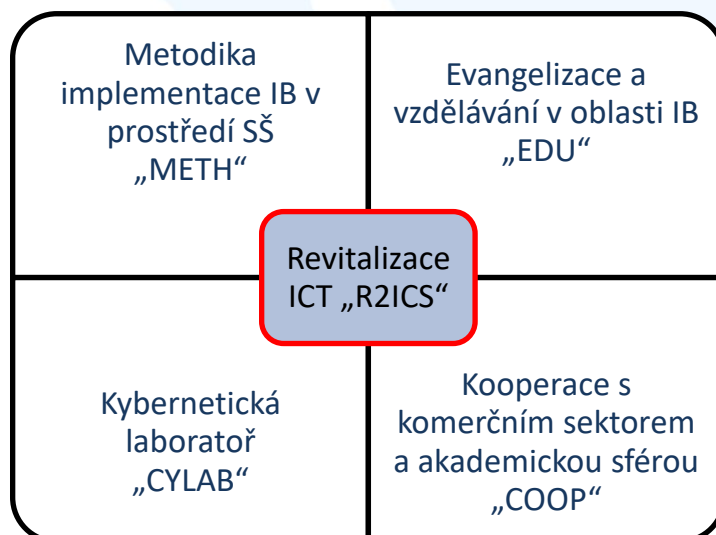


k implementaci informační bezpečnosti ve svém provozním prostředí, k výuce informační bezpečnosti a k její evangelizaci mimo školu, k vybudování laboratoře a ke spolupráci jak s ostatními JC3IB, kandidátskými školami a ostatními SŠ, ZŠ, VŠ a dalšími subjekty.

Pro stanovení směrů rozvoje je žádoucí zohlednit potřeby školy v oblasti ICT, požadavky Koncepce a požadavky MBS NÚKIB.

Klíčovými parametry pro směry rozvoje jsou:

- **R2ICS** – Ready to Information and Cyber Security – uvedení provozní ICT vrstvy školy do stavu, který jí umožní implementovat informační a kybernetickou 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 kandidátskými školami, JC3IB, akademickou sférou, komerčním sektorem, veřejnou správou 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 laboratoře prostřednictvím vzdáleného přístupu nejen mezi kandidátskými školami, JC3IB, ale i mimo ně v rámci regionu.

11.4 Vypracování studie proveditelnosti

Po stanovení směrů rozvoje má kandidát na JC3IB dostatek informací pro specifikaci poptávky na vypracování studie proveditelnosti.

Studie proveditelnosti řeší zejména:

- Požadavky na uvedení kandidátské školy do stavu dle specifikace R2ICS – viz směry rozvoje výše.
- Požadavky na realizaci organizačních a technických opatření pro provozní prostředí školy a technické vybavení CYLAB, v souladu s vytyčenými směry rozvoje.
- Realizují se tedy:
 - GAP analýza podle směrů rozvoje (potřeby školy, požadavky Koncepce).
 - GAP analýza podle Minimálního bezpečnostního standardu NÚKIB.

Studie proveditelnosti stanovuje požadavky dle R2ICS, požadavky na rozsah organizačních a technických opatření v provozním prostředí školy a požadavky na vybavení CYLAB, včetně stanovení hrubé cenové kalkulace (jsou možné i cenové varianty).

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

11.5 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, podkladem, pro realizaci projektu JC3IB.

11.6 Realizace

Na základě vypracované detailní projektové dokumentace je zadán požadavek na VŘ pro realizaci s následnou realizací díla.

Po realizaci se stále jedná o kandidátskou školu na propůjčení licence JC3IB.

11.7 Posouzení souladu s Konceptí a poskytnutí licence pro užívání označení JC3IB

Posouzení kandidáta na JC3IB je finálním krokem k propůjčení licence JC3IB na období tří let. V rámci posouzení bude zkoumáno 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 JC3IB v rámci regionu.

Metodiku posouzení kandidáta má k dispozici autor Koncepce, Jiří Sedláček, který na web stránkách www.jc3.cz zveřejní pomůcku/checklist k posouzení kandidáta. Na základě této pomůcky si budou moci kandidátské školy ujasnit, jestli jsou už na posouzení autorem Koncepce připraveny. Checklist pro posouzení je v současnosti pilotně ověřován na SŠ: Střední průmyslová škola a Střední odborná škola, Dvůr Králové nad Labem (<https://sposdk.cz/>).

Posouzení kandidáta na JC3IB je finálním krokem k propůjčení licence JC3IB a to na období tří let zdarma.

12 Implementace IB/KB v daném JC3IB

Z vytyčených směrů rozvoje kandidáta na JC3IB 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 činností, vysoké úrovně dostupnosti a řešení havarijních situací,
- nástroje na zajištění zvýšené úrovně kybernetické bezpečnosti.

Velice dobrým doplňkovým vodítkem je také např. materiál NÚKIB: BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY

<https://nukib.gov.cz/cs/infoservis/doporuceni/>

12.1 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 úrovně dostupnosti informací (dostupnost IS a KS, u kterých je to vyžadováno),
- 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.

12.2 Zvýšení úrovně fyzické bezpečnosti školy

- Zajištění fyzické bezpečnosti na úrovni perimetru školy,
- zajištění fyzické bezpečnosti prostor, v nichž jsou dostupné nosiče (papírové, elektronické) interních informací a informací s vyšším stupněm důvěrnosti,
- zajištění fyzické bezpečnosti prostor s provozními technologiemi školy,
- zajištění fyzické bezpečnosti režimových prostor včetně serverovny.

12.3 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.

12.4 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 technologie CYLAB,
- zajištění prostor pro komunikační videokonferenční systém.

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

- Zajištění zálohování dat metodou disk2disk2tape (D2D2T) s možností realizace offline záloh a archivace,
- zajištění zálohování důležitých technických aktiv stanovených IS 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 včetně jejich monitoringu.

12.6 Nástroje na zajištění zvýšené úrovně kybernetické bezpečnosti v provozním prostředí školy

- Zajištění segmentace sítě včetně oddělení provozního prostředí školy od internetu, CYLAB a technologických řídicích systémů,
- monitoring datových toků v síti,
- patch management,
- vulnerability management,
- zajištění řízení přístupu do sítě,

- zajištění skenu zranitelností,
- zajištění antivirových prostředků včetně EDR,
- zajištění log managementu,
- zajištění možnosti automatizovaného (logického) odpojení kompromitovaného zařízení od sítě.

Kandidátská škola SŠ IPF Čichnova, má nezanedbatelnou výhodu v napojení na KOC JMK (Security Operations Center – Kybernetické Operační Centrum zřizovatele). S tímto napojením získala SŠ IPF 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 jednotek MIO Kč.



13 Vybudování CYLAB JC3IB

13.1 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 (viz níže) k zajištění cvičebních bezpečnostních scénářů.

13.2 Technologie CYLAB CyberRange

CYLAB je určena zejména pro tyto činnosti:

- Seznámení se s moderními kyberbezpečnostními technologiemi běžně používanými v praxi,
- implementace kybernetické bezpečnosti ve fiktivní organizaci s aplikací organizačních a technických opatření, ať už podle platné legislativy kybernetické bezpečnosti, či podle MBS NÚKIB,
- forenzní vyšetřování,
- soutěže,
- cvičení,
- semináře,
- workshopy,
- vybudování JSOC (Junior SOC).
- ustavení JCSIRT týmu (Junior CSIRT).

CYLAB je určena nejen pro využití školou, v jejíchž prostorách jsou technologie instalovány, ale také pro ostatní střední školy v rámci daného regionu, a to ať už prezenčně, tak i vzdáleně.

Pokud má kandidát na JC3IB k dispozici laboratoř dle této Koncepce, bude v rámci posouzení posuzovatel posuzovat i záznamy o využití CYLAB jinými školami z regionu v souladu s požadavky této Koncepce.

V CYLAB je vhodné, mimo výše uvedené serverové, infrastrukturní a klientské části, uvažovat tyto technologie:

- Provozní monitoring,
- řízení přístupu do sítě,
- monitoring datových toků v síti,
- monitoring zranitelností,
- antivirové řešení s centrální správou včetně EDR,
- Log Management,
- SIEM.

13.3 Sdílení znalostí, zkušeností a konfigurací v prostředí laboratoře

U CYLAB je výhodou, pokud se povede zajistit kompatibilitu technických prostředků mezi JC3IB vzájemně z důvodu zajištění možnosti sdílení scénářů cvičení a konfigurací infrastruktur. Tím je usnadněno předávání know how mezi školami. To je ale bohužel limitováno nejen vývojem technologií v čase, ale i potenciálně odlišnými přístupy financování projektů v krajích a rovněž kvalitou zpracovaných studií proveditelnosti, které jsou realizovány na základě výběrových řízení, kdy autor není schopen garantovat soulad s Konceptí za zvolené zpracovatele studií.

14 Komunikace mezi JC3IB a zbytkem světa s využitím moderních videokonferenčních technologií

14.1 Komunikační infrastruktura (videokonferenční systém - VCF)

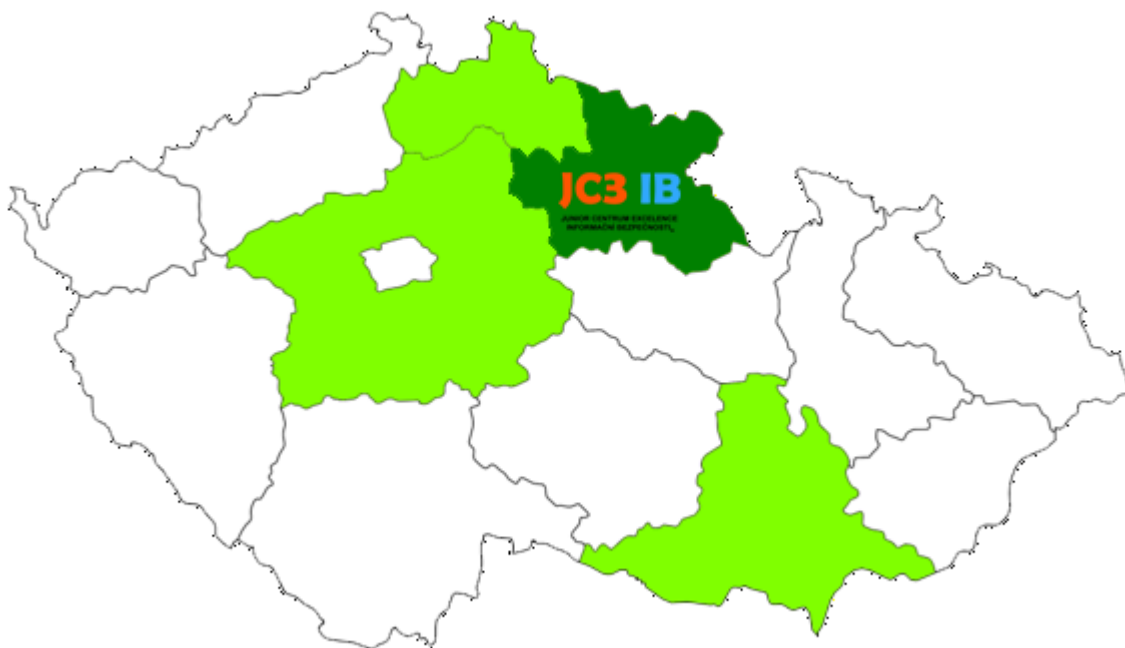
- zajištění kvalitní konektivity pro VCF,
- zajištění VCF sestavy kompatibilní se standardy,
 - HW zařízení,
 - protokoly H.323, SIP, platforma Lync,
 - možný počet spojení minimálně 1+3.

15 Sdílení znalostí a zkušeností mezi JC3IB

Pro sdílení znalostí, zkušeností a know how mezi JC3IB je nezbytné zajistit:

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

16 Stav JC3IB ke dni 9.10.2026



Legenda:

JC3IB – SŠ, v transformačním procesu.

JC3IB s udělenou licenci

Bílá místa identifikují regiony bez zvolených kandidátských škol.

Ve spolupráci s autorem Koncepce probíhá výuka IB/KB na těchto středních školách v ČR:

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

V transformačním procesu na JC3IB se nacházejí tyto školy:

- Střední průmyslová škola, Česká Lípa (<https://sps-cl.cz>).
- SOŠ INFORMATIKY A SPOJŮ A SOU KOLÍN (<https://soskolin.cz>).
- Střední škola informatiky, poštovníctví a finančnictví Brno (<https://www.cichnovabrno.cz/>).

Licenci JC3 IB mají uděleny tyto školy:

- Střední průmyslová škola a Střední odborná škola, Dvůr Králové nad Labem (<https://sposdk.cz/>).
 - Licence udělena 6.2.2026

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.

Ing. Jiří

Sedláček

Digitálně
podepsal Ing. Jiří
Sedláček

Datum:
2026.10.09
16:06:08 +02'00'



17 Použité zkratky

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CYLAB©	Kybernetická laboratoř
JCSIRT©	Junior Computer Security Incident Response Team
EDR	Endpoint Detection and Responce
IB	Informační bezpečnost
IS	Informační systém
JC3IB©®	Junior Centrum Excellence Informační Bezpečnosti
KB	Kybernetická bezpečnost
KICT	Kategorie ICT
KJC3	Kategorie Junior Centrum Excellence
KZ	Kategorie základní
MBS	Minimální bezpečnostní standard NÚKIB (https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/)
NSKB	Národní strategie kybernetické bezpečnosti
SŘBI	Systém řízení bezpečnosti informací
SOC	Security Operations Center
JSOC©	Junior Security Operations Center

PŘÍLOHY

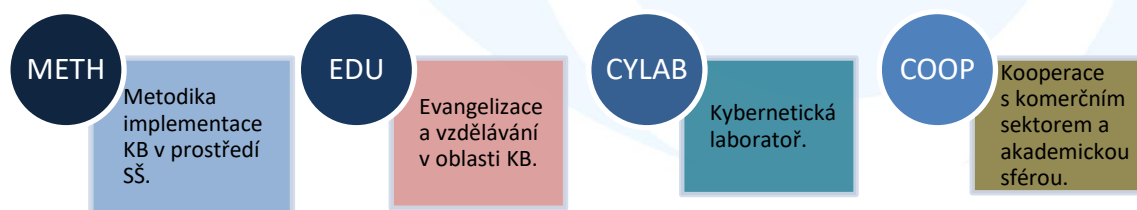
18 PŘÍLOHA Č. 1: ČASOVÁ OSA KANDIDÁTA NA JC3IB, SŠ IPF ČICHNOVA

Popis procesu



18.1 Směry rozvoje kandidáta na JC3IB, SŠ IPF Čichnova

Směry rozvoje na obrázku znázorněné vedou k cíli - k vybudování JC3IB.



18.2 Možnosti kandidáta na JC3IB, SŠ IPF Čichnova

SŠ IPF 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).

18.3 Efektivita projektu budování JC3IB na SŠ IPF Čichnova

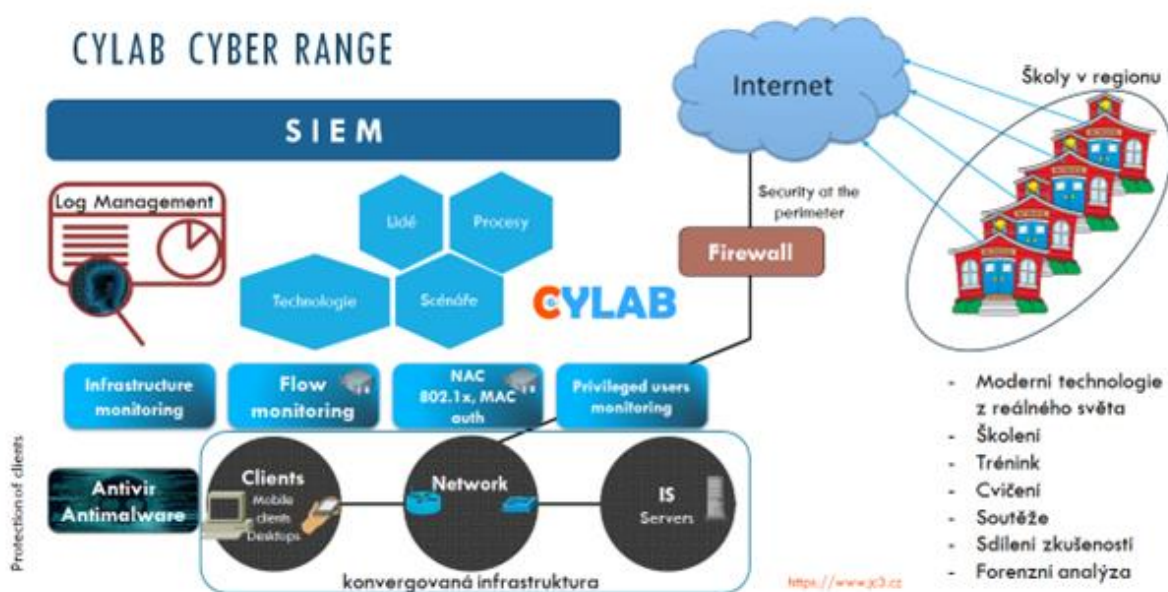
Efektivita projektu je zajištěna:

- 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 (výstavba CYLAB) budou technologie laboratoře školy vzdáleně zpřístupněny i ostatním SŠ v rámci JMK.
- Projekt budování JC3IB na SŠ IPF Čichnova je vzorem pro vznik JC3IB na krajské úrovni v ČR v souladu s touto Konceptí juniorních center excelence v oblasti informační bezpečnosti v ČR. Tato škola je vzorem pro:
 - Vybudování JC3IB na SŠ v ostatních krajích.
 - Aplikaci IB v prostředí SŠ.
 - Výuku IB/KB na SŠ pro všechny typy RVP, které to umožňují.
- Scénáře ve škole vytvořené budou k dispozici (v duchu této Koncepce) ostatním JC3IB. 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 JC3IB vzájemně.

- Vypracování této Koncepce nestálo daňové poplatníky ČR ani korunu.
- Po ukončení projektu JC3IB na jakékoli kandidátské škole budou minimalizovány možné případné budoucí sankce školy za (byť neúmyslné) porušení zákonných povinností při ochraně informací např. za porušení povinností správce z pohledu ochrany osobních údajů – GDPR.

18.4 CYLAB JC3IB



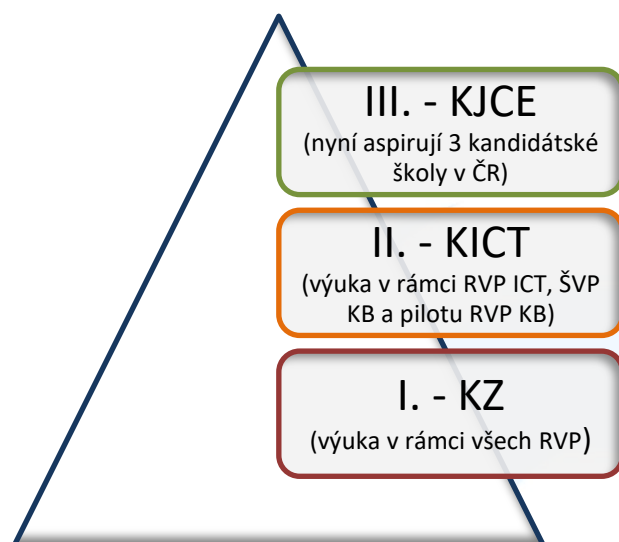
19 PŘÍLOHA Č. 2: KONCEPCE VÝUKY INFORMAČNÍ BEZPEČNOSTI NA VŠECH TYPECH SŠ v ČR

Ambicí autora Koncepce 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.**

19.1 Jak zavést výuku IB/KB do všech SŠ

V rámci analýzy provedené autorem této Koncepce byly identifikovány 3 typy vzdělávacích programů IB pro SŠ v ČR:

- I. **Kategorie základní (KZ).**
- II. **Kategorie ICT (KICT).**
- III. **Kategorie JC3IB (KJC3).**



19.2 Level I. - Základ - KZ

Je uvažována výuka pro všechny typy RVP, tedy pro:

- RVP, které s ICT nesouvisí.
- RVP 18-20-M/01 Informační technologie.
 - ŠVP Kybernetická bezpečnost.
- RVP 37-42-M/01 Logistické a finanční služby.
 - ŠVP Bezpečnost dat.

Tato kategorie pokryje výuku IB/KB na všech školách, které nejsou více na tuto problematiku zaměřeny (specializovány) a dále na školách, které již vyučují ŠVP KB a bezpečnost dat, případně RVP KB v pilotním ověřování.

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.

19.3 Level II. - Střed - KICT

Je uvažována výuka pro:

- ŠVP KB.
- ŠVP Bezpečnost dat.
- Případně RVP KB v pilotním ověřování.

Tato kategorie pokryje výuku IB/KB na všech školách, které již vyučují ŠVP KB a Bezpečnost dat, případně RVP KB v pilotním ověřování.

Informační a kybernetická bezpečnost je vyučována 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. (technická opatření u právnických osob nepodléhajících KB legislativě).

19.4 Level III. - Top - KJ3

Je uvažována výuka pro:

- ŠVP KB.
- ŠVP Bezpečnost dat.
- Případně RVP KB v pilotním ověřování.

Tato kategorie pokryje výuku IB/KB na všech školách, které již vyučují ŠVP KB a Bezpečnost dat, případně RVP KB v pilotním ověřování.

Informační a kybernetická bezpečnost je vyučována 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 KJC3 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.

19.5 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 autor Koncepce 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 podaný projekt (předložen ve spolupráci s kandidátem na JC3IB SŠ IPF Čichnova) nebyl schválen.**

20 PŘÍLOHA Č. 3: PODPOROVATELÉ KONCEPCE

Koncepci podporují:

- Network Security Monitoring Cluster (<https://www.nsmcluster.com>)
- Masarykova univerzita Brno (<https://www.muni.cz>)
- Národní centrum kompetence pro kyberbezpečnost (<https://nc3.cz>)
- Cyber Security Hub CZ (<https://www.cybersecurityhub.cz>)
- Národní klastrová asociace (<https://nca.cz/>)



21 Příloha č. 4 Vzor licence JC3IB

