Recenzovaný článek

Analýza a model systému přípravy odborníků kybernetické obrany

Analysis and model of Cyber security corps professional development

Petr Františ, Jan Hodický

Abstrakt: Článek se zabývá problematikou přípravy odborníků v oblasti kybernetické bezpečnosti. V úvodu jsou popsány jednotlivé prvky, které působí v oblasti kybernetické bezpečnosti. Dále je provedena strategická analýza popisující východiska v oblasti vzdělávání. Stěžejní část práce je věnována návrhu systému vzdělávání. V práci jsou definovány jednotlivé prvky a je vytvořen model vztahů těchto prvků. V příloze je uveden kompletní výčet témat a jejich rozčlenění dle úrovní znalostí pro specialistu kybernetické bezpečnosti.

Abstract: The paper deals with the professional development of cyber security corps. In the introduction the individual elements that are active in cyber security are described. Strategic analysis of the education is carried out to define the initial state. The main part of the paper is devoted to the design of the education system. The individual elements are defined in the paper, and the model of relationships between these elements is shaped. The attachment contains complete set of topics and their classification into the strands to fulfil the profile of the cyber security expert.

Klíčová slova: Kybernetická bezpečnost; modelování; vzdělávání.

Key words: Cyber defense; Modelling; Education.

ÚVOD

Vize AČR je v oblasti kybernetické obrany teprve v procesu přípravy. Ze své podstaty bude vycházet z dokumentu „Koncepce výstavby AČR 2025“[1]. Tento dokument definuje základní východiska a předpokládaný stav AČR v roce 2025. Oblast kybernetické bezpečnosti je zmíněna v následujících souvislostech:

„Armáda ČR bude mít, v součinnosti s orgány odpovědnými za kybernetickou bezpečnost a obranu, schopnosti plánování a řízení operací v kybernetickém prostoru a schopnost vytvářet související krizové plány.“

Kybernetická obrana a kybernetická bezpečnost je dle Národní strategie kybernetické bezpečnosti pro období let 2015 – 2020, definovány následovně[2]:

- Kybernetická obrana, kterou má v gesci Vojenské zpravodajství, je samostatnou oblastí širšího konceptu kybernetické bezpečnosti a zároveň oblastí širšího konceptu zajištění obrany státu. Jejím úkolem je v případě potřeby aktivně působit v kybernetickém prostoru proti útočníkům. Specifikem kybernetické obrany je skutečnost, že bude prováděna jak v případě vyhlášení mimořádných stavů, především formou součinnosti s ostatními složkami zajišťujícími obranu ČR, tak i nepřetržitě mimo tyto stavy.
- Kybernetickou bezpečnost má v České republice v gesci Národní úřad pro kybernetickou a informační bezpečnost. Jeho úkolem je neustálé navyšování bezpečnosti a odolnosti informační a komunikační infrastruktury. Kybernetickou bezpečností se tedy rozumí souhrn prostředků směřujících k zajištění ochrany kybernetického prostoru. Tyto prostředky mohou být různého charakteru – právní, organizační, vzdělávací, technické a další [3].

V kontextu systému vzdělávání termín kybernetická obrana, jehož ekvivalent je v NATO termín Cyber Defense, zahrnuje pasivní prostředky kybernetické bezpečnosti (Cyber Security) a aktivní prostředky obrany[4].

Členství České republiky v Severoatlantické alianci významně ovlivňuje výchovně vzdělávací proces. Podstatou procesu obraného plánování NATO je identifikace a tvorba potřebného rámce schopností k vedení předpokládaných operací krizového řízení v souladu s politicko-vojenskými ambicemi. Tyto požadavky na schopnosti, které NATO definuje a požaduje po jednotlivých členských státech, jsou v souladu s plánovacím procesem v NATO upřesňovány každé čtyři roky.

---

1 Ministerstvo obrany. Koncepce výstavby Armády České Republiky 2025. Praha : Ministerstvo obrany, 2018.

2 Národní centrum kybernetické bezpečnosti (2015a): Národní strategie kybernetické bezpečnosti. Dostupné z: https://www.databaze-strategie.cz/cz/cr/strategie/narodni-strategie-kyberneticke-bezpecnosti-cr-na-obdobi-let-2015-az-2020?typ=struktura.

3 Riethofová, Mgr. Alžběta. Informační servis. www.moccr.army.cz. [Online] 6. 8 2018. http://www.mocr.army.cz/informacni-servis/zpravodajstvi/narodnicentrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/.

4 Feix, Miroslav a Procházka, Dalibor. Aktuální úkoly kybernetické obrany rezortu Ministerstva obrany. Vojenské rozhledy. 2017, Sv. 3.

Oblasti kybernetické obrany se týká schopnost E 6202 N: CYBER DEFENCE, kde v části 3 je uveden požadavek: „Vzdělávání, výcvik a dovednosti v oblasti kybernetické bezpečnosti".

Základní reakcí na tento požadavek je vytvoření a akreditování studijního programu Kybernetická bezpečnost na Univerzitě obrany, který pokrývá především oblast technických specializací. I když obsahuje část tzv. měkkých dovedností (soft skills), tak majoritně je zaměřen na aplikaci bezpečnosti v prostředí informačních technologií, tedy potřeby AČR – AKIS (CIRC). V předmětové skladbě lze nalézt předměty, jako jsou Analýza informačních zdrojů, Vývoj a nasazen malware, Botnetové sítě, které pokrývají část potřeb VZ NCKO.

Výhoda tohoto studijního programu je jeho ucelený průběh – 5 let nepřetržitého studia, tedy nedochází ke zbytečné ztrátě času zpracováním a obhajobou bakalářské práce a navazujících státních zkoušek. Rovněž tak časové schéma průběhu studia poskytuje dostatek času na odborné praxe, které v posledních dvou letech studia mohou probíhat již na pracovišti, kde bude student po skončení studia zařazen.

Vytvořením a úspěšnou akreditací tohoto studijního programu Univerzita obrany položila dobrý základ ke vzdělání specialistů v oblasti kybernetické obrany pro rezort MO.

1 CÍLE A STANOVENÉ OKRUHY PROBLÉMŮ

Hlavním cílem tohoto článku je navrhnout systém vysokoškolského vzdělávání problematiky kybernetické obrany v resortu MO. Samotná existence akreditovaného programu ovšem ještě nevytváří ucelený systém přípravy odborníků kybernetické obrany. Pro dosažení stanoveného cíle článku byly stanoveny následující výzkumné otázky/ oblasti problému.

Jací vnitřní a vnější aktéři ovlivňují problematiku přípravy personálu v resortu MO v oblasti kybernetické obrany?

Jaké jsou vzájemné vazby definovaných aktérů kybernetické obrany v kontextu přípravy personálu resortu MO?

Jaká témata musí být součástí systému přípravy personálu resortu MO v oblasti kybernetické obrany?

2 METODY A DATA

Pro nalezení odpovědí na otázky stanovené v kapitole 2 byla použita analýza činnosti a působnosti jednotlivých aktérů v oblasti vzdělávání problematiky kybernetické obrany. Pro definování východiska stávajícího stavu vzdělávání byla použita strategická analýza, ale pouze její část, která rozkrývá vnitřní a vnější aktéry a definuje příležitosti a hrozby spojené s vnějším okolím vzdělávání. Následně bylo použito modelování na systémové

úrovni[5], které popsalo vazby mezi jednotlivými složkami systému vzdělávání. Grafická reprezentace modelu vazeb mezi složkami vzdělávacího systému byla vytvořena v podobě mentální mapy[6]. Participativní metoda panelu expertů, složeného z 35. účastníků kurzu Generálního štábu (KGŠ) 2018-2019, byla použita pro stanovení výčtu témat a jejich členění do dílčích úrovní znalostí a směrů pro přípravu odborníků specializace kybernetické bezpečnosti. Tyto informace jsou obsaženy v příloze článku. KGŠ byl zvolen z důvodu strategického dopadu nové domény.

3 AKTÉŘI V OBLASTI VZDĚLÁVÁNÍ PROBLEMATIKY KYBERNETICKÉ OBRANY

Tato kapitola popisuje významné složky státu působící v oblasti kybernetické obrany a jejich vztah ke vzdělávání odborníků v této oblasti. Jedná se o složky, které mají vztah k rezortu MO a zasahují do vzdělávání specialistů v oblasti kybernetické obrany.

3.1 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Národní úřad pro kybernetickou a informační bezpečnost je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) [7]. I když tento úřad není součásti resortu MO, tak významně ovlivňuje a formuje požadavky na vzdělávání v oblasti kybernetické obrany.

3.2 Národní centrum kybernetických operací (NCKO)

Národní centrum kybernetických operací je součást Vojenského zpravodajství. Bylo ustanoveno na základě Akčního plánu k Národní strategii kybernetické bezpečnosti pro

5 Frevert, R., Haase, J., Roland, J., Knöchel, U., Schwarz, P., Kakerow, R., Mohsen R. (2005). System Level Modeling. Modelling and Simulation for RF System Design. 10.1007/0-387-27585-1_4.

6 Eppler, M. J. (2006). A Comparison between Concept Maps, Mind Maps, Conceptual Diagrams, and Visual Metaphors as Complementary Tools for Knowledge Construction and Sharing. Information Visualization, 5(3), 202–210. https://doi.org/10.1057/palgrave.ivs.9500131.

7 NÚKIB. Úvod. Národní úřad pro kybernetickou a informační bezpečnost. [Online] 2018. [Citace: 24. 10 2018.] https://www.govcert.cz/.

období let 2015 – 2020. Jeho úkolem je vytvoření účinného systému obrany v kybernetickém prostoru tak, aby Česká republika byla schopna zastavit a případně odvrátit kybernetické útoky, a tím zabezpečit ochranu civilního obyvatelstva a infrastruktury [8]. Národní centrum kybernetických operací vypracovalo Strategii kybernetické obrany ČR 2018 – 2022, která obsahuje nastavení právního rámce, vybodovaní a rozvoj infrastruktury a schopnosti obrany v kyberprostoru.

3.3 Centrum Computer Incident Response Capability (CIRC)

Centrum CIRC je organizačním prvkem Agentury komunikačních a informačních systémů (AKIS) a prvkem kybernetické bezpečnosti s působností pokrývající celý resort MO. Úkolem Centra CIRC je proaktivní identifikace bezpečnostních hrozeb a incidentů pomocí nepřetržitého monitoringu důležitých segmentů datových sítí resortu MO, a jejich následná analýza, vyhodnocování a reportování relevantním partnerům [9]. Mezi další úkoly centra CIRC patří šíření bezpečnostního povědomí mezi uživateli a správci informačních a komunikačních systémů.

3.4 Odbor bezpečnosti Ministerstva obrany

Odbor bezpečnosti Ministerstva obrany odpovídá za plnění úkolů stanovených zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. Odpovídá za nastavení systému řízení bezpečnosti informací včetně kontroly jeho dodržování, ochrany určených neutajovaných informací a kybernetické bezpečnosti v rezortu Ministerstva obrany. Včele odboru bezpečnosti stojí Bezpečnostní ředitel Ministerstva obrany. Bezpečnostní ředitel, kromě jiných povinností, zastává funkci předsedy Rady pro kybernetickou obranu Ministerstva obrany [10].

3.5 Sekce rozvoje sil MO

Sekce rozvoje sil Ministerstva obrany odpovídá za koncepční činnosti a za odborné a metodické řízení výstavby a rozvoje pozemních sil, vzdušných sil, schopností Armády

8 NCKO. Kybernetická obrana. Vojenské zpravodajství. [Online] 2018. [Citace: 24. 10 2018.] https://vzcr.cz/kyberneticka-obrana-46.

9 7. CIRC. O nás. Centrum CIRC. [Online] 2009. [Citace: 24. 10 2018.] http://www.circ.army.cz/onas.

10 Ministerstvo obrany. Organizační řád Ministerstva obrany. [Dokument] Praha : autor neznámý, 2018.

České republiky v kybernetickém prostoru, vojensko-civilní spolupráce (CIMIC – Civil-Military Cooperation), psychologických operací (působení) v místě nasazení (PsyOps – Psychological Operations) a záchranné a výsadkové služby Armády České republiky. Odpovídá za koncepční činnosti a za odborné a metodické řízení systému velení a řízení, za stanovování zásad a norem v oblasti společné přípravy pozemních sil a vzdušných sil, záchranné a výsadkové služby, služby pátrání a záchrany v Armádě České republiky. Koordinuje proces udržení a rozvoje schopností Armády České republiky. Dále odpovídá za zpracování Doktríny Armády České republiky. Zajišťuje plnění úkolů služebního orgánu odpovědného za vojenské odbornosti v odborné gesci ředitele sekce rozvoje sil Ministerstva obrany je zodpovědná za obsah programů přípravy schopností Armády České republiky v kybernetickém prostoru[11].

3.6 Velitelství kybernetických sil a informačních operací

Velitelství kybernetických sil a informačních operací vzniklo dne 1. ledna 2018. Vytvoření tohoto velitelství symbolizuje, že Armáda České republiky zařadila kybernetickou doménu na taktický stupeň velení a dále počítá s jejím plným rozvinutím o podřízené prvky. Mezi jeho základní úkoly patří velení a řízení podřízených útvarů kybernetických sil a informačních operací, plánování a řízení působení v kybernetickém prostoru, plánování a řízení informačních operací [12].

4 STRATEGICKÁ ANALÝZA VZDĚLÁVÁNÍ V OBLASTI KYBERNETICKÉ OBRANY

V této kapitole je provedena strategická analýza problematiky vzdělávání v oblasti kybernetické obrany v rezortu Ministerstva obrany. Výsledky strategické analýzy slouží pro popis stávajícího stavu přípravy odborníků a k vymezení vnitřního a vnějšího okolí dané problematiky. Celkově strategická analýza přispívá ke stanovení východisek pro návrh jednotlivých částí systému přípravy, nebylo tedy s ní dále pracováno ve smyslu návrhu strategie, nebo úpravy již existujících strategií vzdělávání odborníků kybernetické obrany.

4.1 Silné stránky vzdělávání v kybernetické bezpečnosti

- Akreditovaný studijní program „Kybernetická bezpečnost na UO“

11 SRS MO.Sekce rozvoje sil MO. [Online] 2018. [Citace: 24. 10 2018.] http://www.acr.army.cz/struktura/generalni/rozvoj/sekce-rozvoje-sil-mo-142358/.

12 9. Feix, Miroslav. Působnost VeKiS. Praha: GŠ AČR, 2018.

- Vznik Velitelství kybernetických sil a informačních operací
- Postoj Vlády České republiky ke kybernetické bezpečnosti vyjádřen v dokumentu: „Národní strategie kybernetické bezpečnosti České republiky na období let 2015-2020“
- Umístění NÚKIB, NCKO, CIRC, VeKySIO ve stejném městě

4.2 Slabé stránky vzdělávání v kybernetické bezpečnosti

- Personální nenaplněnost,
- Objekt centra NCKO byl nedávno dokončen, ale nezačal ještě pracovat v novém místě
- VelKysIO formálně vzniklo, ale není personálně dostatečně naplněno (až k 1.7),
- Nejsou zpracované všechny potřebné dokumenty (vize a strategie kybernetické obrany AČR)
- Kvalifikovaný personál odchází i se znalostmi do civilní sféry,
- Není spolupráce v oblasti vzdělávání a předávání znalostí mezi všemi složkami.

4.3 Příležitosti vzdělávání v kybernetické bezpečnosti

- NÚKIB je umístěn ve stejném městě v docházkové vzdálenosti od UO, VelKysIO a NCKO
- Blízkost Masarykovy univerzity a jejího kybernetického polygonu
- Brno je studentské město a centrum technologických firem působících v oblasti IT
- Oblast Kybernetické obrany je akcentována za strany vlády a existuje široká podpora, výzkumných projektů a záměrů v této oblasti.

4.4 Hrozby vzdělávání v kybernetické bezpečnosti

- Ztráta důvěry státní správy ve schopnosti složek Ministerstva obrany kvalifikovaně působit v oblasti kybernetické obrany
- Kompromitace schopností zásadním kybernetickým útokem na infrastrukturu Ministerstva obrany a jejích složek
- Lobbing civilních vzdělávacích institucí proti schopnostem vzdělávat odborníky v oblasti kybernetické obrany uvnitř rezortu Ministerstva obrany za účelem získání státních prostředků pro jejich vlastní financování

4.5 Analýza vnitřního prostředí

Z hlediska vnitřního prostředí jsou poměrně jasně definovány silné stránky. Základem je postoj Vlády České republiky, která schválením strategických dokumentů umožnila vznik důležitých center v rámci vládních úřadů a bezpečnostních složek, které se zabývají problematickou kybernetické bezpečnosti a obrany. Tento postoj se promítl i do AČR, která zareagovala vytvořením příslušných složek a změnou kompetencí a struktury již existujících složek. Z hlediska vzdělávání zareagovala Univerzita obrany vytvořením nového studijního programu „Kybernetická bezpečnost". Z pohledu slabých stránek je nejpalčivějším problémem personální situace. Je to zejména nedostatečný přísun vzdělaného personálu, odchod kvalifikovaného personálu a chybějící spolupráce mezi složkami. Zejména odchod kvalifikovaného personálu je velkým problémem. Řešení na jeho zmírnění je v kompetenci resortu MO a jeho personální a finanční politiky, tedy principiálně mu nelze zabránit, ale lze alespoň zmírnit jeho následky tím, že zabráníme odlivu znalostí spolu s odlivem personálu. Důležité je vytvořit zpětnou vazbu pro uložení znalostí, které jsou ukryté v kvalifikovaném personálu a vrátit je nazpět do vzdělávacího systému.

Dalším problémem je malé sdílení schopností a informací mezi hlavními složkami státu v oblasti kybernetické obrany- Výměna informací probíhá převážně na manažersko-strategické úrovni. Z hlediska legislativy není možné sdílení na úrovni operačně taktické, ale bylo by vhodné vytvořit lepší podmínky pro sdílení znalostí a kapacit na úrovni vzdělávací a umožnit tak větší propojení těchto složek do vzdělávacího systému.

4.6 Analýza vnějšího prostředí

Velkou roli v oblasti příležitostí hraje geografická lokace všech zásadních institucí působících v oblasti kybernetické obrany. Umístění těchto složek v městě Brně je výrazně pozitivním prvkem pro jejich vzájemnou integraci a provázanost. Zároveň pozice města Brna jako centra vysokých škol a firem působících v IT (technologický park) a Univerzity obrany vytváří vhodné podmínky pro nábor odborného personálu. Geograficky umístění v centru Moravy a díky dobrému spojení a kapacitě infrastruktury je Brno vhodným městem pro denní dojíždění za prací z moravských měst a vesnic. To vše by mělo pozitivně ovlivnit dobrou personální situaci a propojení vzdělávání a výměnu informací. Z hlediska hrozeb se jako nejvážnější jeví zkompromitování systému vzdělávání na základě vnějšího kybernetického útoku na nějakou část státní infrastruktury, který by mohlo vést ke zkratkovité interpretaci v médiích jako selhání systému přípravy dostatečně kvalifikovaných odborníků. To by mohlo vyústit k necitlivému zásahu do systému vzdělávání na základě politických rozhodnutí. Zbylé hrozby jsou spíše minoritní.

5 NÁVRH SYSTÉMU VZDĚLÁVÁNÍ ODBORNÍKŮ KYBERNETICKÉ OBRANY

Tato kapitola je stěžejní po obsahové stránce a popisuje vertikální a horizontální členění navrženého systému vzdělávání a dále obsahuje model vazeb aktérů v tomto systému.

Na základě panelu expertů, složeného z účastníků kurzu Generálního štábu 2018-2019, je doporučeno jednotlivá témata rozdělit do čtyř úrovní a z pohledu odbornosti do dvou směrů:

- Technicky zaměřená témata
- Manažersky zaměřená témata

Do základní úrovně lze zařadit témata, která by měla být součástí magisterského stupně vzdělávání, např.:

- Analýza paměti
- Senzorové sítě
- Operační systémy

První úroveň má charakter specializace. Zahrnuje témata, která rozšiřují základní IT vzdělání a mohou nebo nemusí být i součástí specializovaného magisterského studijního programu, např:

- Základní informace o malware
- Získávání dat z otevřených zdrojů
- Krizová zákon

Druhá úroveň obsahuje více specializovaná témata týkající se převážně kybernetické bezpečnosti (defensivní schopnosti), např.:

- Regulace v kyberprostoru
- Nakládání s daty jako důkazním materiálem
- Data pro řešení incidentu

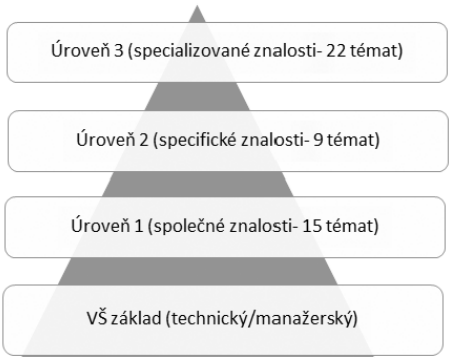
Témata třetí úrovně se týkají ofensivních schopností a vysoce specializovaných znalostí a dovedností, např.:

- Kyberšikana, kyberstalking
- Vývoj vlastních exploitů
- Vývoj nástrojů pro zahlazení identit

Kompletní výčet témat a jejich rozčlenění dle úrovní výstupních znalostí a specializačních směrů je uveden v příloze článku.

5.1 Vertikální členění systému vzdělávání

Úrovně jednotlivých témat přirozeně určují vertikální skladbu vzdělávání. Spodní úroveň je tvořena základním magisterským vzděláním a postupně jsou na tuto spodní úroveň přidávány jednotlivé vrstvy, které jsou tvořeny specializovanými kurzy. Z každé vrstvy odchází specialisté, kteří dosáhli dané úrovně dostatečné pro svoje specializované místo a pracoviště. Tedy množství lidí se v jednotlivých úrovních zmenšuje, viz obrázek 1.



Obrázek č. 1: Vertikální členění systému vzdělávání

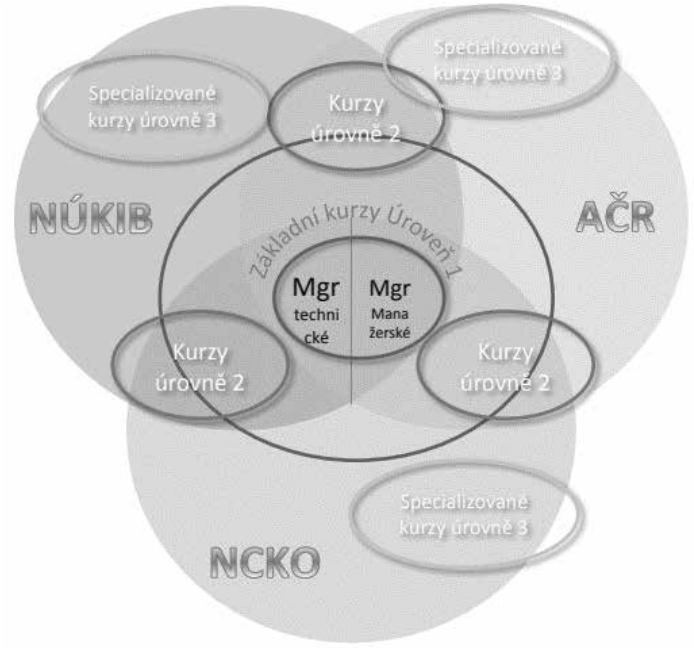
Kurzy první a druhé úrovně by měli být přizpůsobeny tak, aby se jejich absolventi rozdělili a získali potřebné znalosti a dovednosti v následujících směrech:

- bezpečnostní testování.
- správa sítě
- forenzní zkoumání
- vývoj a analýza software
- manažer kybernetické bezpečnosti
- odborník na kybernetické politiky (Cyber policies)

Kurzy třetí úrovně jsou již úzce specializované a spojené s odborností daného pracoviště, na kterém absolventi působí.

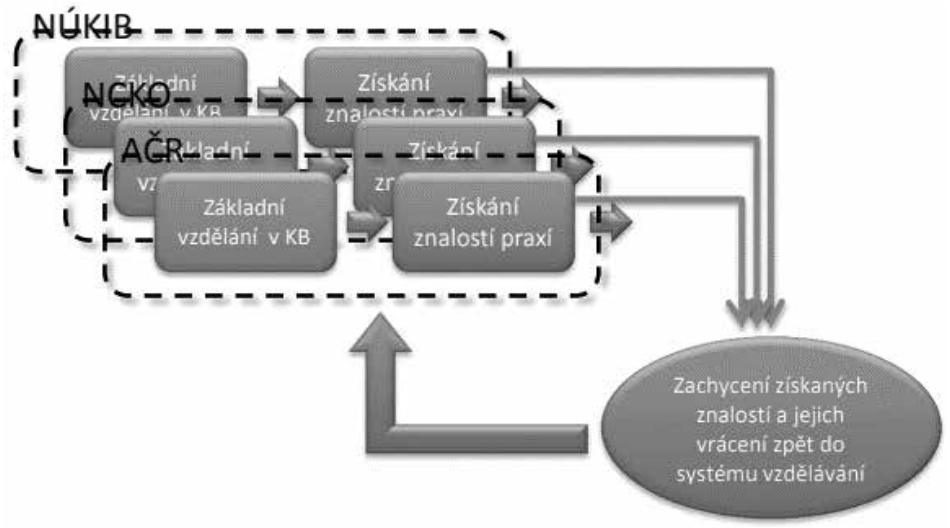
5.2 Horizontální členění systému vzdělávání

Na témata kybernetické obrany lez nahlížet také z hlediska jejich odborné příslušnosti k jednotlivým složkám působící v prostředí kybernetické obrany. Tím lze získat pohled charakterizující co je pro jednotlivé složky společné a co jedinečné, viz obrázek 2.



Obrázek č. 2: Horizontální členění systému vzdělávání

Z uvedeného schématu je vidět, jakým způsobem jednotlivé kurzy pokrývají společné potřeby znalostí a dovedností. Při pohledu na toto schéma z hlediska znalostí lze rozpoznat, že jeho všechny části tvoří uzavřený ekosystém. Tento ekosystém je tvořen všemi potřebnými znalostmi a dovednostmi. Únik těchto znalostí a dovedností je způsoben odchodem kvalifikovaného personálu. Pro udržení znalostí a dovedností uvnitř ekosystému je nutné pracovat se systémem zpětných vazeb. Důvody využití těchto zpětných vazeb a úniku znalostí byly popsány v kapitole zabývající se analýzou vnitřních slabých stránek systému vzdělávání. Implementace tohoto modelu do navrženého ekosystému je znázorněna na obrázku č. 3.

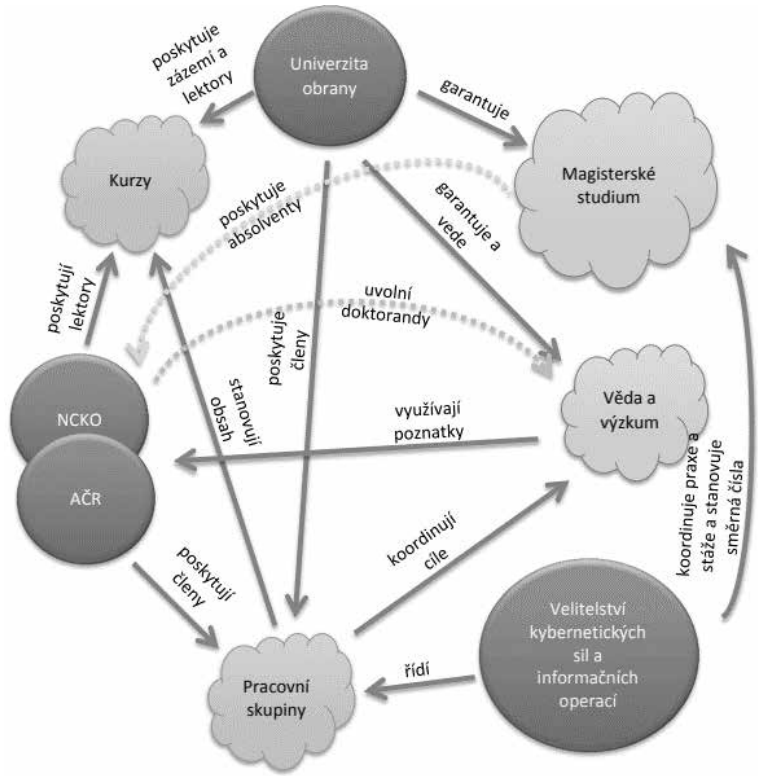


Obrázek č. 3: Zpětná vazba v ekosystému vzdělávání

5.3 Model vztahů prvků systému vzdělávání

Aby navrhovaný systém vzdělání mohl úspěšně fungovat, musí být navržen i model spolupráce mezi jednotlivými složkami. Model spolupráce vychází ze stanovených rolí jednotlivých složek a představuje základní prvek pro udržení navrženého ekosystému v chodu. Dobře fungující spolupráce přispívá jednak k pružnému generování odborně vzdělaného personálu, který je v rovnováze s přirozeným odchodem, ale taktéž k efektivnímu vzdělávání zaměstnanců, kteří se nemusí dovzdělávat praxí, ale jsou již dopředu připraveni na pozici, kde nastupují nebo na kterou se posunují při vývoji své kariéry. Rovněž tak řízení kariér odborných zaměstnanců je pružnější a efektivnější.

Obrázek č. 4 popisuje jednotlivé aktéry a prvky systému vzdělávání odborníku kybernetické obrany a jejich vzájemné vazby.



Obrázek č. 4: Model vztahů prvků systému vzdělávání

ZÁVĚR

Hlavním cíle tohoto článku bylo navrhnout systém přípravy v oblasti kybernetické bezpečnosti v podmínkách rezortu Ministerstva obrany. Stanovené otázky / okruhy problémů v kapitole 2 byly pokryty provedenou analýzou aktérů v kybernetické doméně a provedenou strategickou analýzou pro definování východisek pro navrhovaný systém vzdělávání. V neposlední řadě byl také vytvořený realizovatelný systém přípravy odborníku kybernetické bezpečnosti, který je postaven na konkrétních existujících, nebo právě vytvářených prvcích tohoto systému spolu s definovanými vazbami mezi těmito prvky.

Návrh systémů přípravy vychází z obecně platných principů, respektuje současnou legislativní situaci a je založen na modelu spolupráce, kdy nejsou upřednostňována krátkodobá řešení. Investice jednotlivých složek do implementace tohoto systému vzdělávání může nastartovat vzdělávací ekosystém, který po úspěšném startu pomůže zachovat a prohlubovat míru znalostí a pružně generovat vzdělané odborníky dle potřeby jednotlivých složek. Významným způsobem umožní zkrátit dobu zaškolování jednotlivých pracovníků na systemizované místo a zabrání nenávratnému odlivu znalostí mimo systém.

PŘÍLOHA

Členění témat kybernetické bezpečnosti a jejich profilace v navrženém vertikálním členění systému vzdělávání spolu s identifikací témat, která mohou být obsahem karierových kurzů KVD a KGŠ.

Tato tabulka je souhrnnou informací výsledků panelu expertů účastníků KGŠ.

Tématický blok	Téma	Základní	Úroveň 1	Úroveň 2	Úroveň 3	KVD	KGŠ
1 TECHNICKÉ/ PRAKTICKÉ							
1.1 FORENZNÍ ANALÝZA	Nakládání s daty a HW způsobem, který je „forensically sound“, tzn. způsobem v souladu s právem (vyfotit, nerozbít, logovat, atd.).		X				
	Získání dat pro analýzu (např. obraz paměti, obraz disku). Analýza disku, činností uživatele (historie prohlížečů, manipulace s USB zařízeními, instalované a spouštěné aplikace a dokumenty, atd.), systémových logů, síťová komunikace (potkává se s analýzou síťového provozu).	X					
	Analýza paměti (spouštěné procesy, jejich chování – potkává se s analýzou malware). Přehled používaných nástrojů.	X					
1.2 ANALÝZA MALWARE	Základní informace o malware jako nejběžnější způsoby zajištění persistence, typický modus operandi běžných malware kampaní apod		X			X	
	Znalost základních metod analýzy malware (analýza skriptů ve webových stránkách, dokumentů, dynamická a základní statická analýza PE a ELF) a nástrojů dostupných pro tento účel		X				
	Možné pokračování je pokročilá analýza a reverzní inženýrství.		X				
1.4 ICS/SCADA	Seznámení se světem průmyslových systémů. Odlišnosti od prostředí běžných počítačů.				X		
	Základy elektrotechniky. Úvod do problematiky senzorových sítí, inteligentních sítí („smart grid“), IoT, zabezpečovacích systémů, automatizační techniky. Programování průmyslových systémů.	X					
1.5 OSINT + THREAT INTELLIGENCE	Získávání dat z otevřených zdrojů, analýza a získávání nových poznatků z těchto dat.		X			X	
	Využití dostupných dat při řešení incidentu (mapování neobjevených částí infrastruktury útočníka např. pomocí WHOIS, společného hostingu, způsobu generování doménových jmen).			X			
1.6 INCIDENT HANDLING	Problematika zpracování incidentů jako základní služba CERT týmu. Proces řešení incidentu, klasifikace incidentů, metodika zpracování, spolupráce s dalšími bezpečnostními týmy.			X			X
	Problematika předávání dat, jejich ochrana (např. TLP protokol)			X			

	Podpůrné nástroje pro zpracování incidentů a komunikaci (tiketovací systémy, PGP, X.509), automatizované zpracování strojově generovaných informací (pro identifikaci incidentů)			X			
1.7 SPRÁVA SYSTÉMŮ – WINDOWS, UNIX/ LINUX, (OS X?)	Pro řešení incidentů je nutná znalost běžných operačních systémů a toho, jak fungují. Je nutné vědět co, jakým způsobem a kam systém loguje (platí i pro běžně používané aplikace).	X					
	Pro identifikaci a analýzu malware je nutné umět odlišit anomální chování systému (např. nestandardní procesy, umístění souborů, správa služeb a modulů, linkování knihoven)	X					
1.8 MONITORING A ANALÝZA SÍŤOVÉHO PROVOZU	Zdroje dat pro analýzu – zachytávání paketů, toků, honeypoty, systémy IDS a IPS, atd.	X					
	Nástroje a způsoby sběru, agregace a vizualizace dat. Problematika firewallů (paketové filtry, stavové, aplikační FW) a dalších síťových prvků. Metody analýzy dat. Zaměření nejen na L7 v ISO/OSI modelu, ale i L2, L3 a L4.	X					
1.9 PRÁVO PRO CERT	Zákon o kybernetické bezpečnosti, související vyhlášky a další relevantní zákony, vyhlášky, nařízení apod. Základy mezinárodního práva pro potřeby CERT.	X					
	Nakládání s osobními údaji, které mohou být přítomné v datech					X	
	Základní povědomí o práci PČR v oblasti kybernetické kriminality a o mechanismu trestního řízení	X				X	
	Nakládání a práce s daty tak, aby později mohla být využita jako důkazní materiál. Legal Issues			X		X	
1.10 SOFT SKILLS	Netechnické dovednosti, které jsou ale důležité pro úspěšné působení v CERT týmu	X					
	Prezentační a vyjadřovací schopnosti – kontakt s constituency a reprezentace týmu na konferencích. Jazykové dovednosti – angličtina a čeština a schopnost psát smysluplné texty gramaticky správně	X					
1.11 ZÁKLADNÍ INFO	Co je to CERT, jak funguje. Spolupráce, TI, TF-CSIRT, FIRST, CSIRT Network. RFC 2350	X					
1.12 DALŠÍ	Programování, skriptování, databáze, kryptografie a další předměty (např. většina z BIT na FI MU) by měly sloužit jako základy pro tyhle	X					
2 NETECHNICKÉ / MANAŽERSKÉ							
2.1 ZÁKLADNÍ DIGITÁLNÍ HYGIENA	Základní bezpečnostní doporučení, bezpečné používání ICT technologií	X				X	
	Fyzická bezpečnost, bezpečnost hardware, bezpečnost software, zálohování dat, služby (e-mail, internetové bankovnictví.)	X				X	
	Soukromé vs pracovní využívání ICT	X				X	
	Politika hesel, autentizace	X				X	
	Ochrana soukromí a sdílení osobních údajů	X				X	

	Využívání sociálních sítí, bezpečné prohlížení webu	X				X	
	Bezpečná komunikace vs veřejná wifi, šifrování	X				X	
	Sociální inženýrství	X				X	
	Kyberšikana, kyberstalking, kybergrooming				X		
	Přehled nejčastějších hrozeb/útoků na uživatele – phishing, malware/ransomware	X				X	
2.2 NÁRODNÍ STRATEGIE A POLITIKY	Odborná terminologie – počínaje definicí kyberprostoru atd.	X					
	Koncept zajišťování KB v ČR – kybernetická bezpečnost versus kybernetická obrana versus kybernetická kriminalita, role státu	X					X
	Kybernetická bezpečnostní politika, význam KB ve vztahu ke státu, strategicko-právní rámec	X					X
	Představení relevantních subjektů (NCKB/govcert.cz), zpravodajské služby (NCKS), PČR, Národní CERT a další	X				X	
	Role CSIRT/CERT týmů		X				
2.3 PRÁVO A MEZINÁRODNÍ ORGANIZACE	Zákon o kybernetické bezpečnosti	X					
	Kontrola a audit			X			
	Krizový zákon, vyhláška 315/2014 a 316/2014, další legislativní normy ČR		X				X
	Mezinárodní spolupráce při zajišťování KB – bilaterální, multilaterální (NATO, EU, OBSE, OSN)			X			X
	Právo a kyberprostor, mezinárodní právo, problém atribuce						X
	Regulace v kyberprostoru, směrnice NIS				X		
2.4 KONTEXTUÁLNÍ A ANALYTICKÉ SCHOPNOSTI	Historické aspekty KB, geneze kybernetických hrozeb		X			X	
	Taxonomie útoků	X					
	Kyberkriminalita, kybernetický terorismus, kybernetická špionáž, kybernetický konflikt/válka					X	
	Základní typologie a motivace útočníků					X	
	Znalost a používání základních OSINT nástrojů – vyhledávání z otevřených zdrojů					X	
2.5 VZDĚLÁVÁNÍ A CVIČENÍ KYBERNETICKÉ BEZPEČNOSTI	Typologie cvičení - technické/table-top/komunikační, národní/mezinárodní		X			X	

	Organizace a plánování cvičení				X	X	
	Tvorba scénářů cvičení, reflexe aktuálních trendů a jejich překlopení do scénářů				X		X
	Způsob/formy vzdělávání a prevence v oblasti kybernetické bezpečnosti dle definovaných cílových skupin		X				X
2.6 KRITICKÁ INFORMAČNÍ INFRASTRUKTURA	Informační a komunikační systémy, významné informační systémy	X					
	Struktura klíčových informačních/komunikačních služeb	X					
	Bezpečnostní politiky	X					
	Systémy řízení bezpečnosti informací	X				X	
	Řízení kontinuity činností				X		
	Analýza rizik				**X**		
2.7 OSTATNÍ	Manažerské dovednosti				X	X	
	Motivace a vedení lidí			X			X
	Projektové řízení			X			X
3 SPECIFICKÉ / OFENZIVNÍ	Real-time schopnosti zajišťovat (aktivní) kybernetickou obranu		X				
	Aktivní identifikace a rekognoskace nepřítele v kyberprostoru		X			X	
	Schopnost provádět odvetné útoky (hacking/ striking-back)				X		
	Sběr informací o zájmových aktérech			X			
	Data mining a analýza dat ze sociálních sítí, analýza obsahu			X			
	Analýza malware, reverzní inženýrství				X		
	Znalost jednotlivých fází kybernetických útoků (reconnaissance, scanning, gaining access, maintaining access, covering tracks…)		X			X	
	Schopnosti identifikace útoku, včetně Advanced Persistent Threat (APT) a následná analýza		X				
	Zvládnutí základních technik kybernetické bezpečnosti, blokace a izolace útočníka		X				
	Účinné zabezpečení vlastních sítí, systémů a informací (tj. neustálé hledání zranitelností ve svých sítích a systémech – pen testing, detekce anomálií v sítích, data analysis, šifrovací nástroje + provádění cvičení, kontingenční plány, apod.)		X				

4.1 SPECIFICKÉ SCHOPNOSTI A VZDĚLÁVÁNÍ PRO POTŘEBY STÁTU/ Monitoring zranitelností	Nacházení zranitelností (bez dalšího sdílení), nákup zero-day				X		
	Zvládnutí standardních nástrojů pro exploitaci				X		
	Vývoj vlastních exploitů, exploit-kitů				X		
	Vývoj vlastního malware, botnetů				X		
	Vývoj honeytokenů a beaconing systémů				X		
	Neustálý monitoring a rozvíjení možných vektorů útoku (jak HW, tak SW)				X		
	Tvorba nástrojů pro zahlazení identit a digitálních stop, anonymní pohyb na síti				X		
	Tvorba a monitoring honeypotů / honeynetů se zájmovými informacemi				X		
	Vytváření a budování fiktivních identit na sociálních sítích a dalších fórech (counter-intelligence)				X		
	DoS / DDoS				X		
	Modifikace / přesměrování síťového provozu, provádění MITM útoků				X		
	Spear phishing a další techniky sociálního inženýrství				X		
	Vývoj a nasazení malware				X		
	Příprava, vývoj a nasazení honeytokenů, popřípadě beaconing systém				X		
	Zapojení se do botnetových sítí				X		
	o Převzetí kontroly nad botnetem a možnost plošného odstranění malware z nakažených počítačů				X		
	o Celé spektrum: passive observation – infiltration – manipulation – takeover – takedown – elimination				X		
	Použití / příprava vlastního botnetu				X		
	Hack-back / strike-back				X		
	Nasazení vlastních sond			X			
4. VOJENSKÉ A SPECIFICKÉ PRO STÁTNÍ SLUŽBU	Zásady plánování výcviku, formy, metody a prostředky přípravy příslušníků AČR	X				X	
	Právní předpisy upravující službu v AČR	X					

	Základní interní normativní akty pro výkon služby VZP	X					
	Právo ozbrojeného konfliktu	X				X	
	Zásady ochrany utajovaných informací v prostředí státu, AČR a NATO	X					
	Seznámit se s organizační strukturou resortu MO a AČR, s organizací NATO	X					
	Specializované znalosti v oborových předmětech z oblasti komunikačních a informačních systémů s důrazem na zabezpečení provozu KIS ozbrojených sil a silových složek	X					
	Principy činnosti, funkci, zásady konstrukce a použití komunikačních a informačních systémů AČR a vybraných systémů spojenců	X					
	Základní principy otevřené architektury KIS a kybernetické obrany v prostředí AČR	X					
	Metody, formy a prostředky diagnostiky a hodnocení spolehlivosti vojenských KIS	X					
	Systémy plánování a řízení komunikačních a informačních systémů	X				X	
	Základní software používaný v AČR a zásady jeho licenční politiky s analýzou jeho zabezpečení	X					
	Zásady budování komunikačního systému TAKOM v AČR a požadavky na informační zabezpečení na taktickém stupni velení	X				X	
	Možnosti a využití software v rámci IS VŘ a BVIS, systém IS a jeho zabezpečení	X					
	Členění míst velení, zásady budování a přemísťování spojovacích uzlů míst velení	X				X	
	Rádiové, radioreléové a ostatní komunikační systémy, telefonní ústředny a kabelové soupravy ve výzbroji AČR	X				X	
	Bezpečnost a ochranu informací v míru i v krizových situacích	X					
	Zajišťovat efektivní, hospodárnou a účelnou podporu při využívání KIS v ozbrojených silách	X				X	
	Znát stacionární, mobilní i nasaditelné prostředky KIS zabezpečující komunikační a informační podporu v podmínkách integrovaného informačního prostředí (NEC)	X					
	Využívat a řídit prvky mobilních komunikačních a informačních systémů AČR a kritické informační infrastruktury státu s důrazem na zabezpečení přenosu informací	X				X	
	Znát organizaci, provoz a údržbu KIS používaných na taktické úrovni	X				X	
	Navrhovat a provádět základní správu sítí LAN v rámci IS provozovaných v AČR	X					
	Znát způsob zabezpečení a oddělení tajné domény v GDS a IS VŘ	X					

	Znát a rozumět propojení systému FMN v rámci taktického nasazení i v době míru, propojení do zabezpečených sítí NATO a propojení veřejné a tajné domény. Způsob zabezpečení, oddělení, přenosu informací a způsob použití.	X					
	Znát kritickou infrastrukturu GDS pro potřeby státu, systém zabezpečení datových skladišť a jejich využití	X					X
	Znát způsoby požití speciálních technických prostředků pro ochranu informací a spojovacích soustav	X					X
	Znát procesy certifikace a akreditace KIS pro přenos utajovaných informací	X					
	Rozvoj morálních vlastností jako vlastenectví, služba vlasti, smysl pro povinnost a splnění úkolu.	X					

Authors: ***Pplk. gšt. doc. Ing. Petr František, Ph.D.,*** *narozen v roce 1976. Je absolventem Vojenské akademie v Brně (2001), kde dále absolvoval doktorské studium (2004). Od roku 2003 působí jako odborný asistent na Vojenské akademii a později Univerzitě obrany. V současné době zastává funkci zástupce vedoucího Katedry informatiky, kybernetické bezpečnosti a robotiky. Zabývá se problematikou modelování a simulace, architektury výpočetních systémů a kybernetické bezpečnosti.*

Plk. gšt. doc. Ing. Jan Hodický, Ph.D., *narozen v roce 1977. Je absolventem Vojenské akademie v Brně. V roce 2004 získal doktorát v oblasti Informatiky a výpočetní techniky na Univerzitě obrany v Brně. Do roku 2012 působil jako odborný asistent na katedře Komunikačních a informačních systémů. Poté nastoupil na pozici vedoucího odboru Doktrín, vzdělávání a výcviku na Centru excelence modelování a simulace v Římě. Od roku 2017 do roku 2018 pracoval jako vedoucí vědecký pracovník na Centru bezpečnostních a vojenskostrategických studií na Univerzitě obrany v Brně. V roce 2019 se stal vedoucím Katedry letecké techniky na UO v Brně. Zabývá se problematikou aplikování modelování a simulace do vojenství.*

How to cite: FRANTIŠ, Petr and Jan HODICKÝ. Analýza a model systému přípravy odborníků kybernetické obrany. *Vojenské rozhledy*. 2019, 28 (3), 097-116. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz