Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

DIPLOMOVÁ PRÁCE

2017 **Monika Sulanová**

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra systémové analýzy

Strategie pro rozvoj vzdělávání v oblasti bezpečnosti ICT na vysokých školách

Vypracovala: Bc. Monika Sulanová

Vedoucí práce: Prof. Ing. Petr Doucek, CSc.

duben 2017

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně. Veškeré použité podklady, ze kterých jsem čerpala informace, jsou uvedeny v seznamu použité literatury a citovány v textu.

V..... dne .... Podpis: .....

Poděkování

Ráda bych poděkovala panu Prof. Ing. Petru Douckovi, CSc., za jeho vstřícný přístup a za rady a připomínky z jeho dlouholeté praxe v oblasti vzdělávání ICT odborníků, které jsou pro tuto práci obrovským přínosem. Jeho snahou je přizpůsobovat studium oboru současným trendům, čímž velmi dobře připravuje své studenty na budoucí praxi. Jeho práce si velice vážím a považuji ho za jednoho z nejlepších odborníků v oblasti ICT bezpečnosti v České republice, od kterého jsem měla tu čest se při mém studiu, nejen v problematice ICT bezpečnosti, něco naučit.

Abstrakt

Diplomová práce se zabývá problematikou vzdělávání odborníků v bezpečnosti ICT na vysokých školách s cílem navrhnout strategii pro rozvoj vzdělávání v současných studijních oborech, které se této problematice věnují. Teoretická část práce se zaměřuje na vymezení bezpečnosti ICT a na seznámení čtenáře se základními pojmy z oblasti řízení bezpečnosti informací a řízení kybernetické bezpečnosti. K tomu podává přehled o celkovém vývoji bezpečnosti ICT a o současných trendech v této oblasti. Dále popisuje současnou situaci na pracovním trhu ve vztahu k bezpečnosti ICT a situaci vzdělávání odborníků pro tuto oblast. K tomu charakterizuje existující doporučení pro vzdělávání v bezpečnosti ICT.

Praktická část se zaměřuje na analýzu současného vzdělávání v oblasti bezpečnosti ICT a na analýzu požadavků pracovního trhu na znalosti a dovednosti pracovníků v této oblasti. Definuje základní profesní roli a znalostní domény, které by tato role měla pokrýt. V analytické části jsou hodnoceny profily absolventů současných magisterských studijních oborů s cílem nalézt mezery ve znalostní bázi těchto absolventů, která byla stanovena na základě požadavků trhu práce a existujících doporučení. Výsledky analytické části jsou vstupem pro definování strategie v oblasti vzdělávání v bezpečnosti ICT, která dává základní doporučení, jak eliminovat zjištěné nedostatky.

Klíčová slova

bezpečnost ICT, řízení bezpečnosti informací, kybernetická bezpečnost, vzdělávání, multidisciplinarita

Abstract

The thesis deals with the problems of education in ICT security experts at universities in order to design a strategy for the development of education in present degree courses that dealing with this issue. The theoretical part focuses on the definition of ICT security and to familiarize the reader with the basic concepts of information security management and management of cyber security and gives an overview of the overall development of ICT security and the current trends in this area. It also describes the current situation on the labor market in relation to ICT security and the education of professionals in this field and characterizes the existing recommendations for education in ICT security.

Practical part focuses on analyzing the current education ic ICT security and on analyzing the knowledge and skills requirements of the labor market to professionals in this area. Defines the basic professional role and knowledge domains that should be covered by this role. In the analytical part they are evaluated current profiles of graduates Master's degree programs focused on this area in order to find gaps in the knowledge base of graduates based on the requirements of the labor market and the existing recommendations. The results of the analysis are input to define a strategy on education in ICT security, which gives basic recommendations on how to eliminate the shortcomings.

Keywords

ICT security, information security management, cybersecurity, education, multidisciplinary

Obsah

1. Úvod

Společně s vlnou digitalizace, nabývá bezpečnost ICT v posledních letech na významu, a také v následujících letech lze předpokládat v souvislosti s pokračováním digitální revoluce nárůst významu této oblasti. Nové technologie přináší stále sofistikovanější a doposud neznámé hrozby, na které je nezbytné rychle reagovat. Vzniká spletitá komunikační síť různých zařízení, která se stále více rozpíná a stává se poněkud nepřehlednou. K tomu přispívá také současný trend internetu věcí, jenž generuje obrovské množství dat v různých datových strukturách. S připojením nespočetně mnoha koncových zařízení, jejichž počet je společností Gartner k roku 2020 odhadován na 21 biliónů, vzniká markantní množství dat s vysokou hodnotou, kdy zajištění jejich dostatečné ochrany se stává být významnou úlohou (1).

Digitalizace sebou nese i jiné konsekvence. Naše komunikace ohledně každodenního života, práce a vztahů, se v dnešní době odehrává převážně v digitalizovaném prostředí, které mnohdy nemá nastavena žádná pravidla a kontrolní procesy. Ohroženy nejsou pouze velké organizace, ale i běžní uživatelé, jejich identita, soukromí, majetek, práce, vztahy a v krajních případech také životy. Tyto hrozby zvýšily potřebu ochrany běžných uživatelů v digitálním prostředí. V souvislosti s tím se upravuje právní rámec tak, aby byly co možná nejvíce eliminovány hrozby, které mohou ohrozit bezpečnost uživatelů, přičemž stěžejním tématem od konce roku 2015 je ochrana soukromí uživatelů a na to navazující nařízení Evropské unie označované jako General Data Protection Regulation[1], tzv. GDPR (2).

Na významu nabývá také bezpečnost na úrovni jednotlivých států a krizové řízení. Vznikají pojmy jako kybernetická válka a kyberterorismus. Roku 2014 byl vydán zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů[2] a příslušná prováděcí vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti zaměřující se na ochranu kritické informační a komunikační infrastruktury státu a významné informační

[1] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) (2).

[2] V praxi je zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) často označován jako ZKB (3). Tato zkratka byla zvolena i pro použití v této práci.

systémy[3] (3,4). Cílem právního rámce je zamezit narušení kritické infrastruktury, které by mohlo vést k ohrožení státu, jeho obyvatel a také k významným dopadům na ekonomiku státu.

Tímto vznikají nové požadavky na znalosti a dovednosti ICT odborníků. Počet absolventů v technických oborech dlouhodobě klesá, a to navzdory snahám vysokých škol přilákat studenty do nových studijních programů a oborů. Dalším problémem je nedostatečná kvalita absolventů a nepřipravenost na řešení problémů v praxi, což je v poslední době často zmiňováno ze strany zaměstnavatelů. Jestliže nedojde k bodu zvratu, může být nedostatek odborníků v oblasti bezpečnosti ICT za několik let naprosto kritický, a to na celosvětové úrovni. Tento problém by měl být aktuálně řešen s velkou důležitostí a na jeho řešení by se měla podílet, jak soukromá, tak státní a akademická sféra. Společné diskuze mohou přinést kvalitnější náměty k řešení, jejichž realizace může být za předpokladu sdílení zdrojů a „know how" rychlejší a efektivnější.

Předpokladem pro nalezení řešení je společná diskuze, sdílení informací a námětů k řešení a sdílení zdrojů pro realizaci, ideálně na celosvětové úrovni. Vysoké školy jsou z tohoto pohledu významnými institucemi, které by mohly být jedním z hlavních iniciátorů společné diskuze a jedním z předních řešitelů problematiky. Vzrůstá potřeba diskutovat studijní osnovy a plány nově vznikajících oborů v oblasti bezpečnosti ICT, jejich dostatečnost z pohledu rozsahu znalostí, jejich atraktivitu pro studenty středních škol a bakalářských oborů a uplatnitelnost absolventů těchto oborů na pracovním trhu. Velkou výzvou mohou být úvahy o propojení akademické sféry se soukromou sférou v rámci jedné vzdělávací platformy.

1.1. Cíl diplomové práce

Cílem této diplomové práce je definovat minimální požadavky na znalosti odborníků v poměrně nové oblasti – bezpečnost ICT, vyhledat mezery v současném vzdělávání na vysokých školách v magisterských oborech zaměřených na bezpečnost ICT a na závěr zformulovat strategii ve formě doporučení pro rozvoj vzdělávání v této oblasti. Tato práce může být významným vodítkem při plánování nových studijních programů a oborů, neboť čerpá z dosavadních poznatků o potřebách vzdělávání v této oblasti, a to na celosvětové úrovni. Taktéž může být vhodným podkladem pro společné diskuze mezi vysokými školami a soukromou sférou na téma, jak zlepšit kvalitu absolventů a jejich zapojení do praxe. Cílem analýzy vybraných studijních oborů

[3] V praxi je vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) často označována jako VKB (4). Tato zkratka byla zvolena i pro použití v této práci.

věnujících se bezpečnosti ICT je poukázat na rozdíly v rozsahu získaných znalostí, mezery mezi optimální skladbou znalostní základny a současnou skladbou znalostní základny absolventů těchto studijních oborů.

1.2. Metodika práce

Bezpečnost ICT je poměrně nový obor. Ačkoli začíná být v poslední době více diskutován, neexistuje pro něj, oproti jiným oborům, dostatek odborných materiálů. To je také dáno tím, že se jedná o multidisciplinární obor, a tak při řešení některých problémů v oblasti bezpečnosti ICT, musí spolupracovat několik odborníků napříč různými obory. To také znesnadňuje vytvoření jednotného znalostního rámce. To se projevuje i ve výuce na vysokých školách, kde vzniká mnoho různých pohledů a zaměření na bezpečnost ICT (právní hledisko, politické hledisko, sociologické hledisko, apod.). Přičemž praxe ukazuje, že je stále více potřeba disponovat odborníky, kteří rozumí celé problematice z různých pohledů. Je velmi složité tento požadavek naplnit a zůstává otázkou, zda se ho někdy podaří zcela naplnit. Důvodem je, že potřebné zlepšení vyžaduje spolupráci soukromé, státní, ale i akademické sféry a v neposlední řadě také spolupráci odborníků z mnoha různých oborů.

Teoretická část práce je tak zaměřena na sjednocení současných poznatků do jednoho znalostního rámce. Snaží se vymezit bezpečnost v kontextu ICT prostředí a ukázat, o jak komplexní disciplínu se jedná a jak široké portfolio znalostí zahrnuje. Definuje základní teoretická východiska, které by odborníci na bezpečnost ICT měli znát. Pokrýt však celé portfolio znalostí do hloubky, by bylo nad rámec této práce a není to ani jejím cílem. Záměrem je ukázat, na jak rozsáhlou problematiku se musí současné vzdělávání zaměřit, jak širokou základnu znalostí musí pokrýt, aby byli absolventi takových oborů co možná nejvíce uplatnitelní v praxi. Práce ukazuje základní teoretická východiska, na kterých je bezpečnost ICT postavena a základní pojmy, které na sebe nabaluje: řízení bezpečnosti informací a řízení kybernetické bezpečnosti. A protože bývá akademická sféra často obviňována z toho, že nereflektuje současné trendy ICT, je v práci tato oblast tematicky pokryta a v praktické části analyzována.

Dále se práce zaměřuje na vývoj bezpečnosti ICT, pro pochopení podstaty této oblasti a důvodu, proč je snahou tento obor dále rozvíjet. Historie normalizace bezpečnosti a vývoj legislativy v České republice (ČR) ukazují vývoj normalizačních a legislativních rámců, jejichž znalost je dnes pro odborníky v oblasti bezpečnosti ICT nezbytností. To také dokazuje část práce věnovaná analýze trhu. Té v teoretické části předchází popis situace na současném pracovním trhu v oblasti bezpečnosti ICT, tj. růst poptávky po odbornících v oblasti ICT, výše mezd v této oblasti a bariéry v uplatnění absolventů. Stále však neexistuje dostatek zdrojů, které by tuto problematiku dokázaly dostatečně pokrýt. To se projevuje zejména ve statistikách, jež v ČR vydává

Český statistický úřad (ČSÚ). Právě tyto statistiky prozatím oblast bezpečnosti ICT dostatečně nereflektují, a tak není zcela možné podat konkrétní údaje o současném aktuálním stavu odborníků v oblasti bezpečnosti ICT na trhu práce.

Na tuto část dále navazuje popis současného stavu vzdělávání odborníků v oblasti bezpečnosti ICT: identifikace vysokoškolských oborů se zaměřením na bezpečnost ICT, identifikace nabídky, existující teoretická východiska a obecná doporučení pro oblast vzdělávání těchto pracovníků. V rámci této části je popsáno kurikulum pro vzdělávání v oblasti bezpečnosti ICT „Cybersecurity Curriculum 2017“, které obsahuje model pro strukturu znalostní základny vysokoškolských oborů. Tento model je použit v praktické části analýzy vzdělávání ve vybraných magisterských oborech zaměřených na oblast bezpečnosti ICT. Aby mohla být stanovena strategie pro zlepšení vzdělávání v oblasti bezpečnosti ICT, je nezbytné nejprve nalézt mezery v současném vzdělávání v oblasti bezpečnosti ICT, a teprve potom představit možná doporučení pro rozvoj vzdělávání.

Nalezení nedostatků a mezer ve vzdělávání odborníků na bezpečnost ICT, se věnuje celá praktická část. Ta nejprve stanovuje znalostní bázi v oblasti bezpečnosti ICT, dle které jsou jednotlivé studijní obory hodnoceny. Pro stanovení optimální znalostní báze, vychází práce zejména z existujících doporučení a z analýzy pracovního trhu. Pro hodnocení vybraných magisterských oborů jsou v praktické části definována kritéria hodnocení, na základě nichž, je dále provedeno hodnocení jednotlivých vybraných oborů. Výsledkem hodnocení vysokoškolských oborů jsou unikátní profily absolventů. Závěry z celkového hodnocení oborů jsou následně přeneseny do SWOT analýzy, která hodnotí silné a slabé stránky současného vzdělávání v oblasti bezpečnosti ICT, identifikuje klíčové příležitosti a dále hrozby, které je nezbytné eliminovat. Výsledná doporučení jsou založena na potlačení slabých stránek a eliminaci rizik s návrhem, jak využít některých příležitostí.

2. Vymezení bezpečnosti

Bezpečnost je velmi široký pojem, který je spojován s mnoha oblastmi (např. bezpečnost a ochrana zdraví při práci, bezpečnost potravinových výrobků, bezpečnost letového provozu, atd.). Otázkou je, jak můžeme bezpečnost obecně definovat a jak definovat bezpečnost ICT.

V Ústavu bezpečnostního inženýrství Tomáše Bati ve Zlíně, byly odborníky navrženy postuláty teorie bezpečnosti, které základní principy bezpečnosti popisují. Tyto postuláty byly založeny na bezpečnostním paradigmatu: *„referenční objekt: hrozba*[4] *– riziko*[5] *(újma) – opatření*[6]*“* (6 s. 325). Jedná se o tyto postuláty teorie bezpečnosti (6 s. 326):

- *„Bezpečnost neexistuje sama o sobě, ale je vždy spojena s konkrétním referenčním objektem. Cílem bezpečnosti je zabránit újmě (negativnímu dopadu).“*
- *„Bezpečnost je stav, kdy je riziko (možná újma), plynoucí z bezpečnostních hrozeb, minimalizováno na akceptovatelnou úroveň.“*
- *„Akceptovatelná úroveň rizika je dána normou, rozhodnutím nebo pocitem.“*
- *„K narušení bezpečnosti/bezpečnostnímu incidentu dochází záměrně, nedbalostí nebo náhodně.“*
- *„Bezpečnost závisí na vnitřních a vnějších činitelích.“*
- *„Bezpečnost lze ovlivnit (řídit) přijetím účelových opatření. Preventivní opatření snižují četnost a represivní opatření velikost újmy (negativního dopadu).“*
- *„Bezpečnost se zajišťuje v těch druzích bezpečnosti, na nichž se shodne společnost.“*

Z těchto postulátů lze pak snadno odvodit tyto základní principy bezpečnosti (6 s. 326):

- bezpečnost je konkrétní a váže se k určitému referenčnímu objektu;
- úroveň bezpečnosti může být vnímána subjektivně;
- narušeny mohou být pouze ty vlastnosti referenčního objektu, které jsou mu vlastní;
- cílem bezpečnosti je zabránit negativnímu dopadu;

---

[4] *„Hrozba je zneužitím zranitelnosti“*. (5 s. 61) Zranitelnost je slabé místo referenčního objektu, prostřednictvím něhož může hrozba působit (5 s. 62).

[5] Riziko je kombinací hrozby a zranitelnosti referenčního objektu, která má na tento objekt určitý dopad (5 s. 63). Dopad je škoda způsobená vlivem působení hrozby na referenční objekt (5 s. 64).

[6] *„Opatření je jakákoliv aktivita, zařízení, technika či jiný postup, který umožní snížit sílu hrozby, která na informační systém působí, nebo úplně zabrání v jejím účinku.“* (5 s. 63)

- bezpečnost je stav, který se může vlivem různých proměnných měnit;
- existují různé druhy bezpečnosti.

Cílem kapitoly je:

- vymezit bezpečnosti ICT.

2.1. Druhy bezpečnosti

Mezi první druhy bezpečnosti patřila historicky fyzická a mezinárodní bezpečnost. V průběhu průmyslové revoluce pak bezpečnost zdraví při práci[7], s příchodem automobilů vznikla dále bezpečnost silničního provozu, o něco později vznikla bezpečnost letového provozu, s příchodem technologií a počítačů vznikla nakonec informační bezpečnost (často také označována jako počítačová bezpečnost ve spojení s informacemi v digitální podobě) (6 s. 329). Teprve po vzniku a rozšíření Internetu, a s rozvojem kybernetického prostoru[8] postupně došlo ke vzniku kybernetické bezpečnosti. Obecně lze říci, že *„druhem bezpečnosti je soubor opatření, metod, sil a prostředků, které zajišťují bezpečnost ve vymezené části bezpečnostní reality.“* (6 s. 329)

S informační bezpečností, počítačovou a kybernetickou bezpečností, se lze setkat na několika úrovních (9):

- stát,
- organizace/instituce,
- jednotlivci.

Na těchto třech úrovních může být ohrožen rozvoj, existence a základní lidské potřeby, přičemž zdroje hrozby mohou být různé – např. jiné státy, trhy, globální ekonomika, živelné pohromy, technické poruchy, ale také jednotlivci (9). Hrozbou může být v podstatě jakákoliv událost či akce, která negativně působí na referenční objekt. Negativní působení hrozby je umožněno díky zranitelnosti referenčního objektu. Cílem bezpečnosti je dle výše zmiňovaných postulátů eliminovat zranitelnosti referenčního objektu, aby se zabránilo působení hrozby a zamezit tak možným dopadům.

Referenčním objektem **počítačové bezpečnosti** jsou počítačové (výpočetní) systémy, které se skládají z hardwarových, firmwarových a softwarových prostředků. Tyto systémy zpracovávají data v rámci výpočetních operací, na kterých může záviset například řízení letového provozu.

[7] Tzv. BOZP, bezpečnost a ochrana zdraví při práci (7).

[8] *„Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací.“* (8 s. 59) V praxi často označován jako kyberprostor.

Cílem počítačové bezpečnosti je eliminovat hrozby, které by mohly ohrozit jakoukoliv z těchto částí a narušit tak spolehlivost a důvěryhodnost zpracovávaných dat. Výchozím normativním základem počítačové bezpečnosti je dokument „Kritéria hodnocení důvěryhodných výpočetních systémů“ (TCSEC). Ten definuje systém hodnotících kritérií pro hodnocení počítačových systémů z hlediska bezpečnosti (5 s. 64-65). TCSEC je blíže popsán v kap. 6.1. – „Historie normalizace bezpečnosti ICT“.

Referenčním objektem **kybernetické bezpečnosti** je, dle definice kyberprostoru, digitální prostředí tvořené *„informačními systémy, službami a sítěmi elektronických komunikací“* (8 s. 59). Přičemž některé z těchto systémů mohou být součástí kritické informační infrastruktury či významnými informačními systémy (3). Tyto informační služby, systémy a sítě existují v rámci otevřeného kyberprostoru, kde dochází ke zpracování a výměně dat. Cílem kybernetické bezpečnosti je tedy elimininovat hrozby, které by mohly ohrozit informační systémy, služby či sítě a narušit tak integritu, důvěrnost či dostupnost dat v nich obsažených. K ochraně kyberprostoru a řízení kybernetické bezpečnosti se v ČR váže ZKB a související prováděcí VKB, které jsou dále popsány v kap. 4. – „Řízení kybernetické bezpečnosti“ (3,4).

Primárním cílem počítačové bezpečnosti a kybernetické bezpečnosti je ochrana informací v digitalizované podobě. **Bezpečnost informací** existuje nad těmito druhy bezpečnosti a tvoří nad nimi jakousi „nadstavbu“ (5 s. 59). Informace v digitalizované podobě jsou obsaženy v samotných informačních a komunikačních systémech a pro zachování jejich bezpečnosti je nutné zavádět účinná bezpečnostní opatření, zejména tam, kde jsou nepostradatelné (5 s. 59). Tyto informace mohou být sdíleny napříč Internetem, a tak musí být nastavena i pravidla pro jejich „vynášení“ mimo hranice zabezpečeného prostředí. Informace ovšem nemusí být zneužity pouze v digitalizované podobě, ale také v klasické „papírové“ podobě. Bezpečnost informací se zabývá ochranou informací ve všech těchto formách. Nicméně tato práce je zaměřena na ICT prostředí a ICT odborníky, tudíž bude bezpečnost informací v práci spojována pouze s informacemi v digitální podobě.

Informace zpravidla tvoří informační aktiva[9], které mají pro své vlastníky určitou hodnotu a jejich ztráta, nedostupnost či neoprávněná změna vlivem působení hrozby, mohou organizacím způsobit značnou škodu (5 s. 61). Tato aktiva (v digitální podobě) jsou vždy někde uložena (např. databázový server). To znamená, že pro jejich bezpečnost je nezbytné zajistit bezpečnost jak na úrovni aktiv samotné organizace[10], tak na samotné úrovni informačních aktiv a dále na

[9] *„Aktivum je cokoli v organizaci, co má nějakou cenu.“* (5 s. 61)

[10] V organizacích se jedná o organizační bezpečnost, tj. ochrana majetku, vstupu do objektů, datových sálů, atd. (5 s. 61).

úrovni aktiv ICT prostředí, ve kterém jsou zpracovávána. Výchozím standardem pro řízení bezpečnosti informací v organizaci je sada norem ISO/IEC 27000, která je dále popsána v kap. 3. – „Řízení bezpečnosti informací“ (10). Cílem řízení bezpečnosti informací je zajištění jejich důvěrnosti, integrity a dostupnosti, kde (5 s. 59):

- **DŮVĚRNOST** znamená, že informace mohou být zpřístupněny či sděleny pouze oprávněným osobám či entitám;
- **INTEGRITA** znamená, že informace nemohou být bez oprávnění modifikovány;
- **DOSTUPNOST** znamená, že informace jsou dostupné v okamžiku jejich vyžádání oprávněnou osobou či entitou.

Organizace jsou na informacích, kterými disponují značně závislé, neboť se podílejí na tvorbě jejich hodnoty, a tak je jejich ochrana (nejen v papírové či mluvené podobě) nezbytnou součástí činnosti organizace v rámci řízení bezpečnosti informací (popsáno v kap. 3. – „Řízení bezpečnosti informací“). Organizace, které jsou z pohledu ZKB povinnými subjekty, pro ochranu svých informačních a komunikačních systémů zavádí obdobný systém zaměřený na řízení kybernetické bezpečnosti. Způsob řízení kybernetické bezpečnosti a požadavky na povinné subjekty jsou dále uvedeny v kap. 4. – „Řízení kybernetické bezpečnosti“. Bezpečnost ICT se tak stává součástí řízení informatiky, které svou činností napomáhá k dosažení cílů celé organizace a k tvorbě její hodnoty (viz. kap. 3. - „Řízené bezpečnosti informací“).

Základní rozlišení druhů bezpečnosti v prostředí ICT bylo výše vysvětleno. Protože se tato práce zabývá vzděláváním odborníků v oborech, které se zabývají bezpečností v souvislosti s informačními a komunikačními technologiemi, ochranou kritické informační a komunikační infrastruktury, ochranou zpracování dat v informačních systémech, atd., bude nadále v této práci používán pojem **„bezpečnost ICT“**. Ten pod sebou skrývá pojmy počítačová bezpečnost, kybernetická bezpečnost a samozřejmě také bezpečnost informací v digitalizované podobě, které díky své propojenosti tvoří jeden společný a propojený celek – bezpečnost ICT.

3. Řízení bezpečnosti informací

V kap. 2.1. – „Druhy bezpečnosti“ bylo zmíněno, že výchozím standardem pro řízení bezpečnosti informací je **řada norem ISO/IEC 27000** (10). Tato sada norem definuje celý **systém řízení bezpečnosti informací**[11] (ISMS) (5 s. 95). Jeho zavedení je dnes téměř povinností pro každou větší organizaci, jenž využívá pro zpracování informací informační a komunikační technologie. Taktéž bylo zmíněno, že standard se netýká pouze informací v digitalizované podobě, ale také informací v „papírové“ podobě. Většina organizací dennodenně zpracovává obrovské množství informací, ať už v rámci HR agendy, marketingu, či v rámci rozsáhlých ERP systémů. Některé z těchto informací nemusí být určeny ke zveřejnění. Na těchto informacích zpravidla závisí správné fungování hlavních i podpůrných procesů organizace. Mnohdy i samotná existence organizace.

Už sama historie ukázala, jak důležitou roli hrají informační systémy a spolehlivost informací v nich obsažených. Příkladem mohou být aféry společností Enron či Worldcom, kde nespolehlivé informace a selhání auditních kontrol zapříčinily krizi důvěry v obdobné organizace a následně krizi celého finančního sektoru (5 s. 38). Ta měla za následek narušení ekonomiky mnoha dalších zemí. Spolehlivé zpracování informací a jejich průkaznost v informačních systémech vzrostly na významu. Na IT začaly být kladeny nároky, aby poskytovalo spolehlivé a průkazné informace (5 s. 40). Požadavkem bylo, aby IT tvořilo přidanou hodnotu, podporovalo celkovou strategii organizace a řídilo rizika spojená s používáním IT (5 s.40). Právě jedním z největších rizik je nasazování nových informačních technologií, které ohrožuje zpracovávání dat (5 s. 40). V návaznosti na popsané události tak postupně vznikaly nové koncepce řízení v oblasti IT.

Prvky zmiňovaného ISMS respektují koncepci řízení informatiky s ohledem na zainteresované osoby, tzv. „IT Governance“ (ITG). ITG vychází ze zásad „Corporate Governance“(CG), jejímž cílem je zajistit vyvážený vztah a nastolit důvěru mezi organizací a zainteresovanými osobami (akcionáři, zaměstnanci, zákazníci, statutární orgány, aj.) (5 s. 40). Základní doporučení byla vytvořena v roce 1999 s názvem „OECD Principles of Corporate Governance“ (Principy správy a řízení společností) a v návaznosti na to byl v roce 2001 v ČR vydán dokument „Kodex správy a řízení společností na principech OECD“ (5 s. 40). Základními prvky CG je zajištění souladu s regulatorními požadavky, řízení průběhu procesů a funkcí organizace založených na ukazate-

[11] *„ISMS je část celkového systému řízení organizace, založená na přístupu (organizace) k rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací.“* (11)

lích a na cyklu PDCA, na řízení rizik a etickém řízení (5 s. 41). ITG navazuje na CG jako *„struktura řídících vztahů a procesů umožňující dosažení cílů organizace realizací přidané hodnoty za současného vyrovnání rizika s návratností investic do informačních technologií."* (5 s. 41)

Na ITG navazuje koncepce správy a řízení bezpečnosti informací, tzv. „Information Security Governance" (ISG), která je v odpovědnosti statutárních orgánů a vrcholového vedení organizace a je součástí celkové správy a řízení organizace nazývaného jako „Enterprise Governance" (EG) (5 s. 44). Výstupem ISG by mělo být zejména propojení bezpečnosti informací s celkovou strategií organizace a zaměření na podporu hlavních cílů organizace, řízení rizik, řízení zdrojů, hodnocení realizace cílů ISG a vykazování dosažených hodnot pomocí optimalizace investic do bezpečnosti informací (5 s. 45). V uplatňování této koncepce může pomoci právě standard ISO/IEC 27000, který reflektuje základní principy ISG a ukazuje „best practices", jak účinně řídit bezpečnost informací v organizaci s ohledem na principy správy a řízení organizace (10).

Za účelem podpory naplňování hlavních cílů prostřednictvím IT, pro zajištění kontinuity činností organizace a ochranu aktiv je nezbytné vynaložit určité investice do bezpečnosti ICT. K tomu je vhodné zavádět ISMS pro zajištění bezpečnosti informací zpracovávaných v prostředí ICT. Certifikací svého ISMS mohou organizace získat nejen zvýšení efektivity investic vynakládaných na zajištění požadované míry bezpečnosti informací, ale také konkurenční výhodu prokázáním splnění určité úrovně bezpečnosti (např. při výběrových řízeních, kde může být certifikace na ISMS jedním z hlavních požadavků), nebo také zvýšení důvěryhodnosti organizace pro partnery a zákazníky, či jednoduše splnění povinnosti ochrany osobních údajů, atd. (12 s. 48). A právě požadavky normy poskytují organizacím sadu doporučení, které pomáhají dosáhnout efektivního řešení bezpečnosti informací pro každou organizaci bez ohledu na odvětví, ve kterém působí.

Systém řízení bezpečnosti informací je založen na konceptu Demingova cyklu PDCA (Obr. 1) – metoda postupného zlepšování procesů řízení bezpečnosti na základě činností (12 s. 24-25, 13):

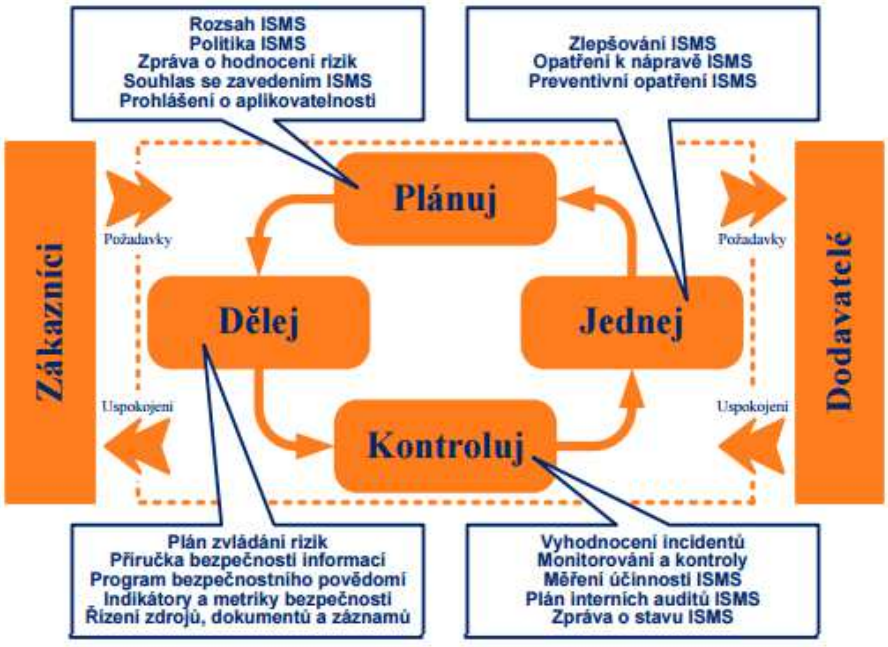
- **plan** (plánuj) – ustanovení ISMS,
- **do** (dělej) – zavádění a provozování ISMS,
- **chec**k (kontroluj) – monitorování a přezkoumání ISMS,
- **act** (jednej) – udržování a zlepšování ISMS.

Základní norma ISO/IEC 27001:2013 – „Systém řízení bezpečnosti informací – Požadavky" (Information Security Management Systems – Requirements), tvoří množinu závazných požadavků, které daný ISMS musí splňovat. Pro získání certifikace v oblasti řízení bezpečnosti informací dle této normy, je nezbytné splňovat veškeré požadavky, které norma ukládá

(5 s. 95,13). Navazující norma ISO/IEC 27002:2013 – „Soubor postupů pro řízení bezpečnosti informací“ (Code of Practice for Information Security Controls) tvoří soubor doporučených postupů, jak daný systém zavádět (5 s. 96, 14). Tyto postupy na rozdíl od požadavků na ISMS uvedené v ISO/IEC 27001:2013 závazné nejsou (5 s. 95-96,13). Tvoří však jádro „best practices“ zejména pro manažery bezpečnosti a ostatní zainteresované osoby na ISMS. Popis dílčích etap životního cyklu ISMS jsou popsány v následujících podkapitolách.

Cílem kapitoly je:

- definovat základní pojmy bezpečnosti informací,
- představit sadu norem pro řízení bezpečnosti informací ISO/IEC 27000,
- představit etapy životního cyklu ISMS.



Obr. 1: Demingův cyklus PDCA pro řízení bezpečnosti informací (11)

3.1. Ustanovení ISMS

Ustanovení ISMS zahrnuje definici rozsahu ISMS (hranic) a odsouhlasení dokumentu „Prohlášení o politice ISMS“, kdy by celá etapa měla být ukončena deklarovaným souhlasem vrcholovým vedením společnosti se zavedením ISMS v organizaci (5 s. 96). Tím dává vedení organizace na vědomí svou podporu zaváděného ISMS.

V rámci této etapy jsou prováděny činnosti (5 s. 96):

- definice rozsahu (vč. vazeb a hranic systému);
- zpracování a schválení dokumentu „Prohlášení o politice ISMS“[12];
- identifikace a ohodnocení aktiv ISMS;
- identifikace, analýza a vyhodnocení rizik ISMS;
- zpracování závěrečné zprávy z hodnocení rizik;
- schválení zbytkových (reziduálních) rizik vedením organizace;
- deklarace souhlasu vedením organizace k zavedení ISMS;
- příprava dokumentu „Prohlášení o aplikovatelnosti“[13].

Nová verze ISO/IEC 27001:2013 klade důraz na pochopení kontextu organizace (13,15). Organizace nejprve musí být schopna analyzovat prostředí, ve kterém působí. Měla by pomocí SWOT analýzy identifikovat veškeré vnitřní, ale také externí činitele (slabé a silné stránky organizace, příležitosti a hrozby) (15). Teprve potom by měla určit, jak rozsáhlý bude celý systém ISMS (15). Bezpečností by se měla zabývat zejména tam, kde se nachází hlavní procesy organizace a hodnotná aktiva. Teprve požadavky kladené na ochranu fungování hlavních procesů organizace a na ochranu aktiv determinují rozsah celého ISMS (15). Nově je navíc ve verzi z roku 2013 povinností vrcholového vedení stanovit dvě konkrétní role, z nichž jedna bude odpovědná za shodu nastaveného ISMS s požadavky normy ISO/IEC 27001:2013 a druhou odpovědnou osobu za podávání zpráv o výkonnosti celého ISMS (13,15).

Stěžejním úkolem v rámci této etapy je analýza rizik. Od jejich výsledků se teprve odvíjí způsob zvládání[14] a mitigace rizik. V literatuře se doporučuje nejprve začít s počáteční analýzou rizik na hrubé úrovni pro všechny systémy IT (12 s. 91). Teprve u systémů, které jsou významné pro činnost organizace, je vhodné dále zpracovat podrobnou analýzu rizik, neboť tyto systémy mohou být vystaveny vysokým rizikům (12 s. 91). V rámci organizace by měla být v průběhu této úvodní etapy nejprve nastavena akceptovatelná úroveň rizika (5 s. 107). V případě, že z analýzy rizik vzejdou rizika, jež jsou z pohledu organizace neúnosná (např. velká finanční

[12] Upřesňuje cíl zavedení ISMS v organizaci a rámec pro řízení bezpečnosti informací a stanovuje kritéria pro hodnocení rizik (5 s. 98).

[13] Dokument, který popisuje jednotlivá vybraná bezpečnostní opatření a jejich cíle (5 s.108). Je důležitým podkladem pro auditory, neboť vypovídá o celkovém stavu zavedeného ISMS a je vhodným podkladem pro kontrolu toho, zda byla pokryta všechna identifikovaná rizika (5 s. 109).

[14] Proces, kdy jsou vybírána bezpečnostní opatření k mitigaci rizik a jejich následné přijetí (5 s. 99).

ztráta, ztráta zákaznické základny, apod.), musí se zavést příslušná bezpečnostní opatření, aby takové riziko bylo sníženo na minimální a pro organizaci akceptovatelnou úroveň (5 s.107). Pro přebývající zbytková rizika, by měly být vytvořeny krizové plány, které jasně říkají, co mají odpovědné osoby dělat, pokud dojde k působení rizika (5 s. 96).

Analýza rizik je úkolem manažera bezpečnosti, který by měl v této oblasti disponovat patřičnými znalostmi a dovednostmi. Sada norem ISO/IEC 27000 mu přináší normativní podporu, jak k analýze a k plánování zvládání rizik přistupovat (10). Jako metodická příručka mu může posloužit norma ISO/IEC 27005:2011 – „Řízení rizik bezpečnosti informací" (Information Security Risk Management) (5 s.91,16). Zcela nově v požadavcích normy ISO/IEC 27001:2013, na rozdíl od verze z roku 2005, není nutnou podmínkou, aby identifikace aktiv, hrozeb a zranitelností, byla prerekvizitou pro samotnou identifikaci rizik. Tím je zajištěna větší variabilita v možných použitých metodách pro hodnocení rizik (12,13). Analýza rizik je důležitá nicméně obsahově a rozsahem náročnější disciplína. Není cílem této práce popisovat metodický přístup k analýze rizik, ale upozornit na to, že pojmy s ní spojené jsou základním předpokladem znalostí pracovníků v oblasti bezpečnosti ICT.

Vyústěním analýzy rizik je vyhodnocení rizik a zpráva o hodnocení rizik, jež navrhuje vhodná protiopatření pro eliminaci identifikovaných bezpečnostních rizik (5 s. 106-107). K jejich výběru se nejčastěji využívá rozsáhlý katalog opatření z normy ISO/IEC 27002:2013, který popisuje vždy charakter opatření a jeho cíle (5 s. 106-107,14). Zpráva z hodnocení rizik slouží jako důležitá podkladová dokumentace pro potřeby auditu a organizace v ní dokazuje, že identifikuje a řídí svá rizika spojená se zpracováním informací (5 s. 107). Obdobně je analýza rizik základním východiskem pro ochranu osobních údajů (2). Navržená bezpečností opatření musí být dále schválena na úrovni nejvyššího vedení organizace, které se vyjadřuje i ke zbytkovým rizikům[15] (5 s. 107).

Závěrečným dokumentem vyžadovaným ISO/IEC 27001:2013 je dokument „Prohlášení o aplikovatelnosti", jež by měl obsahovat matici identifikovaných rizik namapovaných na vybraná bezpečnostní opatření a cíle těchto opatření. (5 s. 107-109,13). Celá etapa ustanovení ISMS je následně ukončena. Nicméně řízení rizik není jednorázová záležitost, ale naopak kontinuální proces. Každá z etap v zásadě probíhá v menších PDCA cyklech a pro zlepšování zralosti procesů k zajištění bezpečnosti, nestačí projít celým cyklem jedenkrát, ale mělo by docházet

15 Každá organizace může mít jiný rizikový apetit, a tak některá může být ochotna akceptovat vyšší zbytková rizika než organizace jiná. Samotná úroveň standardem dána není, a tak je na organizaci, jakou únosnou úroveň si sama zvolí.

k neustálému zlepšování na základě zpětné vazby. U analýzy rizik by mělo probíhat pravidelné přehodnocení a aktualizace, zejména v návaznosti na etapy monitorování ISMS, údržbu a zlepšování ISMS.

3.2. Zavádění a provoz ISMS

Další etapa je zaměřena na zavedení a prosazení všech navržených bezpečnostních opatření v etapě ustanovení ISMS (5 s. 111). V této etapě jsou detailně připraveny plány zavádění včetně termínů, potřebných finančních a lidských zdrojů, apod. (5 s. 112). To vyžaduje i určité projektové dovednosti a celý proces zavádění by měl být řízen jako projekt. Vybraná bezpečnostní opatření jsou v rámci této etapy detailně zdokumentována v dokumentu „Příručka bezpečnosti informací“. Příručka musí být vždy předložena k prostudování všem zaměstnancům v organizaci (5 s. 113-114). Jejich povinností je seznámit se s těmito definovanými pravidly a principy ochrany informací v organizaci. K tomu pomáhá taktéž plán budování bezpečnostního povědomí, jehož cílem je kontinuálně prohlubovat bezpečnostní povědomí napříč celou organizací. Za prohlubování bezpečnostního povědomí by měl odpovídat sám manažer bezpečnosti.

V rámci této etapy je celý průběh více zaměřen spíše na samotnou činnost než na tvorbu bezpečnostní dokumentace. Veškerá činnost se tak primárně přenáší na operativní úroveň řízení a činnost specialistů. Ti se svou činností podílí na zavádění dílčích vybraných opatření, jako například vytvoření plánu kontinuity činností a plánu obnovy, nastavení přístupových oprávnění do informačních systémů, konfiguraci firewallů[16], nastavení ochrany před škodlivým kódem, apod. Přesto musí být každá činnost v rámci zavádění a provozu ISMS patřičně zdokumentována pro potřeby auditu. Etapa zahrnuje zejména tyto činnosti (5 s. 111-112):

- zpracování plánu zvládání rizik;
- zavedení vybraných bezpečnostních opatření dle navrženého plánu;
- zpracování „Příručky bezpečnosti informací“;
- definice a realizace plánu budování bezpečnostního povědomí;
- upřesnění způsobu měření účinnosti zavedených bezpečnostních opatření;
- sledování stanovených ukazatelů;

[16] Firewall – HW či SW, který může být pomocí sady pravidel nakonfigurován tak, aby zabránil neoprávněnému přístupu k počítači či službám v síti. (8 s. 38)

- zavedení procesu detekce a reakce na bezpečnostní incidenty;
- řízení zdrojů, dokumentů a záznamů ISMS.

Přesto v této etapě vzniká několik velmi zásadních bezpečnostních dokumentů – „Příručka bezpečnosti informací“. Tu tvoří souhrn bezpečnostních politik, směrnic, pravidel, procesů a postupů (5 s. 113). Jde o druhou úroveň bezpečnostní dokumentace (první jsou dokumenty, jež vyžaduje samotný systém řízení), která slouží k podpoře ISMS v rámci organizace a tvoří základ pro zavádění bezpečnostních opatření (5 s. 113). Na úrovni bezpečnostních politik by dokumentace neměla být až příliš detailní. V podstatě se jedná o srozumitelné vysvětlení základních principů a pravidel pro zajištění bezpečnosti informací, které mají platnost pro všechny zaměstnance dané organizace. Ti jsou dále v rámci plánu budování bezpečnostního povědomí pravidelně školeni.

Teprve na nejnižší úrovni se definují detailní pracovní postupy, které popisují, jak konkrétně navržené bezpečnostní politiky naplňovat (5 s. 113). Zde by mělo být jednoznačně rozlišeno, komu je bezpečnostní dokumentace určena a jaký způsob vyjadřování zde používat (5 s. 113). Jinak může vypadat pracovní postup určený pro administrátory informačního systému a naprosto odlišně pro uživatele tohoto informačního systému. Taktéž je důležité dodržet návaznost na ostatní bezpečnostní dokumentaci, zejména na deklarované bezpečnostní politiky. Kontrola návaznosti je obzvláště namístě tam, kde vzniká velké množství samostatných bezpečnostních dokumentů, a tak se snadno může projevit nekonzistentnost dokumentace.

Bezpečnostní politika by měla pokrývat všechny oblasti bezpečnosti informací, jež jsou definovány v ISO/IEC 27002:2013 (14,17):

- *„řízení aktiv;*
- *řízení přístupu a přístupových práv;*
- *organizace bezpečnosti informací;*
- *bezpečnost lidských zdrojů;*
- *technologie kryptování;*
- *fyzická bezpečnost pracovišť a zařízení;*
- *bezpečnost provozu;*
- *bezpečnost komunikací a přenos dat;*
- *akvizice, vývoj a údržba informačních systémů;*

- *řízení kontinuity činností organizace*[17]*;*
- *zvládání bezpečnostních incidentů;*
- *soulad s interními a externími požadavky.“*

Norma obsahuje „best practices“ pro řízení bezpečnosti informací, a navíc respektuje trend současné doby, jako je outsourcing oblasti IT. Z toho důvodu je vhodné držet se minimálně této doporučené struktury. Ze struktury je patrné, že část doporučení se týká opatření technického charakteru (technická opatření) a část opatření organizačního charakteru (organizační opatření). Ty nejsou v normě striktně odděleny, neboť se vzájemně doplňují a navazují na sebe. To je zásadní rozdíl oproti opatřením uvedeným v ZKB a jeho prováděcí VKB (3). Při návrhu bezpečnostních opatření je nezbytné disponovat dostatečnými znalostmi z obou těchto oblastí.

Předchozí norma ISO/IEC 27002:2005 zahrnovala tyto oblasti (5 s. 13,18):

- *„řízení aktiv;*
- *řízení přístupu;*
- *organizace bezpečnosti informací;*
- *bezpečnost z hlediska lidských zdrojů;*
- *fyzická bezpečnost a bezpečnost prostředí;*
- *řízení komunikací a řízení provozu;*
- *akvizice, vývoj a údržba informačních systémů;*
- *řízení kontinuity činností organizace;*
- *zvládání bezpečnostních incidentů;*
- *soulad s požadavky.“*

Aplikovaná bezpečnostní opatření se dále sledují dle navrženého systému metrik. Systém měření účinnosti[18] by měl být navržen již v rámci etapy plánování, kdy jsou navrženy ukazatelé, způsob sběru dat, způsob měření a výpočtu a způsob vyhodnocování včetně reportovací povinnosti (5 s. 114-115). Samotný proces řízení účinnosti ISMS tak probíhá, obdobně jako ISMS, v PDCA cyklu.

---

[17] Tzv. Business Continuity Management – *„Procesy a/nebo postupy k zajištění nepřetržitého chodu organizace.“* (8 s. 53)

[18] *„Měření je proces získávání informací o účinnosti ISMS a bezpečnostních opatřeních, dosažení cílů bezpečnostních opatření a výkonnosti procesů ISMS, který využívá metody měření, funkce měření, analytický model a kritéria pro rozhodování.“* (5 s. 116)

3.3. Monitorování a přezkoumání ISMS

Předposlední etapa je zaměřena na poskytnutí zpětné vazby ohledně účinnosti zavedeného ISMS (5 s. 123). Zde hraje důležitou roli posouzení fungování ISMS a samotné účinnosti ISMS oddělením interního auditu, které by mělo poskytnout dostatek podkladů o jeho současném fungování, pro přezkoumání vedením organizace (5 s. 123-124). To by mělo být prováděno minimálně jednou ročně. Na základě zpětné vazby z přezkoumání by měly být učiněny konkrétní kroky pro zlepšení zavedeného ISMS.

V rámci etapy probíhají následující činnosti (5 s. 123):

- monitorování a kontrola účinnosti zavedených bezpečnostních opatření;
- provedení interního auditu ISMS;
- zpracování zprávy o stavu ISMS pro účely dalšího přezkoumání;
- přezkoumání[19] ISMS vedením organizace.

Pro měření účinnosti zavedeného systému se nejprve definují počáteční hodnoty vybraných ukazatelů a tento systém měření se následně testuje a teprve potom dochází ke sběru dat a monitorování ISMS v provozu (5 s.116). Nasbírané informace o provozu ISMS dále slouží jako podklad pro audit, jehož úkolem je hodnotit účinnost zavedeného systému (5 s. 116).

Zejména stěžejním cílem kontroly a případného přezkoumání ISMS by měl být proces detekce a reakce na bezpečnostní události[20] a incidenty[21], tj. zvládání bezpečnostních incidentů (5 s. 123). Výsledkem celého procesu přezkoumání mohou být různé podněty pro úpravu procesů, pravidel a postupů, ale také podněty pro aktualizaci příslušné dokumentace a plánů ISMS, zejména pak pro aktualizaci analýzy rizik (5 s. 124-125). To následně přispívá k celkovému zlepšování zavedeného ISMS.

3.4. Údržba a zlepšování ISMS

Poslední etapou cyklu PDCA je udržování a zlepšování zavedeného ISMS. Zavedením, přehodnocením a certifikací ISMS celý cyklus nekončí. Na základě zpětné vazby z pravidelného pře-

---

[19] *„Činnost prováděná k určení vhodnosti, přiměřenosti a efektivnosti předmětu zkoumání k dosažní stanovených cílů“*. (5 s. 124)

[20] Bezpečnostní událost je taková událost, která *„může způsobit nebo vést k narušení informačních systémů a technologií a pravidel definovaných k jeho ochraně.“* (8 s. 28) Tj. vést k bezpečnostnímu incidentu.

[21] Bezpečnostní incident je již konkrétní porušení/narušení nastavených bezpečnostních politik, pravidel, zásad a postupů či bezpečnostních pravidel provozu ICT (8 s. 25).

hodnocování, by mělo naopak docházet k větší zralosti a také dokonalosti zavedených procesů ISMS. To vyjadřuje tzv. model zralosti procesů (CMM), který definuje šestistupňovou stupnici pro hodnocení zralosti procesů od neexistujícího procesu, až po jeho optimalizovanou úroveň (5 s. 52). Získaná zpětná vazba by měla zajistit kontinuální zlepšování celého systému. Etapa je vyhraněna především pro nápravu neshod a nedostatků zjištěných v etapě monitorování a přezkoumání ISMS (5 s. 125). Pro etapu jsou typické činnosti, jako (5 s. 125):

- zavádění zlepšení ISMS na základě identifikovaných podnětů;
- provádění opatření k nápravě a preventivní opatření pro odstranění nedostatků.

4. Řízení kybernetické bezpečnosti

Obdobně jako je definován systém řízení bezpečnosti informací, je definován **systém pro řízení informací v kybernetické bezpečnosti**, který je založen na ISMS. Ten je definován ZKB a související prováděcí VKB (3,4). Nejedná se již jen o doporučení, ale o právní předpis, který je pro zákonem definované subjekty povinný. Aby bylo vůbec možné chápat požadavky zákona, je nezbytné se orientovat i v souvisejících předpisech. Mezi ně patří vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích (VVIS), nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (NKI) a v neposlední řadě zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (ZKŘ)[22] (19,20,21).

Cílem kapitoly je:

- definovat základní pojmy kybernetické bezpečnosti,
- představit zainteresované subjekty,
- představit oblasti bezpečnostních opatření,
- ukázat návaznost na související legislativu.

4.1. Povinné subjekty

Důležité je zejména pochopení toho, kterých subjektů se ZKB týká. Dodržování zákona není totiž povinné pro všechny organizace, ale povinné subjekty jsou stanoveny přímo v ZKB. Kybernetická bezpečnost ve smyslu zákona se sice týká pouze subjektů v něm definovaných. Mohou se s ní však setkat i subjekty, které jsou dodavateli ICT řešení (např. SW) subjektů, kteří jsou správci kritických informačních systémů či například správcem „Informačního systému o informačních systémech veřejné správy“ (IS o ISVS) (19).

Existují **čtyři kategorie subjektů**, na něž se požadavky zákona vztahují. Tyto subjekty jsou vyjmenovány v ZKB § 3 písm. a) až e) (3):

- *„poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmena b),*
- *orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d),*

[22] ZKB lze chápat jako jakýsi doplněk ZKŘ, a to v tom smyslu, že konkretizuje požadavky na zajištění bezpečnosti průmyslových a řídících systémů.

- *správce informačního systému kritické informační infrastruktury,*
- *správce komunikačního systému kritické informační infrastruktury a*
- *správce významného informačního systému".*

Zajištěním sítě elektronických komunikací se v zákoně č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (ZEK) dle § 2 písm. f) myslí *„zřízení této sítě, její provozování, dohled nad ní, nebo její zpřístupnění"* (22). Službou elektronických komunikací se pak dle § 2 písm. n) uvedeném v ZEK myslí *„služba obvykle poskytována za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací"* (22). Poskytovatelé elektronických komunikací lze vyhledávat v „Evidenci podnikatelů v elektronických komunikacích podle všeobecného oprávnění"[23] vedené Českým telekomunikačním úřadem (ČTÚ).

Významnou sítí je dle ZKB § 2 písm. g) myšlena *„síť elektronických komunikací zajišťujících přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře"* (3). Žádný jiný předpis významnou síť blíže nespecifikuje tak, jako tomu bylo v předchozím případě u poskytovatelů elektronických komunikací. V případě, že subjekt poskytuje datovou síť, nebo je na tento subjekt napojen významný informační systém či kritická infrastruktura, pak tento subjekt spadá do kategorie stanovené v ZKB § 3 písm. b) (3).

Další dvě kategorie v ZKB § 3 písm. c) a d) se týkají správců systémů kritické informační a komunikační infrastruktury (3). V případě písm. c) se jedná o *„správce informačního systému kritické informační infrastruktury"* (správce IS KII) a v případě písm. d) se jedná o *„správce komunikačního systému kritické informační infrastruktury"* (správce KS KII) (3). Přičemž kritická infrastruktura je ve „Výkladovém slovníku kybernetické bezpečnosti" definována jako *„systémy a služby, jejichž nefunkčnost nebo špatná funkčnost by měla závažný dopad na bezpečnost státu, jeho ekonomiku, veřejnou správu a v důsledku na zabezpečení základních životních potřeb obyvatelstva"* (8). Dle ZKŘ § 2 písm. g) je kritickou informační infrastrukturou *„prvek, nebo systém prvků kritické informační infrastruktury."* (21)

NKI rozlišuje v § 1 a § 2 dvě oblasti kritérií pro určení prvku kritické infrastruktury, tzv. „průřezová a odvětvová kritéria" (20). Průřezová kritéria pro určení prvku kritické infrastruktury definují různá hlediska, na základě nichž, by měl být daný prvek zařazen do kritické infrastruktury státu. Jedná se o hledisko počtu obětí, ekonomický dopad a dopad na veřejnost (20). Tato průřezová kritéria dle ZKŘ § 10 odst. 1 písm. e) navrhuje Ministerstvo vnitra ČR (21). Dále dle

[23] Dostupné z: https://www.ctu.cz/vyhledavaci-databaze/evidence-podnikatelu-v-elektronickych-komunikacich-podle-vseobecneho-opravneni

ZKŘ § 10 odst. 1 písm. f) Ministerstvo vnitra ČR *„zpracovává seznam, který je podkladem pro určení prvků kritické infrastruktury a prvků evropské kritické infrastruktury dle § 4 odst. 1 písm. e)“* (21). Odvětvová kritéria jasně vymezuje NKI. Tato kritéria se již opírají o odvětví, které zajišťují veřejnou infrastrukturu a jsou z jejich podstaty považována za kritická, například energetika, vodní hospodářství, zdravotnictví, doprava, aj. (20)

Posledním subjektem podléhajícím ZKB je správce významného informačního systému (správce VIS), jehož ZKB v § 2 písm. d) definuje jako *„informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci“* (3). Identifikace správců VIS je závislá na VVIS, která převážnou většinu správců vyjmenovává, ale neudává konečný seznam správců VIS (19). Opět stanovuje kritéria pro identifikaci významných IS, a to dopadová určující kritéria a oblastní určující kritéria a dále zmiňuje v § 3 odst. 3, že *„naplnění určujících kritérií významného informačního systému, který není uveden v příloze č. 1 k této vyhlášce, posuzuje správce informačního systému“* (19).

4.2. Kontrolní orgány

Povinné osoby jsou kontrolovány v rámci průběžných auditů, zda naplňují ZKB a prováděcí VKB ze strany kontrolního orgánu. K tomu musí dokladovat soulad s těmito právními předpisy. Nejvyšší autoritou v oblasti problematiky kybernetické bezpečnosti v rámci ČR a kontrolním orgánem dle ZKB § 23 je Národní bezpečnostní úřad (NBÚ) (23). Mimo oblast kybernetické bezpečnosti se NBÚ věnuje dále ochraně utajovaných informací a posuzování bezpečnostní způsobilosti fyzických a právnických osob (24). Ve své působnosti se řídí zejména ZKB a zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (3,24,25). Pro koordinaci a spolupráci v rámci ČR a na mezinárodní úrovni vzniklo jako součást NBÚ Národní centrum kybernetické bezpečnosti (NCKB) (23).

NCKB se zaměřuje svou činností na prevenci, detekci a návrh opatření při řešení bezpečnostních incidentů (26). Pro tyto potřeby provozuje vládní CERT ČR, spolupracuje jak s vládními, tak i mezinárodními CERT a CSIRT týmy, podílí se na přípravě bezpečnostních standardů, podporuje budování bezpečnostního povědomí a provádí výzkum a vývoj v oblasti kybernetické bezpečnosti (26). Vládní CERT je tým odborníků, který pomáhá reagovat správcům VIS a KII na vzniklé bezpečnostní incidenty a snaží se zvyšovat bezpečnostní povědomí v oblasti kybernetické bezpečnosti a informovat o aktuálních hrozbách (26). Vůči Vládnímu CERTu jsou správci VIS a KII povinni hlásit kontaktní údaje, vzniklé kybernetické bezpečnostní incidenty a provádět reaktivních opatření na bezpečnostní incidenty (3).

CSIRT tým je národním CERT týmem, který je zaměřený na koordinaci při řešení bezpečnostních incidentů v oblasti elektronických komunikací, sítí elektronických komunikací a v oblasti významných sítí (27). Jeho primárním úkolem je zlepšovat bezpečnost internetových sítí v ČR a globálního Internetu (27). Tj. zejména vyhodnocovat nahlášené kybernetické bezpečnostní incidenty a poskytnout podporu povinným subjektům při zvládání bezpečnostních incidentů. Poskytovatelé služeb elektronických komunikací, subjekty zajišťující síť elektronických komunikací a orgány či osoby zajišťující významnou síť jsou povinni hlásit kontaktní údaje CSIRT týmu (3). Přičemž orgány či osoby zajišťující významnou síť jsou dále povinny hlásit i kybernetické bezpečnostní incidenty (3).

4.3. Systém řízení bezpečnosti informací v kybernetické bezpečnosti

Kybernetická bezpečnost definovaná v ZKB a příslušné VKB vychází z ISMS a je obdobně založena na cyklu PDCA. Správci IS KII, KS KII a VIS jsou povinni implementovat ISMS definovaný ve VKB a dále provádět povinná bezpečnostní opatření. Jak mají systém implementovat, je definováno ve VKB (4). Ta se stává v tomto ohledu jakousi metodikou. Bezpečnostní opatření jsou ve VKB (na rozdíl od ISO/IEC 27002:2013) striktně rozdělena na opatření organizačního charakteru a na opatření technického charakteru (4,14). Základní koncept ISMS dle sady norem ISO/IEC 27000, však zůstává základním východiskem pro implementaci ISMS v kybernetické bezpečnosti (10). Z této normy přímo požadavky definované ve VKB vychází, avšak nepřebírají požadavky normy v plném rozsahu (11). Minimální znalost ISO/IEC 27000 významně usnadňuje orientaci v problematice ZKB a příslušné VKB.

Jádro bezpečnostních opatření ve VKB (obdobně jako v sadě norem ISO/IEC 27000) tvoří samotný ISMS (4). Dle VKB jsou ISMS povinni implementovat v plném rozsahu dle této VKB správci IS KII a KS KII (4). Ti jsou povinni v rámci ISMS dle VKB § 3 odst. 1 písm. a) – i) zajistit (4):

- ustanovení rozsahu ISMS;
- řízení rizik;
- vytvoření a schválení bezpečnostní politiky;
- monitorování účinnosti bezpečnostních opatření;
- vyhodnocování vhodnosti a účinnosti bezpečnostní politiky;
- zajištění provedení auditu kybernetické bezpečnosti min. 1x za rok;
- vyhodnocení účinnosti systému řízení bezpečnosti informací;

- aktualizaci systému řízení bezpečnosti informací a příslušné dokumentace na základě zjištění z auditů kybernetické bezpečnosti;
- řízení provozu a zdrojů systému řízení bezpečnosti informací;
- zaznamenávání činnosti spojené se systémem řízení bezpečnosti informací a řízením rizik.

Obdobně jako u ISMS dle sady norem ISO/IEC 27000, tyto aktivity probíhají ve všech etapách životního cyklu systému řízení (10). Nejdříve je v rámci plánování ISMS ustanoven rozsah, následně je provedena analýza rizik. V rámci etapy implementace a provozu jsou překlopena vybraná bezpečnostní opatření do bezpečnostní politiky. Všechny činnosti probíhající v rámci ISMS se evidují. Následně přichází etapa monitorování a přezkoumávání zavedeného ISMS, kde je účinnost zavedených bezpečnostních opatření monitorována. Vyhodnocuje se vhodnost a účinnost bezpečnostní politiky, provádí se audity a vyhodnocuje se celková účinnost ISMS. Celý cyklus je zakončen údržbou a zlepšováním ISMS, kdy se aktualizuje stávající ISMS a příslušná dokumentace dle konkrétních zjištění z auditů.

Správci VIS mají taktéž povinnost zavádět ISMS, avšak rozsah povinností je pro ně menší (4). Dle VKB § 3 odst. 2 písm. a) – c) jsou povinni zajistit (4):

- řízení rizik;
- vytvoření a schválení bezpečnostní politiky;
- provádění aktualizace definovaných výstupních dokumentů ISMS v souvislosti s prováděnými či plánovanými změnami.

Každá fáze cyklu PDCA má ve VKB jasně definované výstupy. Ty jsou vyjmenovány ve VKB v § 28, kde pro správce IS KII a KS KII je dle odst. 1 písm. a) – k) uveden povinný obsah bezpečnostní dokumentace (4). Pro každou fázi, existuje ve VKB povinný výstup (4):

- **plánuj**
  - přehled právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků;
  - metodika pro identifikaci a hodnocení aktiv a rizik;
  - zpráva o hodnocení aktiv a rizik;
  - prohlášení o aplikovatelnosti;
- **dělej**
  - plán zvládání rizik;
  - bezpečnostní politika;

- plán rozvoje bezpečnostního povědomí;
- zvládání kybernetických bezpečnostních incidentů;
- strategie řízení kontinuity činností;

- **kontroluj**
  - zprávy z přezkoumání systému řízení bezpečnosti informací;
  - zprávy z auditu kybernetické bezpečnosti.

Pro správce VIS je ve VKB § 28 odst. 2 písm. a) – i) stanovený následující povinný obsah bezpečnostní dokumentace (4):

- **plánuj**
  - metodika pro identifikaci a hodnocení aktiv a rizik;
  - zpráva o hodnocení aktiv a rizik;
  - přehled právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků;
  - prohlášení o aplikovatelnosti;
- **dělej**
  - plán zvládání rizik;
  - bezpečnostní politika;
  - plán rozvoje bezpečnostního povědomí;
  - zvládání kybernetických bezpečnostních incidentů;
  - strategie řízení kontinuity činností.

Protože VKB správcům VIS neukládá povinnost provádět audity kybernetické bezpečnosti pravidelně (minimálně jedenkrát ročně), nedefinuje také povinnost zpracovávat zprávy z přezkoumání ISMS a z auditu kybernetické bezpečnosti (4). Nicméně neznamená to, že by přezkoumání neměla být prováděna vůbec, a že by neměly o přezkoumání existovat záznamy. VKB to opět pouze jasně výslovně neukládá, neboť nároky na správce VIS by měly být méně administrativně a finančně náročné, než pro správce KII.

I tak si můžeme všimnout, že oproti ISMS dle ISO/IEC 27000 v kybernetické bezpečnosti některé dokumenty odpadají. Příkladem mohou být „Prohlášení o politice ISMS“ či „Ustanovení rozsahu ISMS“. Ačkoli mají správci IS KII a KS KII povinnost stanovit rozsah, nemusí zpracovávat přímo rozhodnutí o stanovení rozsahu ISMS, které by muselo být schváleno na vrcholové úrovni. Dohodnutý rozsah je však patrný z analýzy rizik a taktéž může být uveden přímo

v metodice pro identifikaci a ohodnocení aktiv a rizik, která aktiva budou do analýzy zahrnuta a která již nikoliv.

4.4. Bezpečnostní role

V návaznosti na řízení ISMS a cyklus PDCA jsou ve VKB § 6 odst. 1 a 2 definovány požadavky na organizační bezpečnost (4). Zajištění organizační bezpečnosti je jedním z velmi důležitých organizačních opatření stanovených VKB v § 6, které ukládá správcům IS KII a KS KII ustanovit bezpečnostní role, jejich práva a povinnosti (4). Pro zajištění ISMS ukládá VKB v § 6 odst. 1 ustanovit výbor pro řízení kybernetické bezpečnosti a dále dle § 6 odst. 2 písm. a) - d) garanty aktiv, manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a auditora kybernetické bezpečnosti (4). Takto definovaná organizace řízení zajišťuje řízení ISMS na všech řídících úrovních organizace, od strategické až po operativní.

Hlavní činností výboru pro kybernetickou bezpečnost je řídit kybernetickou bezpečnost na strategické úrovni. Výbor zodpovídá za celkové řízení a rozvoj IS KII, KS KII či VIS a obvykle je tvořen zástupci z vrcholového a středního managementu a zároveň zástupci z IT a oblasti bezpečnosti (28 s. 4). VKB přímo neukládá složení výboru, nicméně je dobré se řídit právě dle sady norem ISO/IEC 27000, kde je nejvyšším orgánem pro řízení ISMS vrcholové vedení organizace, které schvaluje, podporuje a vydává prohlášení (5 s. 129). Dále zde bývá rada pro bezpečnost informací jako nejvyšší orgán pro oblast řízení bezpečnosti informací a také tým pro plánování bezpečnosti informací, jež zodpovídá za ustanovení a implementaci ISMS (5 s. 129).

VKB dále definuje v § 6 odst. 2 písm. a) roli manažera kybernetické bezpečnosti (4). Manažerem kybernetické bezpečnosti je osoba, která odpovídá za celý systém řízení kybernetické bezpečnosti v organizaci, je pro tuto činnost vyškolena a zároveň disponuje praxí v této oblasti (min. 3 roky) (28 s. 4). Svou činností působí na taktické úrovni řízení a je jakousi spojkou mezi operativní a strategickou úrovní řízení (28 s. 4). Mezi jeho hlavní činnost patří zejména prosazování bezpečnosti informací v organizaci, koordinace realizace stanovených bezpečnostních politik a bezpečnostních opatření, projektová činnost, reportování a informování výboru, monitorování výkonnosti stanoveného ISMS a účinnosti zavedených bezpečnostních opatření, příprava podkladů pro přezkoumání ISMS (28 s. 5).

Další bezpečnostní rolí definovanou VKB v § 6 odst. 2 písm. b) je architekt kybernetické bezpečnosti (4). Ten má za úkol navrhnout a implementovat bezpečnostní opatření a stejně tak jako tomu bylo u manažera, musí být pro tuto činnost vyškolen a musí prokázat odbornou způsobilost praxí s navrhováním bezpečné architektury (min 3 roky) (28 s. 5). Architektů kybernetické bezpečnosti může být v organizaci samozřejmě více, neboť úkolem je zajistit bezpečnou archi-

tekturu od fyzické infrastruktury až po aplikační úroveň, což v praxi vyžaduje různé specializace, které nemusí pokrýt jediný pracovník (28 s. 5).

Nestrannou entitu zde tvoří bezpečnostní role dle § 6 odst. 2 písm. c) auditor kybernetické bezpečnosti, který musí být funkčně oddělen od ostatních rolí a opět platí, že tato osoba musí být pro tuto činnost vyškolena a musí prokázat odbornou způsobilost praxí s prováděním auditů kybernetické bezpečnosti (min. 3 roky) (28 s. 5). Ten na základě přezkoumání dává zpětnou vazbu k zavedenému ISMS. Je odpovědný za plánování a provádění interních auditů kybernetické bezpečnosti, a to zejména hodnocením míry souladu zavedeného ISMS a realizovaných bezpečnostních opatření s definovanými požadavky, stanovenými bezpečnostními politikami a dále regulacemi ZKB a VKB (28 s. 5). Vydává závěrečnou zprávu z auditu, která poskytuje nezávislou zpětnou vazbu o fungování ISMS a zavedených bezpečnostních opatřeních (28 s. 5).

Poslední bezpečnostní rolí definovanou VKB, která působí na operativní úrovni je garant aktiva. Ten je ustanoven v § 6 odst. 2 písm. d) a odpovídá za rozvoj, použití a bezpečnost aktiv, které vlastní (28 s. 6). Tuto roli, na rozdíl od manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti a auditora kybernetické bezpečnosti nelze outsourcovat. Taktéž neexistují požadavky na jeho kvalifikaci.

Z definovaných bezpečnostních rolí je tedy patrné, že pro zastávání těchto rolí (manažer, architekt či auditor) musí uchazeč disponovat určitou délkou praxe. Není tak možné, aby se role ujal čerstvý absolvent magisterského oboru v bezpečnosti ICT. V současné době, kdy je však nedostatek odborníků na oblast bezpečnosti ICT na trhu práce, se nejčastěji tyto bezpečnostní role outsourcují, případně se definované nároky na uchazeče zmírňují. Čerství absolventi studia mohou být minimálně součástí týmu specialistů, kteří kybernetickou bezpečnost řeší. Mohou participovat na zavádění bezpečnostních opatření v organizaci, jenž je povinným subjektem či jeho dodavatelem. V praxi se tak tito pracovníci mohou setkat s požadavky na znalosti ZKB, příslušné prováděcí VKB a navazujících předpisů.

4.5. Oblasti bezpečnostních opatření

Obdobně jako v sadě norem ISO/IEC 27000, jsou i v ZKB a příslušné prováděcí VKB definována bezpečnostní opatření. Minimální rozsah bezpečnostních opatření, které však musí povinný subjekt implementovat, je dán přímo VKB. Tato bezpečnostní opatření musí být náležitě zdokumentována v bezpečnostní dokumentaci. V případě, že povinný subjekt dané bezpečnostní opatření neimplementoval (např. není povoleno používání mobilních zařízení), musí tuto výjimku v bezpečnostní dokumentaci náležitě odůvodnit. Stěžejní činností v rámci ISMS je stejně jako v ISO/IEC 27000 řízení rizik. Na základě výsledků z analýzy rizik, musí být vytvořena

a schválena bezpečnostní politika. Ta obsahuje hlavní zásady, pravidla, principy, práva a povinnosti v různých oblastech bezpečnostních opatření (3).

Bezpečnostní politika je specifikována pro jednotlivé oblasti definované ve VKB § 5, kde pro správce IS KII a KS KII je dle odst. 1 písm. a) – u) tohoto paragrafu požadováno zavedení „Bezpečnostní politiky" v oblastech (4):

- *„systém řízení bezpečnosti informací,*
- *organizační bezpečnost,*
- *řízení vztahů s dodavateli,*
- *klasifikace aktiv,*
- *bezpečnost lidských zdrojů,*
- *řízení provozu a komunikací,*
- *řízení přístupu,*
- *bezpečné chování uživatelů,*
- *zálohování a obnova,*
- *bezpečné předávání a výměna informací,*
- *řízení technických zranitelností,*
- *bezpečné používání mobilních zařízení,*
- *poskytování a nabývání licencí programového vybavení a informací,*
- *dlouhodobé ukládání a archivace informací,*
- *ochrana osobních údajů,*
- *fyzická bezpečnost,*
- *bezpečnost komunikační sítě,*
- *ochrana před škodlivým kódem,*
- *nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí,*
- *využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí,*
- *používání kryptografické ochrany."*

Správci VIS mají opět oblasti, ve kterých jsou povinni zavádět příslušná bezpečnostní opatření, zúžené. Dle VKB v § 5 odst. 2 písm. a) – n) jsou povinni stanovit „Bezpečnostní politiku" pouze v oblastech (4):

- *„systém řízení bezpečnosti informací,*
- *organizační bezpečnost,*
- *řízení dodavatelů,*
- *klasifikace aktiv,*

- *bezpečnost lidských zdrojů,*
- *řízení provozu a komunikací,*
- *řízení přístupu,*
- *bezpečné chování uživatelů,*
- *zálohování a obnova,*
- *poskytování a nabývání licencí programového vybavení a informací,*
- *ochrana osobních údajů,*
- *používání kryptografické ochrany,*
- *ochrana před škodlivým kódem a*
- *nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí.“*

Z přehledu opatření je patrné, že většina bezpečnostních opatření byla převzata ze sady norem ISO/IEC 27000 (10). Některé oblasti opatření byly ve VKB vyděleny zvlášť do speciálních sekcí jako například ochrana osobních údajů či ochrana před škodlivým kódem. Nově vznikly požadavky související s oblastí opatření zaměřené na zvládání bezpečnostních incidentů, konkrétně nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí a používání nástroje pro sběr kybernetických bezpečnostních událostí. Tyto nové oblasti také reflektují současné požadavky na trhu práce.

Požadavky ZKB a související VKB kladou nové nároky na znalosti a dovednosti pracovníků nejen v oblasti bezpečnosti ICT, ale také na běžné pozice jako je například obchodník v oblasti ICT. Minimálně v tom smyslu, že pokud chtějí spolupracovat s povinnými subjekty, měli by se v problematice ZKB a související VKB orientovat. Na základě požadavků jako je detekce a vyhodnocování kybernetických bezpečnostních událostí a incidentů, ochrana před škodlivým kódem, řízení technických zranitelností a podobně, pak vzniká velká poptávka po pracovnících v oblasti bezpečnosti ICT, kteří disponují znalostmi a dovednostmi v těchto oblastech.

5. Bezpečnost ICT jako multidisciplinární obor

Bezpečnost ICT je velmi komplexní, rozsáhlá a dynamická disciplína, která se v posledních letech s rozvojem společnosti a zrychlením technologických inovací stala dominantním tématem v současném světě ICT. Vzrůstající potřeba digitální komunikace na celosvětové úrovni přinesla řadu změn a nových požadavků, a to nejen na poskytovatele internetového připojení, ale dopadá na každého, kdo přijde do styku s digitálním světem. Jedná se o problém vyžadující mezinárodní spolupráci a zapojení adekvátně kvalifikovaných odborníků, kteří budou schopni vnímat a respektovat mnohdy i diametrální rozdíly v zastávaných kulturních hodnotách jednotlivých států. Celosvětovým cílem je vychovat tyto odborníky a vnést do kyberprostoru etiku a základní práva a principy, jež jsou nám známy z reálného světa.

Cílem kapitoly je:

- poukázat na potřebu multidisciplinárního přístupu ve vzdělávání odborníků na bezpečnost ICT.

K tomu je zapotřebí identifikovat veškeré potřebné okruhy znalostí a dovedností pracovníků v oblasti bezpečnosti ICT. Pracovníci v oblasti bezpečnosti ICT by dle existujících doporučení měli v první řadě disponovat znalostmi výpočetní techniky, výpočetních věd, informačních systémů, bezpečnosti a softwarového inženýrství (1). Dále také znalostmi a dovednostmi z oblasti managementu, obchodní administrativy, etiky, sociologie, politických věd, práva, ale také například specifickými znalostmi zejména z oblasti e-commerce[24] (1). Z toho jednoznačně vyplývá, že **bezpečnost ICT je multidisciplinární obor**, což implikuje i samotná povaha kyberprostoru. Ten je velmi rozsáhlý a prochází napříč hranicemi jednotlivých států s rozdílnými právními systémy a s rozdílným systémem hodnot. Dosavadní absence základních práv a principů, které by byly unifikované napříč všemi státy, dává prostor kriminalitě. Dnes často označované jako kybernetická kriminalita či také kybernalita[25].

Již samotné studium kybernality je rozsáhlá mezioborová disciplína, která vyžaduje nejen technologické znalosti, ale také znalosti z oblasti práva a policejní praxe (29 s. 26). Jen k jejímu odhalení je třeba velmi sofistikovaných nástrojů, znalostí, postupů a odborníků mnoha oborů. Vysoce kvalifikovaní pracovníci se znalostmi z více oborů se však v praxi hledají velmi obtížně, a to platí nejen pro oblast kybernetické kriminality, ale pro bezpečnost ICT obecně. Obdobně,

[24] Pojem e-commerce je v praxi běžně používaný termín pro elektronické obchodování. Jedná se zejména o internetové obchody, on-line marketing, booking, apod.

[25] *„Kybernalitou rozumíme takovou činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti.“* (29 s. 19)

jako je tomu v reálném světě, i ke kybernalitě se pojí hospodářská kriminalita. Ta se odehrává v nepřehledném a neviditelném kyberprostoru, a tak napáchaná škoda nemusí být ihned patrná.

K tomu nutno dodat, že motivace útočníků může být různá. Některé útoky mohou být vedeny záměrně s přímým cílem obohatit se a způsobit oběti útoku vysoké finanční ztráty, jinde jsou vysoké finanční ztráty vedlejším efektem útoku. Příkladem může být odchod velkého počtu zákazníků vlivem ztráty důvěrnosti vůči prodejci, u kterého bylo zjištěno, že si databázi zákazníků odnesl bývalý zaměstnanec. Kolikrát i zdánlivě menší narušení bezpečnosti, může společnostem způsobit obrovské finanční ztráty. Dle globální analýzy, kterou zveřejnil americký institut Ponemon v červnu roku 2016, se pohybovaly celkové náklady plynoucí z narušení bezpečnosti za uplynulý rok okolo 4 miliónů dolarů, což byl 29% nárůst oproti zjištění z roku 2013.[26] Je tedy pochopitelné, že se téma bezpečnosti ICT stává být v okruhu odborníků více diskutovaným.

Pro boj proti kybernalitě a páchání trestné činnosti s pomocí technických a technologických prostředků je nezbytné vychovat odborníky, kteří budou schopni vnímat souvislosti mezi kyberprostorem a reálným světem, a jež budou schopni řešit problémy nejen za pomoci svých znalostí z oblasti bezpečnosti ICT a výpočetních věd, ale také za pomoci znalostí z oborů, jako je právo, finance a účetnictví, management, sociologie, politologie a etika (29). Je zcela jasné, že nelze vychovat jednoho univerzálního pracovníka, ale pro rozvoj kvalitního vzdělávání v oblasti bezpečnosti ICT je nezbytné, aby komplexní vzdělávací programy poskytovaly komplexní pohled na tuto problematiku.

Zejména vhodné se jeví zakomponování etických principů[27] do výuky technických předmětů, kdy studenti často přichází do styku s metodami možných útoků, s tvorbou a generováním škodlivých kódů, apod., a to bez základního etického povědomí (29). Přitom již z historie jsou známé případy, kdy bývalí studenti byli iniciátoři útoků na bankovní instituce – viz. kap. 6. – „Vývoj bezpečnosti ICT“. Mezi základní principy etiky ve spojení s ICT technologiemi však patří také principy ochrany intelektuálního vlastnictví (licenční práva a politiky), ale také ochrana soukromí (32). Ta je aktuálně silně spojována s bezpečností ICT. S účinností GDPR, budou organizace dle tohoto nařízení jakkoli zpracovávající osobní údaje, nuceni přijmout adekvátní

[26] Analýza byla provedena za finanční podpory společnosti IBM a zúčastnilo se jí 383 společností z 12 zemí: Spojené státy americké, Velká Británie, Německo, Austrálie, Francie, Brazílie, Japonsko, Itálie, Indie, Spojené arabské emiráty, Saudská Arábie, Kanada a Jižní Afrika (31).

[27] Snaha propojit výuku etiky se světem ICT technologií se objevila například na univerzitě George Mason University. O cílech a náplni pilotního kurzu pojednává článek Anne Marchant (32).

bezpečnostní opatření (2). V důsledku toho, lze očekávat větší důraz na dodržování principů etiky v prostředí ICT.

Sankce za případné nedodržení nařízení GDPR jsou totiž dle čl. 83 tohoto nařízení značně vysoké (2). K tomu lze přičíst obrovský tlak na ochranu osobních údajů[28] ze strany veřejnosti a v důsledku toho velmi negativní obraz společnosti, u níž k úniku osobních údajů došlo. Za osobní údaj navíc budou považovány i údaje jako IP adresa, fotografie či e-mail, neboli údaje se kterými dennodenně přichází do styku téměř každá organizace. Nejenže pro každé zpracování osobních údajů bude muset organizace dokládat oprávnění, na jehož základě může tyto údaje zpracovávat (čl. 6 odst. 1 nařízení GDPR), ale musí zajistit také možnost výmazu těchto údajů, jakmile si o to subjekt údajů zažádá (čl. 17 odst. 1 písm. b) a c) nařízení GDPR) či pomine-li platnost takového oprávnění (čl. 17 odst. 1 písm. a) nařízení GDPR) (2).

Tyto základní principy ochrany soukromí tak kladou nové nároky na organizace a jejich znalosti a také přímo na fungování IT oddělení a na používané technologie. Bez znalostí základních etických principů se organizace vystavují značným rizikům a vysokým sankcím. Stejně tak bez základních znalostí právních předpisů a rámců. Je na samotné organizaci, jak k integraci těchto znalostí přistoupí. Nicméně je zřejmé, že integrace těchto znalostí vyžaduje spolupráci odborníků napříč různými obory.

[28] Dle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů § 4 písm. a) je *„osobním údajem jakákoliv informace týkající se určeného nebo určitelného subjektu údajů“* (33). Dle čl. 4 odst. 1 nařízení GDPR se jedná o údaje, na základě nichž, lze přímo či nepřímo pomocí určitého identifikátoru (jméno, lokační údaje, síťový identifikátor, aj.) identifikovat fyzickou osobu (2).

6. Vývoj bezpečnosti ICT

„Jsme přesvědčeni, že data jsou fenoménem dnešní doby. Je to nový přírodní zdroj světa. Je to nový základ konkurenční výhody, jež transformuje každou profesi a průmysl. Pokud je toto tvrzení pravdivé, pak je počítačová kriminalita, dle definice, největší hrozbou pro každou profesi, každé průmyslové odvětví a každou firmu na světě.“[29] (34)

„We believe that data is the phenomenon of our time. It is the world´s new natural resource. It is the new basis of competitive advantage, and it is transforming every profession and industry. If all of this is true – even inevitable – then cyber crime, by definition, is the greatest threat to every profession, every industry, every company in the world.“ (34)

Cílem kapitoly je:

- poskytnout přehled událostí, které vedly k rozvoji bezpečnosti ICT;
- poskytnout přehled o historii normativů v oblasti bezpečnosti ICT;
- poskytnout přehled o historii legislativy ČR v souvislosti s bezpečností ICT.

Bezpečnost informací existuje již od pradávna. Již naši předci skrývali svá tajemství a snažili se zachovat jejich důvěrnost zpravidla tím, že začali používat jednoduchou substituci znaků. S postupem času vznikl nový vědní obor zvaný kryptografie, jež zkoumá různé metody šifrování zpráv (35). Analýza těchto textů, kryptoanalýza, hrála velmi důležitou roli několikrát v historii lidstva. Například ve druhé světové válce, kdy se britští analytici pod vedením Alana Turinga snažili prolomit kód šifrovacího stroje Enigma, jež používali Němci pro utajenou komunikaci o plánovaných vojenských aktivitách (35). S rozvojem výpočetní techniky a následně i informačních systémů, potřeba ochrany informací rostla. Informace v digitální podobě mohly být nejen „vyzrazeny“, ale začaly vyžadovat také ochranu z pohledu jejich integrity a dostupnosti.

Když vznikl v 70. letech minulého století Internet (tehdy ARPANET), těžko by si někdo mohl představit, jak významnou transformaci přinese v následujících letech a v budoucím století (36). Byl postaven základní stavební kámen globální informační infrastruktury, jež umožňuje rozsáhlou interakci napříč celým světem bez ohledu na geologickou lokaci a přináší tak doposud neznámé příležitosti. ARPANET byl zpočátku používán pro armádní účely a přístup k němu měli pouze oprávnění jedinci. Avšak postupně došlo k rozšíření Internetu zprvu na akademickou

[29] Tuto řeč pronesla Ginny Rometty, předsedkyně představenstva, prezidentka a CEO společnosti IBM, na pravidelně pořádaném Security Summitu v New Yorku v listopadu roku 2015, před publikem tvořeným zejména vrcholovými manažery (34).

půdu (36). V listopadu roku 1991 proběhly i na akademické půdě ČR první pokusy o připojení do rakouského národního uzlu EARN v Linci (36). Teprve dne 13.2.1992 proběhlo slavnostní a oficiální připojení ČR do Internetu na Českém vysokém učení technickém v Praze (ČVUT), teprve potom následovalo budování celorepublikové páteřní sítě (36).

Neoprávněné zneužití technického prostředku ve prospěch útočníka je však zaznamenáno již před samotným vznikem Internetu. **Hacking**[30] se dostává do povědomí již na přelomu šedesátých a sedmdesátých let, kdy John Draper (známý jako „Captain Crunch“) se svou skupinou využil tehdejší nedokonalosti telefonní sítě a umožnil zdarma dálkové telefonní hovory pomocí jednoduchého oklamání přepojovacího mechanizmu dětskou píšťalkou (29 s. 48). Tato skupina pořádala skrz telefonní sítě dlouhé telefonní hovory o několika účastnících a ve svých technikách se postupně zdokonalovala (29 s. 48). Vytěžování telefonní linek však přineslo obrovské riziko toho, že linky používané v nouzových situacích budou nedostupné, což vyvolalo dokonce zásah FBI (29 s. 48). Tak začalo být významně vnímáno riziko potencionálního zneužití technických prostředků pro úmyslné páchání trestné činnosti.

S rozšířením výpočetní techniky se další hackerské techniky soustředily na prolamování hesel, tzv. „brute force“ útoky (útoky hrubou sílou) založené nejprve na hádání hesel, kdy veškeré kompromitované přístupové údaje byly sdíleny napříč celou komunitou[31] (29 s. 48). Teprve díky vzniku Internetu známe pojem počítačový virus. V roce 1988 internetový červ „Worm“ vypuštěný Robertem Morrisem nakazil něco okolo 6000 počítačů (29 s. 29). Ve stejném roce se počítačová kriminalita objevila poprvé v bankovním sektoru, kdy se Národní banka v Chicagu stala první obětí počítačové kriminality (29 s. 49). V roce 1995 následoval další bankovní útok ruských studentů, kteří si na svá konta převedli 10 miliónů dolarů (29 s. 49). Hackerské techniky se dále používaly pro útoky na významné vládní instituce v USA a s postupem času začaly být používány také jako jeden z dalších nástrojů konkurenčního boje.

Od počátku 90. let začal Internet pronikat z velkých organizací a významných institucí k obyčejným uživatelům (36). Do té doby byli hackeři[32] obvykle studenti, kteří měli přístup

---

[30] Někdy také používaný jako crack/cracking, je termín pro podařené, originální, rychlé a jednoduché řešení problému (29). Obvykle používán ve spojení s programováním.

[31] Sdílení kompromitovaných údajů známe dodnes, jen s tím rozdílem, že v dnešní době bývají poskytovány ostatním za úplatu skrz tomu určené prostředí, tzv. dark web. Někdy také označovaný jako deep web. Je termín pro všechny webové stránky, které nejsou dostupné z klasických vyhledávačů, ale pouze za pomoci speciálního software (37). Tyto stránky mívají ilegální obsah a uživatel si zde může zakoupit ilegální zboží či služby.

[32] Označení hacker se dnes často (a ne zcela přesně) používá i pro útočníky, kteří páchají trestnou činnost v rámci kyberprostoru. Toto označení však není zcela správné. Hacker je dle „Výkladového slovníku

v rámci svého působení na univerzitách k Internetu (29 s. 49). Označení hacker v té době znamenalo, že je daný jedinec skutečný odborník a není tedy divu, že většina těchto hackerů se později stala řediteli velkých firem v oblasti informačních a komunikačních technologií (například Steve Jobs, Bill Gates, ale také slavný Kevin Mitnick) (29 s. 49). Ve chvíli, kdy se Internet otevřel světu, postupně nastala digitální transformace, jež přenesla každodenní interakce do virtuálního světa, jehož hlubiny jsou dodnes neprobádané a mohou představovat velké riziko.

Paralelně s rozšířením Internetu vzniká nová vědní disciplína, počítačová bezpečnost, které se nejprve věnovaly zejména silové resorty a teprve později se disciplína přenesla do komerčního prostředí (38 s. 16). Teprve později s integrací technologií do procesů organizací a státních institucí se rozšiřuje pojem kybernetická bezpečnost. Rozvoj těchto disciplín je dodnes neustále stimulován hackery, jejichž stále více sofistikované metody vyvíjejí tlak na zlepšování bezpečnosti ICT prostředí. Dále vznikala různá odborná sdružení. V roce 1993 vznikla v ČR Asociace firem pro ochranu dat a informací (AFOI) a poté také první pobočka významné mezinárodní organizace Information Systems Audit and Control Asociation (ISACA) (38 s. 16). Začínají se také konat první odborné konference a koncem roku 1996 začíná vycházet odborný časopis Data Security Management (DMS), který pravidelně vychází dodnes (38 s.16).

6.1. Historie normalizace bezpečnosti ICT

První snahy o normalizaci počítačové bezpečnosti se objevily v 80. letech minulého století. Avšak první dokumenty se zaměřovaly spíše na řízení bezpečnosti informačních systémů a informačních technologií, teprve později se normalizace ubírá směrem k řízení celé bezpečnosti informací (5 s. 64). Vůbec jako první vzniká ve Spojených státech amerických (USA) v roce 1983 doporučení koncipované pro vojenské prostředí **TCSEC** nazývané jako „Oranžová kniha“ (Orange book), které bylo zmiňováno v kap. 2.1. – „Druhy bezpečnosti“ (5 s. 64). Toto doporučení je v roce 1985 uznáno jako norma Ministerstva obrany USA a tvoří základ pro sadu norem a doporučení nazývaných jako „Duhová série“ (Rainbow Series) (5 s. 64).

Dokument TCSEC definuje kritéria pro hodnocení bezpečnosti výpočetních systémů. Slouží jako základ pro měření účinnosti bezpečnostních kontrol zabudovaných do systémů pro automatické zpracování dat. Tato kritéria mají poskytnout uživatelům míru důvěryhodnosti počítačových systémů pro ukládání citlivých a utajovaných informací a výrobcům produktů návod,

---

kybernetické bezpečnosti“ osoba, která se zabývá hackingem zpravidla pro svou zvídavost a své sebezdokonalení (8 s. 49). Naopak Cracker je osoba, která zneužívá těchto metod a znalostí, aby páchala úmyslnou trestnou činnost (8 s. 49). Obdobnou definici uvádí Jirovský, který rozlišuje dva typy hackerů: hackera a crackera (8 s. 54).

jak samotnou důvěryhodnost zajistit (40 s. 8). Tímto vznikl normativní základ počítačové bezpečnosti. Dle této normy vychází počítačová bezpečnost z bezpečnostních požadavků kladených na výpočetní systémy, mezi něž patří vlastnosti jako: umožnění přístupu k informacím pouze oprávněným osobám, přidělení oprávnění těmto osobám pro čtení, zápis, výmaz či jakoukoli modifikaci informací v tomto systému (40 s. 9).

TCSEC dělí požadavky kladené na výpočetní systém na tři části (5 s. 66, 40 s. 10):

- **zásady** – definují způsoby řízení přístupů k datům a klasifikaci informací z hlediska jejich utajení;
- **odpovědnost** – část zaměřená na zjišťování zodpovědné entity za provedené akce/činnosti v rámci systému;
- **záruky** – část definující požadavky na bezpečnostní mechanismy HW/SW, které musí podat dostatečnou záruku, že si systém vynucuje splnění bezpečnostních zásad a principů odpovědnosti.

TCSEC dal normativní základ v oblasti bezpečnosti ICT. O něco později, v roce 1990, vznikla v Evropě norma nazývaná „Kritéria hodnocení bezpečnosti informačních systémů“ (ITSEC), jež byla na rozdíl od TCSEC vytvořena více obecně (5 s. 65). Kanada přibližně ve stejné době vydala vlastní „Kanadská kritéria hodnocení bezpečnosti počítačových produktů“ (CTCPEC) a americká norma byla v prosinci roku 1992 přepracována a vydána organizací NIST a NSA jako „Federální kritéria pro bezpečnost informačních technologií“ (FC) (5 s. 65). Po společných mezinárodních snahách a harmonizaci dosavadních kritérií byly nakonec vydány v polovině 90. let „Společná kritéria pro hodnocení bezpečnosti informačních technologií“ (CC) (5 s. 73). Ta byla přijata standardizačním úřadem ISO jako norma ISO/IEC 15408 (Evaluation criteria for IT security - Part 1: Introduction and general model) (41).

Tyto standardy však nebyly příliš praktické pro komerční prostředí, a tak byly zahájeny práce na tvorbě norem vycházejících z předchozích kritérií, které by byly použitelné pro řízení bezpečnosti informací v komerčním prostředí, a nejen pro odvětví informačních systémů a technologií, ale právě také i pro řízení bezpečnosti informací (5 s. 86). První publikace takové normy vznikla v roce 1995 ve Velké Británii, v roce 2000 byl první díl této normy schválen jako mezinárodní standard ISO/IEC 17799:2000 a v roce 2001 se stává součástí českých technických norem s označením ČSN ISO/IEC 17799:2001 (5 s. 87,42). Následně v roce 2005 organizace ISO ohlásila zavedení nové sady norem ISO/IEC 27000 věnující se problematice řízení bezpečnosti informací, která byla popsána v rámci kap. 3. – „Řízení bezpečnosti informací“ (5 s 90,10).

6.2. Vývoj národní kybernetické bezpečnosti a legislativy

Národní zabezpečení a ochrana kritické infrastruktury začala být intenzivněji diskutována po sérii teroristických útoků v USA 11. září roku 2001. V té době začala být vnímána potřeba ochrany národních informačních systémů, sítí a infrastruktury. V návaznosti na to, bylo v USA v roce 2002 založeno Ministerstvo vnitřní bezpečnosti (DHS) a v únoru roku 2003 byla vydána první verze „Národní strategie pro zabezpečení kyberprostoru“ (National Strategy to Secure Cyberspace) (43 s. 9). Cílem strategie bylo zajistit prevenci proti kybernetickým útokům vedeným proti kritické infrastruktuře státu, odstranit zranitelnosti a minimalizovat škody a čas potřebný k obnově kritické infrastruktury (43 s. 8). Právě zde vznikla myšlenka vytvořit národní systém reakce na kybernetické bezpečnostní incidenty a tím přispět k zajištění bezpečného kyberprostoru na celosvětové úrovni (43 s. 10).

V ČR došlo k rozvoji národní kybernetické bezpečnosti a ochrany kritické infrastruktury o něco později. První „Národní strategie kybernetické bezpečnosti České republiky období 2012 až 2015“ byla vydána v roce 2012 (44). A v roce 2014 následovalo vydání ZKB reflektující tuto problematiku a navazující VKB (3,4). V roce 2015 následovalo vydání nové národní strategie (45). Právě nová strategie zmiňuje zásadní vizi a tou je rozšíření expertní základny v oblasti kybernetické bezpečnosti a spolupráce se subjekty ze soukromé a akademické sféry na výzkumu a vývoji v oblasti ICT (45). ČR dle této strategie navyšuje investice do výzkumu a vývoje v oblasti kybernetické bezpečnosti, ale také do vzdělání (45). Nedostatek odborníků v této oblasti a nutnost revize stávajících studijních programů je jednou z mnoha výzev uvedených v tomto dokumentu.

6.2.1. Legislativa ČR

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)[33] navazuje na zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů[34], který definuje kritickou informační infrastrukturu a definuje základní požadavky na řešení krizových situací při narušení bezpečnosti kritické infrastruktury státu (3,21). Konkrétní návaznosti byly popsány v kap. 4. – „Řízení kybernetické bezpečnosti“. ZKB a pří-

[33] ZKB

[34] ZKŘ

slušná prováděcí VKB[35] dále konkretizují požadavky na ochranu kritické infrastruktury státu v kyberprostoru (3,4). ZKB přineslo poprvé v historii ucelený pohled na kybernetickou bezpečnost ve státním sektoru ČR.

Na úrovni evropských států byly tyto snahy o sjednocení pohledu na kybernetickou bezpečnost a legislativy na celoevropské úrovni od roku 2013. Snahou bylo vytvořit jednotný právní předpis pro úpravu kyberprostoru, což nakonec vyvrcholilo vydáním směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS) (46). Jedná se o první regulaci, která komplexně pokrývá problematiku kybernetické bezpečnosti v EU a jejích členských státech. Na základě toho bylo NBÚ provedeno přenesení směrnice NIS do právního řádu ČR, a to vypracováním návrhu zákona, kterým se v budoucnu změní ZKB (47). Cílem směrnice je mimo jiné nastolit mezinárodní spolupráci v oblasti kybernetické bezpečnosti a uložit povinnost všem členským státům vytvořit a přijmout národní strategii pro bezpečnost sítí a informačních systémů, obdobně jako tomu bylo v USA a ČR (47).

V neposlední řadě nelze nezmínit souvislost mezi kybernetickou bezpečností a ochranou osobních údajů. První právní předpis věnující se problematice ochrany osobních údajů v ICT prostředí ČR byl zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech, který byl v roce 2000 zrušen a nahrazen zákonem č. 101/2000 Sb., o ochraně osobních údajů a změně některých zákonů (48,33). Ve stejném roce byl založen Úřad pro ochranu osobních údajů (ÚOOÚ) (49). Nový právní předpis přinesl razantní změnu podmínek zpracování osobních údajů a změny v odpovědnosti správců a zpracovatelů (49). Další velká změna je očekávána právě s účinností nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) známým jako GDPR (2). Některé zásadní změny byly zmíněny v kap. 5. – „Bezpečnost ICT jako multidisciplinární obor“.

S digitálním prostředím samozřejmě také souvisí řada dalších zákonů, zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, zákon č. 106/1999 Sb., o svobodném přístupu k informacím (50,51,52,53). Nicméně, rozbor těchto zákonů a vysvětlení souvislosti s bezpečností ICT je rozsahově nad rámec této práce.

[35] Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti zaměřující se na ochranu kritické informační a komunikační infrastruktury státu a významné informační systémy.

Je však důležité, aby studenti a absolventi VŠ v oblasti bezpečnosti ICT měli alespoň obecný přehled o těchto právních předpisech, jejich účelu a souvislosti s bezpečností ICT. Obdobně jako obecný přehled o událostech, jež vzniku těchto právních rámců předcházely.

7. Trendy v bezpečnosti ICT

O trendech v oblasti bezpečnosti ICT rozhoduje především vývoj společnosti, který je v posledních letech spjat s velkou mírou automatizace a digitalizace. Současný zvýšený zájem o bezpečnost lze mimo jiné přisuzovat i nástupu nové průmyslové revoluce tzv. „Průmyslu 4.0". Jedná se o koncept, který byl představen v Německu v roce 2013 jako jeden z národních projektů (54 s. 2). Česká republika na koncept zareagovala v roce 2015, kdy Ministerstvo průmyslu a obchodu ČR vydalo „Národní iniciativu Průmysl 4.0." (55). Koncept staví na technologických fenoménech dnešní doby jako je internet věcí (IoT), zpracování obrovského množství dat (Big data), počítačová simulace a virtualizace, cloud, 3D tisk, rozšířená realita a mnohé další. Jejich integrace do podnikových procesů sice přináší pro obchod a průmysl nové příležitosti[36], ale i zvýšené nároky na kybernetickou bezpečnost a potřebu multidisciplinárního přístupu (55 s. 8).

„Nestojíme na prahu čtvrté průmyslové revoluce, ona již totiž započala. Započala v nejrozvinutějších světových ekonomikách, sice pod různými názvy, ale vedena stejnou snahou, a to snahou o udržení a posílení konkurenceschopnosti a technologického prvenství těchto států na světových trzích. Jedná se o zcela novou filozofii přinášející celospolečenskou změnu a zasahující celou řadu oblastí od průmyslu, přes oblast technické standardizace, bezpečnosti, systému vzdělávání, právního rámce, vědy a výzkumu až po trh práce nebo sociální systém." (55 s. 6)

Cílem kapitoly je:

- poskytnout přehled současných trendů v bezpečnosti ICT.

Technologické inovace reflektující potřeby vývoje společnosti přináší každým rokem řadu trendů v oblasti bezpečnosti ICT. Pro každý rok vychází řada studií, které z různých analýz trhu predikují budoucí trendy. Pořádá se řada odborných konferencí na aktuální témata a problémy, vytváří se různorodé platformy pro sdílení znalostí a praktických řešení. V oblasti bezpečnosti nejsou aktuální trendy závislé pouze na potřebách široké veřejnosti, ale jsou ovlivňovány také politickou situací a dále nápaditostí a vynalézavostí samotných útočníků. Jejich útoky jsou postupem času sofistikovanější, složitější a propracovanější. Navíc velmi snadné sdílení a rozšiřování škodlivých skriptů prostřednictvím dark webů zvyšuje počet pokusů. Avšak právě díky neustálému „zbrojení" mezi útočníkem a obráncem dochází k průběžnému zdokonalování bezpečnostních mechanismů a technik na straně obránce.

[36] Koncept využívá nejmodernější technologie v procesech obchodu a průmyslu, což oproti běžnému způsobu fungování procesů přináší zejména možnost optimalizace výrobních procesů a produktů a také efektivitu zdrojů (55).

Tím, jak technologická úroveň zabezpečení stále roste, zaměřují se útoky více na zranitelnost, kterou nikdy nelze zcela eliminovat, a tou je sám člověk – uživatel. Nadále se ukazuje se, že nízkou počítačovou gramotností trpí nejen malé, ale i velké organizace. Tomu naznačuje současný trend útočníků, kdy v průběhu loňského roku 2016 nastala obrovská vlna výskytu ransomware[37] v dosavadní historii (56). Tato vlna stále trvá a predikce říkají, že potrvá ještě minimálně po celý rok 2017 (56). Ransomware útoky stále více cílí na organizace, o kterých se ví, že nemají dostatečné zabezpečení.[38] Příkladem může být útok na zdravotnické zařízení v Atlantě, kde se tento typ útoku objevil v sofistikovanější podobě, než která byla doposud známa (57).

V roce 2017 bude dle predikcí největším cílem zejména sektor zdravotnictví, kde je vlivem nedostatečného technického know how, absence bezpečnostního povědomí personálu, absencí politik a bezpečnostních mechanismů pravděpodobnost úspěšného útoku největší (56). K úspěšnosti přispívá i fakt, že zdravotnická zařízení svá data pro svou práci nezbytně potřebují, a tak jsou ochotna zaplatit požadované výkupné. Doposud navíc neexistovala ani dostatečná právní úprava, která by podobným organizacím nařídila, jak mají digitalizovaná data o svých klientech adekvátně chránit. To se však týká i poskytovatelů digitálních služeb, například poskytovatelů cloudu. Ti se stávají dalším vhodným cílem a téma zabezpečení cloudových služeb tak nabývá na významu. Situace by se však mohla s vydáním novely ZKB a s účinností GDPR v příštím roce změnit.

Ransomware bude v tomto roce představovat velký problém pravděpodobně i pro další sektory. Důvodem je nový model fungování tohoto zločinu, tzv. ransomware as a service (ransomware jako služba), což umožní i méně zdatným útočníkům napáchat poměrně rozsáhlé škody (56). Navíc se objevuje doposud neznámé chování tohoto programu, který se po napadení počítače zeptá uživatele, zda chce zaplatit výkupné, nebo dále rozšířit škodlivý kód výměnou za vrácení dat (56). Tím hrozí spuštění další velké vlny ransomware útoků, která se bude velmi rychle šířit. Budování bezpečnostního povědomí tak bude v organizacích nabývat na stále větším významu. Zvyšující se počet bezpečnostních incidentů bude vyžadovat více odborníků a specialistů v oblasti bezpečnosti ICT na straně obránce. Těch je však nedostatek, a tak lze očekávat mini-

---

[37] *„Program, který zašifruje data a nabízí jejich rozšifrování po zaplacení výkupného (např. virus, trojský kůň).“* (8 s. 83)

[38] Příkladem může být útok na zdravotnické zařízení v Atlantě, kde se tento typ útoku objevil v sofistikovanější podobě, než která byla doposud známa (57). Namísto toho, aby byla data o pacientech zašifrována, byla vyčištěna z databáze a uložena na nedůvěryhodný on-line server (57). Tím útočník předešel odborníky (zejména antivirové společnosti), kteří v současnosti vyvíjejí programy pro dešifrování kompromitovaných dat ransomwarem (58).

málně zvýšený zájem o automatizované analytické nástroje zaměřené na strojové učení (56). Jejich vývoj však vyžaduje taktéž velmi specifické znalosti a dovednosti odborníků.

V souvislosti s lidským pochybením a ransomware útoky je vhodné zmínit další trend, který neustává, ale naopak nabírá na síle a tím je phishing[39]. Velmi jednoduchý a v mnoha případech úspěšný. Navíc se v poslední době daří maskovat podvodné stránky a dotazy tak dobře, že jsou pro běžného uživatele k nerozeznání od originálu a tím vzbuzují naprostou důvěryhodnost. Vzrůstající trend naznačují i zveřejněné statistiky Národního CSIRTu České republiky, kde ani ne za první čtvrtletí roku 2017 evidují na 112 nahlášených phishingových útoků[40] v ČR (59). Přestože by se mohlo zdát, že je bezpečnost a bezpečné chování v kyberprostoru širokou veřejností více vnímána tím, že jsou častěji odhalovány a medializovány bezpečnostní incidenty, není tomu zcela pravda. To ostatně dokazují i zprávy o používání velmi triviálních přihlašovacích hesel, které usnadňují úspěšnost útoku typu brute force[41] (60).

Pokud se situace zásadně nezmění, lze očekávat i nadále cílené brute force útoky proti uživatelským a zejména administrátorským účtům. To dle predikcí povede dodavatele bezpečnostních řešení a poskytovatele cloudových řešení k novým metodám autentizace, které budou více sofistikovanější než pouhé přihlašování heslem (61). Trendem bude víceúrovňová autentizace, s níž se můžeme setkat u některých poskytovatelů již dnes (např. zasílání SMS s ověřovacím kódem), ale také využití biometrických údajů pro autentizaci uživatelů (61 s. 17). Nebude se však jednat pouze o otisky prstů, ale i o rozpoznávání obličeje, frekvence tlukotu srdce či sítnice oka (61 s.17). Pro odhalení různých útoků v zárodku, se budou čím dál častěji používat behaviorální analýzy pro detekci anomálií (61 s. 18). K tomu bude využíváno strojové učení pro predikci potencionálních útoků a schopnost zamezit útokům dříve, než napáchají rozsáhlé škody (61 s. 18).

---

[39] *„Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtů apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.). Vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat.“* (8 s. 70) Jedná se o jednu z možných forem sociálního inženýrství.

[40] Bezpečnostních incidentů však mohlo být ve skutečnosti podstatně více. Některé bezpečnostní incidenty nemusely být nahlášeny – například nebyly detekovány. Navíc ne každý subjekt je povinen bezpečnostní incident hlásit. Povinnost hlásit bezpečnostní incidenty vznikla osobám a orgánům provozujícím významnou síť, spravujícím významný informační systém a spravujícím kritické informační a komunikační systémy 1. ledna roku 2015 s účinností ZKB (3).

[41] Tzv. útoky hrubou silou.

Další hrozbou pro tento rok je razantní nárůst DDoS[42] útoků cílených na zařízení IoT (56). Jak již bylo zmíněno, Průmysl 4.0 se vyznačuje zejména integrací technologických fenoménů (jako je například právě IoT) do obchodních a výrobních procesů. Tím se tyto technologie stávají velmi lákavým cílem útoku, protože jedním z největších efektů nedostupnosti služby je zpravidla ztráta zisku. To bude klást důraz na témata jako je zajištění kontinuity činností a plánů obnovy, kde primárním cílem bude zachovat hlavní procesy organizace alespoň v nouzovém běhu a obnovit chod organizace v co možná nejkratším čase. Zařízení IoT jsou mimo jiné velmi náchylné na různé škodlivé kódy[43] (viry, červy, trojské koně, špionážní software, apod.). Je tedy velmi pravděpodobné, že se začnou objevovat nové typy útoků, které byly doposud neznámé. Lze tedy očekávat, že bezpečnost IoT se tak stane jedním z největších témat pro rok 2017.

Současný vývoj tlačí organizace ke zlepšení, a tak vznikají nové iniciativy z řad odborníků a organizací, kteří se bezpečnosti věnují. Například aliance Cloud Security Alliance v současné době pracuje na standardech, návodech a nejlepších praktikách pro řízení cloudových služeb (62). To samozřejmě přispěje ke zvýšení celkové důvěryhodnosti státní infrastruktury, avšak s rostoucí základnou znalostí rostou i požadavky na nové odborníky v oblasti bezpečnosti ICT. Tím se stále více prohlubuje krize nedostatku odborníků v této oblasti. Snaha o budování kompetencí by však neměla směřovat pouze ze stran velkých organizací, ale také ze stran státních institucí, neboť i v jejich zájmu by mělo být budování národního know how v oblasti bezpečnosti ICT. Zejména v období, kdy světem hýbou témata jako kyberterorismus[44] a kybernetická válka[45].

---

[42] *„Distribuované odmítnutí služby (Distributed denial of service) je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele, a to útokem mnoha koordinovaných útočníků.“* (8 s. 33)

[43] Často obecně označované jako malware (malicious software) (8 s. 99).

[44] *„Trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či neadekvátní reakci.“* (8 s. 59) Útok může být motivován cílem zastrašit či donutit vládu, popřípadě obyvatelstvo, jednat v souladu se sociálním či politickým záměrem (29 s. 130).

[45] Někdy také označována pojmem kybernetický warfare. Válka vedená v kyberprostoru znepřátelenými stranami, jenž v sobě spojuje kyberterorismus, sémantický útok a simulovanou válku (29 s. 162).

8. Situace na pracovním trhu v oblasti bezpečnosti ICT

Nové průmyslové revoluci lze jednoznačně přisuzovat vliv na organizaci práce, změny v náplni práce většiny profesí a také nové požadavky na znalosti a dovednosti pracovníků, a to napříč všemi odvětvími (55 s. 20). S nástupem Průmyslu 4.0 lze očekávat i zánik určitých profesí. Vlivem automatizace jsou ohroženy nízkokvalifikované pracovní pozice a dále také pracovní pozice, jejichž náplň práce je spojena s rutinní činností, jako je administrativa, jednoduché zpracování dat, atd. (55 s. 20). Méně ohroženy budou pracovní pozice, které vyžadují kupříkladu kreativitu, kritické myšlení, schopnost aktivního vyjednávání, sociální inteligenci, navazování vztahů se zákazníkem a vysokou specializaci neboli činnosti, jež není možné v současnosti plně nahradit umělou inteligencí (54 s. 20). Tím, že bezpečnost ICT je velmi komplexní disciplína lze očekávat, že tyto odborné pozice budou nejméně zasaženy (63).

Cílem kapitoly je:

- popsat současnou situaci na pracovním trhu v oblasti bezpečnosti ICT.

Digitální technologie přináší pro pracovní trh také nové příležitosti a profese. S turbulentním technologickým prostředím se požadavky na nové znalosti a dovednosti často a velmi rychle mění. Na to však není současný proces vzdělávání dostatečně připraven, a tak kvalita nabídky mnohdy neodpovídá skutečným požadavkům trhu. Národní iniciativa Průmyslu 4.0 zmiňuje důležitost podpory technických oborů z několika důvodů. Tím primárním důvodem je, že je více studentů a absolventů v humanitně zaměřených oborech, což nereflektuje potřeby strategických odvětví ČR (55 s. 24). Dalším důvodem je fakt, že studium technických oborů dává na rozdíl od těch humanitních velmi dobrý znalostní základ pro mnoho pracovních příležitostí v různých disciplinárních oborech (55 s. 24). Absolventi jsou tak v praxi vícero uplatnitelní.

Pracovní trh se nyní navíc potýká s nedostatkem kvalifikované pracovní síly pro oblast bezpečnosti ICT a s největší pravděpodobností se tato krize bude i nadále prohlubovat. Předpokládá se, že v roce 2022 bude v oblasti bezpečnosti chybět až 1,8 miliónů odborníků (64). Problém je o to komplexnější, neboť nastupuje nová tzv. generace Y, jež se vyznačuje oproti předešlé generaci X velkou diverzitou a je pro ni typické častěji měnit zaměstnání (64). To klade nové nároky na zaměstnavatele. Aby byli schopni reagovat na tento nový trend, měli by umožňovat především práci na dálku, více podpořit trainingové programy a možnost certifikací, zaměřit se na atraktivitu projektů a celkově nastavit flexibilnější pracovní podmínky (například možnost jednorázové práce na určité časové období) (64).

V ČR je pracovní trh v ICT sektoru vymezen dle standardu „Klasifikace ekonomických činností“ (CZ-NACE) (65). Zde je ICT sektor definován jako *„kombinace ekonomických činností produkujících výrobky a poskytující služby, jež jsou primárně určeny ke zpracování, komunikaci*

a distribuci informací elektronickou cestou, včetně jejich zachycení, ukládání, přenosu a zobrazení.“ (66) Ekonomické činnosti spadající do ICT sektoru jsou vymezeny dle klasifikace do čtyř hlavních skupin ICT činností výroba ICT (ICT průmysl), obchod s ICT, telekomunikace[46] a IT služby (65).

Počet aktivních subjektů v ICT sektoru a jejich podíl na celkovém podnikatelském sektoru uvádí Tab. 1. Zde je patrný pozvolný kontinuální růst tohoto sektoru v posledních letech, nicméně celkový podíl na podnikatelském sektoru pozvolna narůstá až od roku 2012. Celkový nárůst od roku 2012 až 2015 dosáhl hodnoty 0,3 %.

	2007	**2008**	**2009**	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Celkem	30 554	29 931	31 259	32 315	32 657	32 789	32 876	33 931	35 182
Podle skupin činností definovaných dle CZ-NACE									
ICT průmysl	2 886	2 600	2 663	2 702	2 610	2 520	2 457	2 388	2 348
ICT obchod	1 675	1 618	1 735	1 854	1 925	2 080	2 258	2 459	2 275
Telco	1 210	828	868	888	902	885	954	1 010	1 063
IT služby	24 773	24 885	25 993	26 871	27 220	27 304	27 207	28 074	29 496
% podíl v ČR	**3**	**2,9**	**2,9**	**2,9**	**2,8**	**2,8**	**2,9**	**3**	**3,1**

Tab. 1: Počet subjektů v sektoru ICT dle klasifikace CZ-NACE v letech 2007-2015 a jejich podíl na celkovém podnikatelském sektoru (65)

Výrazný rozvoj ICT sektoru lze zaznamenat na nárůstu zaměstnaných osob v tomto sektoru (viz. Tab. 2). Podíl zaměstnaných osob v sektoru ICT na celkovém počtu zaměstnaných osob v podnikatelském sektoru kontinuálně rostl v průběhu posledních let a od roku 2009 do roku 2015 došlo k celkovému nárůstu o 0,2 %. Nejsilněji roste skupina IT služeb, a naopak celkově poklesl počet zaměstnaných osob v telekomunikacích a v posledních letech také v ICT průmyslu.

[46] Někdy označováno také jako „Telco“.

	2009	2010	2011	2012	2013	2014	2015
Celkem	137 406	136 668	140 917	141 139	140 418	143 425	147 389
Podle skupin činností definovaných dle CZ-NACE							
ICT průmysl	33 177	28 602	30 293	27 355	24 462	23 346	23 771
ICT obchod	10 254	10 791	10 965	11 741	11 821	12 356	11 837
Telco	21 410	21 261	19 822	18 191	18 191	17 733	17 733
IT služby	76 014	76 014	79 838	85 945	89 535	94 048	94 048
% podíl v ČR	**3,5**	**3,6**	**3,6**	**3,6**	**3,6**	**3,7**	**3,7**

Tab. 2: Počet zaměstnaných osob (fyzických osob) v ICT sektoru (dle klasifikace CZ-NACE) v letech 2007-2015 a jejich podíl na celkovém počtu zaměstnaných osob v podnikatelském sektoru (65)

Nicméně Tab. 1 a Tab. 2 ukazují převážně na dodavatelskou část odborníků v ICT. Přičemž i ostatní subjekty zaměřené na jinou ekonomickou činnost dle klasifikace CZ-NACE mohou zaměstnávat odborníky v ICT. Přesto zmiňované statistiky naznačují potenciál růst pracovních míst v ICT sektoru. Identifikovat konkrétní potenciál pro bezpečnost ICT je ale dle této klasifikace nemožné. Navíc k identifikaci konkrétního počtu pracovníků a potenciálu vývoje pracovních míst v oblasti bezpečnosti ICT, by bylo nutné zahrnout i podnikatelé v této oblasti.

Motivací pro pracovníky musí být samozřejmě také finanční odměna. V roce 2014 vyšel výzkum[47], který zveřejnil výši příjmů pracovníků v oblasti bezpečnosti ICT v USA a jejich vývoj od roku 2008, kdy byl výzkum poprvé zpracováván. V něm se ukázalo, že navzdory predikci, která předpovídala zvýšení příjmů v oblasti ICT, se výrazně zvedly příjmy pouze těm pracovníkům, kteří zastávali manažerskou pozici (67). Právě v této kategorii v roce 2014 dosahoval průměrný příjem rozmezí od 100 000-11 999 USD ročně (67). Zatímco u nemanažerských pozic bylo rozpětí od 80 000-99 999 USD[48] ročně, přičemž celková průměrná hodnota příjmů dosaho-

[47] Prováděný výzkumnickou a vzdělávací organizací SANS Institute v USA (67).

[48] Nejčastěji se jednalo o administrátorské či inženýrské pozice.

vala částky 95 149 USD ročně (67 s. 7). Tab. 3 ukazuje, že největší vliv na výši příjmu mají zejména získané zkušenosti, tj. délka odborné praxe.

	Délka praxe				
Profese	**0-3**	**4-6**	**7-10**	**11-15**	**16-20**
CISO/CSO	89 500	97 750	125 400	138 529	148 000
Ředitel bezpečnosti/ Manažer bezpečnosti	108 846	115 189	120 381	128 379	134 538
Ředitel IT/Manažer IT	96 429	104 242	107 184	123 588	114 070
Inženýr bezpečnosti/ Architekt bezpečnosti	70 238	97 128	105 828	119 568	123 358
Systémový inženýr/ Systémový integrátor	89 444	89 706	108 750	115 556	129 615
Síťový architekt/ Síťový inženýr	91 944	85 000	107 179	107 625	109 118
Forenzní analytik (vyšetřovatel)	67 273	83 625	101 000	123 448	159 286
Auditor	65 278	82 600	97 143	107 115	113 333
Analytik bezpečnosti	72 393	79 034	93 498	101 618	109 915
Systémový administrátor	62 679	75 000	85 469	87 333	91 000

Tab. 3: Průměrný roční příjem (v USD) v závislosti na pracovní pozici a délky praxe (67)

V ČR vydává ČSÚ statistiky ICT odborníků, jejichž klasifikace se od té ve zmíněném průzkumu poněkud liší. Statistický popis ICT odborníků vychází z mezinárodní klasifikace zaměstnání „International Standard Classification of Occupations“ (ISCO-08), který byl v ČR převzat a upraven do klasifikace zaměstnání CZ-ISCO (68). Na tu se přešlo z původní klasifikace KZAM-R, která byla pro oblast ICT poněkud zastaralá (69). Přesto klasifikace CZ-ISCO není pro oblast bezpečnosti ICT vyhovující, neboť speciálně pro tuto oblast definuje pouze jednu jedinou kategorii zaměstnání s názvem „2529 - Specialisté v oblasti bezpečnosti dat a příbuzní pracovníci“ (68). Ta definuje pozice jako právě „Specialista pro bezpečnost informačních a komunikačních technologií“ a „Specialista v oblasti bezpečnosti dat“.

V klasifikaci ale chybí právě pozice, které ukazuje Tab. 3, například manažer kybernetické bezpečnosti, specialista řízení bezpečnosti informací, forenzní analytik (vyšetřovatel) nebo auditor (68). Ačkoli klasifikace CZ-ISCO není zcela přizpůsobena vývoji v oblasti bezpečnosti ICT,

můžeme zde alespoň najít specialisty v oblasti počítačových sítí, systémové administrátory a další kategorie zaměstnání, které jsou s bezpečností úzce spjaty (68). Problémem však je, že statistiky vydané ČSÚ nezahrnují například právě specialisty v oblasti řízení rizik do struktury zveřejňované statistiky ICT odborníků, a tak je velký problém celkový počet odborníků v oblasti bezpečnosti ICT kvantifikovat.

Podskupina nazvaná „252 - Specialisté v oblasti databází a počítačových sítí“, pod kterou spadá kategorie „2529 - Specialisté v oblasti bezpečnosti dat a příbuzní pracovníci“, obsahovala v roce 2015 na 21,4 tisíc odborníků (13 % z celkového počtu ICT odborníků), přičemž v roce 2013 to bylo pouhých 15,8 tisíc (10 % z celkového počtu ICT odborníků)[49] (70). Mezi nimi však mohli být i odborníci, kteří nemusí mít nutně znalosti z oblasti bezpečnosti ICT. K identifikaci celkového počtu odborníků na pracovním trhu by bylo nutné navíc k této kategorii připočítat i jiné kategorie, jako jsou řídící pracovníci v oblasti bezpečnosti, specialisté v oblasti prodeje bezpečnostních produktů a řešení, auditoři a další. Tyto pozice však v samotné klasifikaci takto definovány nejsou, což by mohlo způsobit, že konečné výsledky budou velmi zkreslené. Věrohodná statistika o současném počtu odborníků v oblasti bezpečnosti ICT v ČR prozatím neexistuje, a tak je velmi obtížné zjistit konkrétní údaje.

V souvislosti s příjmy, je však zajímavé zmínit alespoň průměrnou mzdu kategorie pracovníků, kteří spadají do této podskupiny s názvem „252 - Specialisté v oblasti databází a počítačových sítí“ a mzdu pracovníků podskupiny „133 – Řídící pracovníci v oblasti ICT“. Zejména zajímavé je pak porovnání s průměrnými příjmy v USA uvedenými v Tab. 3. Kdyby byl brán v úvahu nejvyšší kurz USD v roce 2013, který byl ve 2. čtvrtletí roku 2013 roven 19,78 Kč, mohl dle těchto údajů systémový administrátor s maximálně tříletou praxí v USA dosáhnout příjmů v přepočtu až 1 239 791 Kč ročně (čistý příjem) (71). Systémový administrátor v ČR si přitom dle údajů ČSÚ v té době mohl průměrně přijít až na 499 884 Kč hrubého ročně, tedy o více jak polovinu méně (72).[50] Přičemž žena na pozici specialisty v ICT by si v té době mohla přijít na částku o dost nižší, v průměru až 486 888 Kč (72). Jedná se však o průměrnou hrubou měsíční mzdu, která bývá často velmi zkreslená vyššími příjmy. Z tohoto důvodu je vhodnější přihlížet k mediánu mezd.

[49] Toto šetření bylo provedeno metodou dotazování v běžných domácnostech.

Klasifikace dle CZ-ISCO	Průměrná hrubá měsíční mzda			Medián mezd		
	2013	2014	2015	2013	2014	2015
(133) Řídící pracovníci v oblasti ICT	72.968	69.963	72.934	60.425	57.282	59.110
(2522) Systémoví administrátoři, správci počítačových sítí	41.657	43.118	45.306	37.454	38.218	40.271
(2523) Specialisté (kromě správců) v oblasti počítačových sítí	53.267	55.281	54.429	47.185	48.600	46.757
(2529) Specialisté v oblasti bezpečnosti dat a příbuzní pracovníci	56.822	58.068	58.789	49.419	50.353	52.445

Tab. 4: Průměrná hrubá měsíční mzda a medián mezd[51] řídících pracovníků a specialistů v ICT v ČR; 2013-2015 (72)

Ačkoli výše příjmů v ČR nedosahují takové úrovně jako v USA, pozice v oblasti bezpečnosti sítí a informací jsou v ČR aktuálně jedny z nejvyhledávanějších. To má jednoznačný vliv na výši příjmů těchto pracovníků (73). Společnost Hays, přední světová společnost v oboru lidských zdrojů a získávání specialistů, zveřejnila v roce 2016 průzkum[52], který odhaluje měsíční platy specialistů a analytiků v oblasti bezpečnosti ICT (74). V roce 2016 dosahovaly platy v sektoru IT/Telco v rozmezí od 40 do 80 tisíc Kč (nejčastěji tomu bylo okolo 60 tisíc Kč) a vykazovaly růst v průběhu roku celkem o 2,5 % (74 s. 29). Problém však je, že tento průzkum neuvádí metodiku, která byla použita. Z tohoto důvodu není zcela jasné, proč jsou zveřejněny platy, nikoli mzdy těchto pracovníků a taktéž není jasné, jaké organizace jsou v rámci IT sektoru zahrnuty (v návaznosti na klasifikaci CZ-NACE).

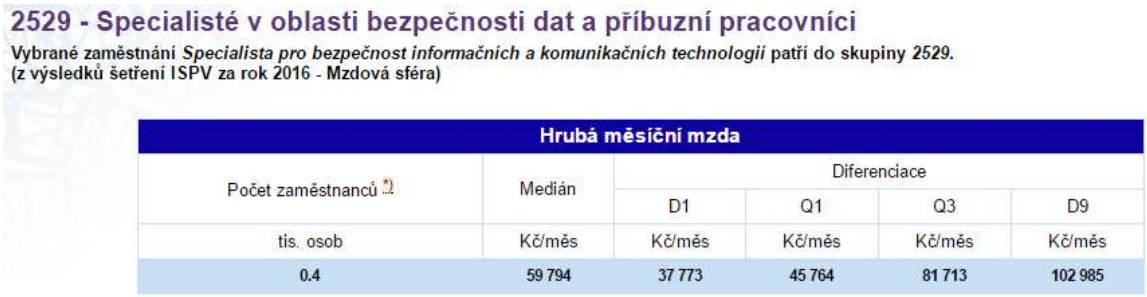
Pro přesnější a aktuálnější údaje o mzdách pracovníků v oblasti bezpečnosti ICT v ČR, je možné nahlédnout do „Informačního systému o průměrných výdělcích“ (ISPV)[53] spadající pod Ministerstvo práce a sociálních věcí ČR. Zde byl v roce 2016 medián hrubé měsíční mzdy pro kategorii zaměstnání „2529 – Specialisté v oblasti bezpečnosti dat a příbuzní pracovníci“

[51] V Kč.

[52] Tento průzkum nebyl na rozdíl od statistiky ČSÚ založen na klasifikaci CZ-ISCO.

[53] Ačkoli byly metodiky ČSÚ a MPSV sjednoceny a obě využívají klasifikace CZ-ISCO, jimi zveřejňovaná data jsou rozdílná, neboť slouží pro jiné účely.

roven částce 59 794 Kč, tedy o něco výše než v roce 2015 (viz. Tab. 4) (75). Celkový rozptyl hrubé měsíční mzdy pracovníků v této kategorii v roce 2016 ukazuje Obr. 2.



2529 - Specialisté v oblasti bezpečnosti dat a příbuzní pracovníci

Vybrané zaměstnání *Specialista pro bezpečnost informačních a komunikačních technologií* patří do skupiny *2529*.
(z výsledků šetření ISPV za rok 2016 - Mzdová sféra)

Hrubá měsíční mzda					
Počet zaměstnanců [?]	Medián	Diferenciace			
		D1	Q1	Q3	D9
tis. osob	Kč/měs	Kč/měs	Kč/měs	Kč/měs	Kč/měs
0.4	59 794	37 773	45 764	81 713	102 985

Obr. 2: Medián hrubé měsíční mzdy „Specialisty pro bezpečnost informačních a komunikačních technologií" na základě výsledků šetření ISPV za rok 2016[54] (75)

Výrazně vzrostl zájem také o obchodníky v oblasti bezpečnosti ICT (74). A i nadále jsou nejvíce poptávaní odborníci v oblasti programování, cloudu a v oblasti CRM a ERP systémů (74). Poptávku zvyšuje současná situace na trhu s IT technologiemi, kdy v současné době řada nadnárodních společností buduje svá IT centra právě v ČR (74). Důvodem je levnější pracovní síla oproti jiným evropským zemím (74). Předpokladem je, že poptávka po odbornících v těchto oblastech i nadále poroste a mohla by se v budoucnu zvýšit cca o 20 %, což je pro ekonomiku ČR velmi příznivé (74). Celkově lze tak hodnotit situaci na současném pracovním trhu jako velice příznivou. Nicméně je nezbytné vybudovat dostatečnou a kvalitní základnu odborníků v oblasti bezpečnosti ICT, která by zvyšující se poptávku dokázala dostatečně pokrýt. Ukazuje se však, že pro uplatnění absolventů existují různé bariéry.

Největší bariérou v zaměstnávání absolventů vysokých škol jsou jejich poměrně vysoké nároky na výši mzdy, které mnohdy neodpovídají možnostem zaměstnavatelů (76). Častým důvodem nepřijetí absolventa je také nedostatek odborné praxe a zkušeností. U absolventů s praxí se předpokládá, že: *„se lépe orientují v oboru, jsou schopni snadněji se adaptovat na pracovní režim a jsou zodpovědnější"* (76). Zaměstnavatelé také zmiňují, že všeobecně klesla kvalita absolventů a chybí propojení výuky s odbornou praxí (76). Studenti bez praxe potřebují mnohem delší dobu na adaptaci v pracovním prostředí. Dále je ze strany zaměstnavatelů požadována zejména jazyková vybavenost, schopnost práce s výpočetní technikou a kreativní přístup při řešení problémů (77).

[54] *„Výsledky mzdové a platové sféry jsou publikovány každé pololetí. Do mzdové sféry patří ekonomické subjekty, které odměňují mzdou podle § 109, odst. 2 zákona č. 262/2006 Sb., zákoníku práce, ve znění pozdějších předpisů."* (75)

9. Vzdělávání v oblasti bezpečnosti ICT na VŠ

Jak již bylo v této práci zmíněno, současný proces vzdělávání na vysokých školách (VŠ) není dostatečně připraven na rozvoj vzdělávání v oblasti bezpečnosti ICT. Odklon k digitalizaci a automatizaci vyžaduje vytvářet studijní obory a vyučovat ty studijní předměty, které nebudou příliš úzce specializované, ale budou reflektovat potřebu multidisciplinárního systémového přístupu (55 s. 24). S přenesením částečné odpovědnosti na digitální systémy nabývá na významu důvěryhodnost zpracování, integrita zpracovávaných dat a samotná dostupnost těchto systémů (55 s. 17). K tomu je zapotřebí disponovat nejen kvalitními odborníky na oblast bezpečnosti ICT, ale také dostatkem pedagogických pracovníků s adekvátními znalostmi, kteří dokáží tyto odborníky vzdělávat. Otázkou zůstává, zda při stejném vývoji budou VŠ vůbec schopny produkovat požadovaný počet absolventů v tomto oboru.

Cílem kapitoly je:

- popsat současnou situaci vzdělávání v oblasti bezpečnosti ICT na VŠ;
- představit existující doporučení pro vzdělávání odborníků v této oblasti;
- popsat model pro strukturování znalostní základny v oblasti bezpečnosti ICT.

9.1. Současný stav vzdělávání odborníků v bezpečnosti ICT

Konkrétní statistické údaje o velikosti nabídky odborníků v oblasti bezpečnosti ICT nejsou dostupné[55]. K tomu, aby bylo možné alespoň odhadnout přibližnou velikost nabídky, je nutné vycházet z dat dostupných statistik a jiných dostupných zdrojů. V první řadě, je vhodné zmínit vzdělanostní strukturu obyvatel ČR. Zde podíl osob s vysokoškolským vzděláním dosahoval v roce 2015 24,5 % (ve věku 25-54 let) (78). Přesto však ČR oproti ostatním zemím EU poněkud zaostává a dělí se o poslední místa se zeměmi jako je Chorvatsko (25 %), Slovensko (23,5 %), Malta (23 %), Rumunsko (19,6 %) a nakonec Itálie (19,1 %) (78). Naopak mezi přední země s největším podílem vysokoškolsky vzdělaných osob patří Irsko, Finsko, Lucembursko, Kypr a Belgie. Česká republika je v porovnání s těmito zeměmi výrazně pozadu[56] (78).

Poslední statistické údaje uvádí, že v roce 2015 byl celkový počet odborníků v podskupině „252 – Specialisté v oblasti databází a počítačových sítí“, kam spadají zaměstnanci s názvem

[55] Jednak z toho důvodu, že neexistuje vyhovující klasifikace zaměstnání, která by reflektovala oblast bezpečnosti ICT. A za další z toho důvodu, že současné statistiky o počtech absolventů nejsou rozděleny na jednotlivé obory. Současnou nabídku absolventů tak lze stěží kvantifikovat.

[56] Nicméně výraznou roli hraje i demografické rozdělení obyvatelstva.

„2529 - Specialisté v oblasti bezpečnosti dat a příbuzní pracovníci“, roven 21,4 tisícům (70). Šetření bylo provedeno dotazováním v domácnostech, a tak nelze s jistotou říci, že zahrnuje skutečně všechny odborníky na bezpečnost ICT. Navíc jsou data uvedena za celou podskupinu, kam mohou spadat i odborníci na počítačové sítě a databáze, ale bez faktických znalostí z oblasti bezpečnosti ICT. Velmi těžko tak lze současnou nabídku z dostupných údajů kvantifikovat. Lze se však podívat na vývoj počtu absolventů v informatických oborech, který by mohl indikovat vývoj této nabídky.

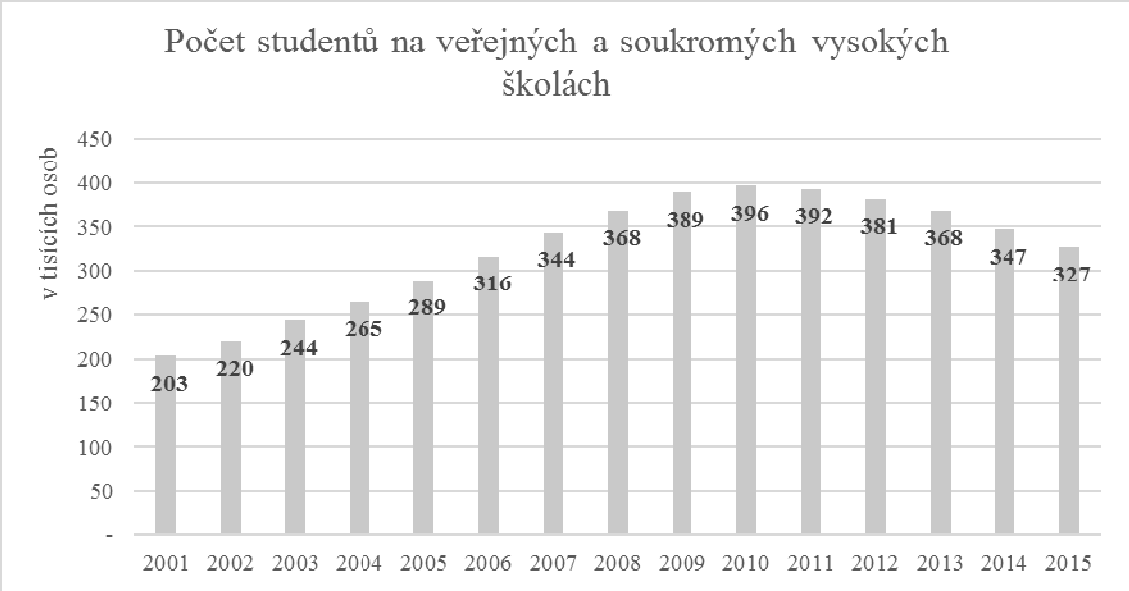
V letech 2001 až 2010 v ČR postupně stoupal počet studentů veřejných a soukromých VŠ, kdy v roce 2010 počet studentů dosáhl vrcholu necelých 396 tisíc osob (79). Poté začal počet studentů mírně klesat až v roce 2015 dosáhnul počtu necelých 327 tisíc osob (viz. Obr. 3). Statistiky ČSÚ neobsahují data státních vysokých škol. Je to z toho důvodu, že v roce 1998 bylo zákonem změněno právní postavení státních vysokých škol na veřejné instituce, mimo Policejní akademii České republiky v Praze a Univerzitu obrany, které zůstaly státními institucemi, jež spadají pod Ministerstvo obrany a Ministerstvo vnitra (79). Tímto zákonem také vznikla povinnost vést matriky studentů, avšak tyto dvě zmíněné školy nemají povinnost předávat informace do informačního systému s názvem „Sdružené informace matrik studentů“ (SIMS), odkud informace čerpá ČSÚ (79,80).

Otázkou zůstává, zda při stejném vývoji budou VŠ vůbec schopny produkovat požadovaný počet absolventů v oboru. Dostupné statistiky ČSÚ a MŠMT jsou zaměřeny především na studenty a absolventy IT oborů obecně, z nichž teprve určitou část mohou tvořit odborníci na bezpečnosti ICT. Problémem je, že taková statistika zaměřující se konkrétně na studenty a absolventy v oblasti bezpečnosti ICT v ČR není k dispozici, neboť se nepoužívá taková klasifikace, která by tuto oblast zahrnovala. Statistiky ČSÚ používají data získaná ze SIMS, které následně převádějí na programy dle klasifikace ISCED 97 (81). Dalším problémem je fakt, že statistiky MŠMT a ČSÚ se často liší. Ve statistikách ČSÚ je každý student uveden jen jednou (jako fyzická osoba), ačkoli může studovat více studijních programů najednou. Celkové počty studentů, které uvádí MŠMT jako součty za jednotlivé VŠ tak neodpovídají statistikám uváděným ČSÚ[57] (82).

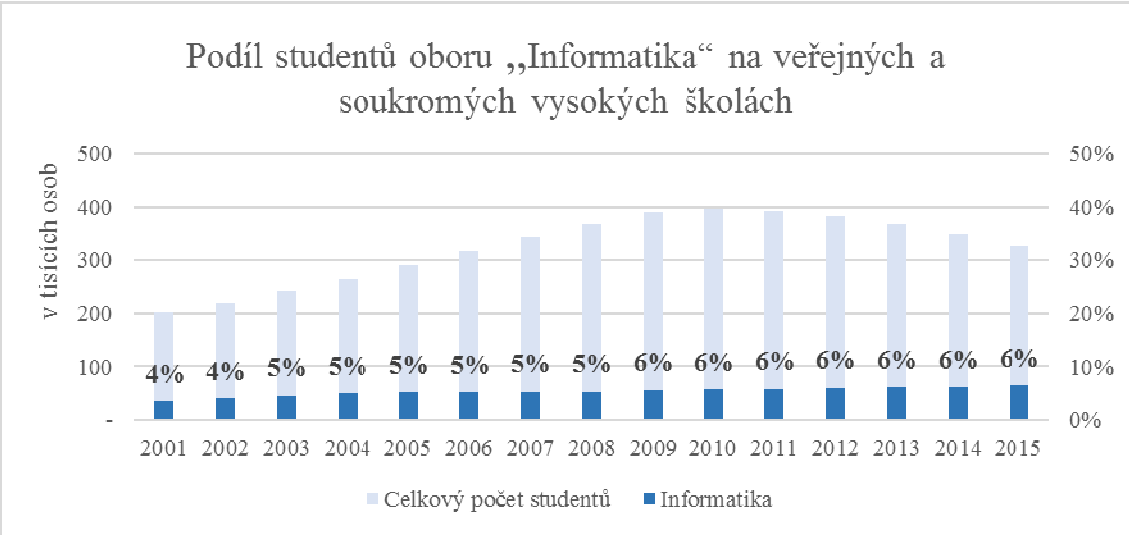
Dle statistik ČSÚ (od roku 2001) podíl studentů IT oborů na celkovém počtu studentů veřejných a soukromých VŠ významněji stoupnul poprvé v roce 2003 a podruhé v roce 2009 (82). V průběhu vývoje nárůst počtu studentů IT oborů reflektoval vývoj a nárůst celkového počtu studentů VŠ (viz. Obr.4). Od roku 2014 pak statistiky zaznamenaly, v návaznosti na pokles

[57] Jinak je tomu u absolventů, kteří mohou být započítáni do celkového počtu absolventů v průběhu let vícekrát (82). Například jedenkrát po ukončení bakalářského studia a podruhé po ukončení magisterského studia. Z tohoto důvodu narůstá v uvedených statistikách v posledních letech celkový počet absolventů.

studentů VŠ, prozatím mírný pokles studentů IT oborů (viz. Tab. 5). Mírně klesající počet studentů v IT oborech tak nahrává spíše prognózám o prohlubování nedostatku odborníků v IT obecně, ale také o samotnému nedostatku odborníků v oblasti bezpečnosti ICT. Ti tvoří pouze určitý podíl na celkovém počtu studentů v IT.



Obr. 3: Počet studentů na veřejných a soukromých VŠ v ČR v letech 2001–2015 (82)



Obr. 4: Podíl studentů IT oborů na celkovém počtu studentů veřejných a soukromých VŠ

Obor ISCED 97	2010	2011	2012	2013	2014	2015
Informatika	22 608	22 852	22 965	22 637	21 726	20 935
Obory celkem	395 979	392 100	381 021	367 898	347 096	326 909

Tab. 5: Vývoj celkového počtu studentů veřejných a soukromých VŠ a počtu studentů IT oborů v letech 2010-2015 (82,83)

Důležité je také zmínit, které obory jsou v oboru s označením „48 - Informatika“ dle mezinárodní klasifikace vzdělání ISCED 97 zahrnuty. Tento úzce vymezený obor je součástí široce vymezeného oboru s názvem „4 - Přírodní vědy, matematika a informatika“ a dělí se dle metodiky na dva podrobně vymezené obory s názvy: „481 – Počítačové vědy“ a „482 – Užití počítačů“ (81). Kde obor „Počítačové vědy“ (informatika) je definován jako *„studium navrhování a vývoje počítačových systémů a operačního prostředí“* (81). *„Zahrnuje studium navrhování, údržby a integrace softwarových aplikací.*“ (81). Obor má dle metodiky klasifikace ISCED 97 následující obsah (81):

- *„analýza počítačového systému,*
- *informatika (počítačová věda),*
- *lokalizace softwaru,*
- *návrh počítačového systému,*
- *operační systémy,*
- *počítačová věda,*
- *počítačové programování,*
- *programovací jazyky (Visual Basic, C++ atd.),*
- *programování (počítač),*
- *správa sítě,*
- *testování software.“*

Obor „Užití počítačů“ je definován jako *„studium používání počítačů a počítačového softwaru a aplikací pro různé účely“* (81). Metodika uvádí, že tyto obory jsou obvykle krátké a v rámci nich jsou zařazeny programy zaměřené na oblasti (81):

- *„používání počítačového softwaru,*
- *používání počítačů,*
- *programy používání internetu,*

- *software pro vydávání publikací pomocí počítače (DTP),*
- *software pro výpočty (tabulkové procesory),*
- *software pro zpracování dat,*
- *software pro zpracování textu.“*

Ačkoli zde není explicitně uvedená oblast týkající se bezpečnosti ICT, nelze říci, že by v rámci oboru „Informatika“ nemohli být zahrnuti také odborníci na bezpečnosti ICT. S velkou pravděpodobností není bezpečnost ICT v klasifikaci ISCED 97 vnímána jako samostatná oblast, ale spíše jako okrajová součást každé oblasti, se kterou je úzce spjata. Například správa sítě či návrh počítačového systému jsou oblasti, kde by měla být bezpečnost ICT zahrnuta. Nelze však říci, že by musela být nutně zahrnuta ve všech uvedených oblastech. Uvedené statistiky lze vnímat spíše jako orientační, ale rozhodně nevypovídají o konkrétním celkovém počtu studentů v oblasti bezpečnosti ICT.

Pro konkrétnější představu je nutné vycházet z jiných údajů. K přibližnému počtu studentů a absolventů studijních oborů věnující se bezpečnosti ICT lze dojít tak, že budou ze statistických údajů vyselektována jen data o počtech studentů a absolventů pouze těch VŠ, jež nabízejí studijní obory zaměřené na bezpečnost ICT. Až na úroveň jednotlivých studijních programů a oborů není možné dojít, neboť souhrnné statistiky v této struktuře neexistují.[58] V následujících analýzách budou dále obsažena data pouze těch VŠ, které vyučují v rámci svých fakult studijní obor zaměřený na bezpečnost ICT. Jedná se o seznam fakult veřejných VŠ v ČR s příslušnými studijními obory, který uvádí Tab. 6. Studijní plány těchto oborů jsou uvedeny v Příloze C. Seznam byl vytvořen na základě podkladu NCKB a na základě ověřování dostupných informací na Internetu (85).

Soukromé VŠ nebyly do seznamu zahrnuty. Jednak z toho důvodu, že zpravidla nevyhovují definici bezpečnost ICT, jež byla v této práci uvedena, tj. bezpečnost není vyučována v těsné souvislosti s ICT prostředím a studentům tak chybí hlubší znalosti z IT. Nebo potom z důvodu, že bezpečnost ICT na škole neexistuje jako samostatný studijní obor, ale pouze jako předmět v rámci některého ze studijních oborů. Studenti tak získávají sice obecný přehled, ale nezískávají hlubší znalost nezbytnou pro výkon dané profese v oblasti bezpečnosti ICT. Státní vysoké školy nebyly do seznamu zahnuty jednak z důvodu nedostupnosti dat a za další z toho důvodu,

[58] Nutno zmínit, že některé dílčí údaje je možné získat. Příkladem může být Vysoké učení technické v Brně a jeho Fakulta informačních technologií, která v rámci své výroční zprávy z roku 2015 uvádí počet absolventů s rozlišením na jednotlivé studijní obory. V rámci navazujícího magisterského studia oboru „Bezpečnost informačních technologií“ zde bylo v akademickém roce 2014/2015 celkem 15 absolventů. Od akademického roku 2010/2011 se eviduje 65 absolventů. (84)

že není zcela jasné, které údaje je možné zveřejňovat. V následujících analýzách byly proto vynechány. Zahrnuty byly jen ty veřejné VŠ, jejichž obory nabízely studijní obory zaměřené na bezpečnost ICT, tak jak byla vymezena v kap. 2. – „Vymezení bezpečnosti“. Výsledkem je seznam uvedený v Tab. 6.

Vysoká škola	**Fakulta**	**Studijní obor**	**Typ studia**
ČVUT	FIT	Bezpečnost a informační technologie	Bc.
ČVUT	FIT	Počítačová bezpečnost	nMgr.
ČVUT	FEL	Kybernetická bezpečnost	Mgr.
MU	FI	Bezpečnost informačních technologií, zaměření: Kybernetická bezpečnost	nMgr.
UTB	FAI	Bezpečnostní technologie, systémy a management	Bc.
UTB	FAI	Bezpečnostní technologie, systémy a management	nMgr.
VŠB-TUO	FEI	Informační a komunikační bezpečnost	nMgr.
VUT	FEKT	Informační bezpečnost	Bc.
VUT	FIT	Bezpečnost informačních technologií	Mgr.

Tab. 6: Seznam veřejných vysokých škol, jejich fakult a oborů zaměřených na bezpečnost ICT

Vysvětlivky:

Bc. – obor bakalářského studijního programu

Mgr. – obor magisterského studijního programu

nMgr. – obor navazujícího magisterského studijního programu

ČVUT – České vysoké učení technické v Praze

MU – Masarykova Univerzita

UTB – Univerzita Tomáše Bati ve Zlíně

VŠB-TUO – Vysoká škola báňská – Technická univerzita Ostrava

VUT – Vysoké učení technické v Brně

Z dat, jež uvádí MŠMT je již možné kvantifikovat celkový počet studentů dle jednotlivých fakult (86). Vybrané fakulty zahrnuté do výpočtu uvádí Tab. 6. V roce 2015 bylo na těchto fakultách celkem 17 681 studentů, což je 84,5 % z celkového počtu studentů oboru „Informatika" (dle klasifikace ISCED 97) v tom samém roce (86). A v roce 2016 to bylo pouze 16 701 studentů, což je podstatně méně než předchozí rok (86). Tím se množina počtu studentů o něco zmenšila a lze předpokládat, že konečný výsledek by byl ještě nižší. Nutno však podotknout, že určité alespoň základní bezpečnostní povědomí z oblasti bezpečnosti ICT mohou mít také studenti spadající do jiných oborů uvedených ve statistikách dle klasifikace ISCED 97.

Ze statistik MŠMT lze kvantifikovat také celkový počet absolventů. Ten byl v roce 2015[59] roven počtu 82 004, přičemž v IT oboru bylo evidováno 4 350 absolventů a 3 809 absolventů na fakultách ze seznamu, jež uvádí Tab. 6 (83,86). Celkový přehled o počtech studentů a absolventů v roce 2015 přináší Tab. 7 a Tab. 8. Tab. 7 znázorňuje „Podíl 1" – podíl studentů IT oborů na celkovém počtu studentů VŠ v ČR, „Podíl 2" – podíl studentů vybraných fakult s obory zaměřenými na bezpečnost ICT na celkovém počtu studentů IT oborů a „Podíl 3" – podíl studentů vybraných fakult na celkovém počtu studentů VŠ v ČR. Položka „Vybrané fakulty v ČR", „Podíl 1", „Podíl 2" a „Podíl 3" byly dopočítány. Obdobně tomu bylo v Tab. 8.

Celkem v ČR	**Informatika v ČR**	**Podíl 1**	**Vybrané fakulty v ČR**	**Podíl 2**	**Podíl 3**
326 909	20 935	6,4 %	17 681	84,5 %	5,4 %

Tab. 7: Stav počtu VŠ studentů v ČR, studentů IT a studentů vybraných fakult v roce 2015 (83,86)

Tab. 8 znázorňuje „Podíl 1" – podíl absolventů IT oborů na celkovém počtu absolventů VŠ v ČR. Sloupec s názvem „Podíl 2" – ukazuje podíl absolventů vybraných fakult s obory zaměřenými na bezpečnost ICT na celkovém počtu absolventů IT oborů. Sloupec „Podíl 3" – je podíl absolventů vybraných fakult na celkovém počtu absolventů VŠ v ČR. Tím, že byla vymezena skupina odborníku v bezpečnosti ICT na jednotlivé fakulty, došlo k omezení množiny absolventů o 12,4 % a studentů o 15,5 %, než kdyby byl započítán celkový počet studentů IT oborů dle klasifikace ISCED 97. Odhadovaná základna studentů a absolventů v oblasti bezpečnosti ICT je tímto daleko nižší, než uvádí dané statistiky pro oblast IT. Z dostupných zdrojů není možné odhadovat přesný vývoj počtu studentů a absolventů v oborech, jež uvádí Tab. 6, neboť tyto obory byly v průběhu času založeny v různém časovém období a přesný rok jejich otevření není

[59] Zúžení množiny studentů a absolventů v oblasti bezpečnosti ICT bylo možné provést pouze do roku 2015. Za rok 2016 neexistovaly všechny potřebné zdroje pro provedení výpočtu.

zcela vždy dostupný. Vzhledem k tomu, že však byli započítáni všichni studenti příslušných fakult, lze očekávat celkovou množinu odborníků na bezpečnost ICT výrazně menší.

Celkem v ČR	Informatika v ČR	Podíl 1	Vybrané fakulty v ČR	Podíl 2	Podíl 3
82 004	4 350	5,3 %	3 809	87,6 %	4,6 %

Tab. 8: Stav počtu VŠ absolventů v ČR, absolventů IT oborů a absolventů vybraných fakult v roce 2015 (83,86)

Z dostupných zdrojů je velmi obtížné odhadnout skutečný vývoj studentů a absolventů v oblasti bezpečnosti ICT, nicméně při zveřejňování různých statistik je vhodnější si tuto skupinu odborníků vymezit spíše jednotlivými fakultami, než pouze vymezením na informatické obory definované v klasifikaci ISCED 97. Z uvedených údajů je patrné, že vymezená skupina zahrnuje podstatně méně odborníků, ačkoli pro konkrétní vymezení na oblast bezpečnosti ICT by bylo zapotřebí rozdělit statistiku až na konkrétní obory. Z uvedených statistik je alespoň možné zpozorovat velmi nízký podíl počtu studentů a absolventů těchto oborů na celkovém počtu studentů a absolventů. To nahrává spíše predikcím o nedostatku odborníků v této oblasti.

9.2. Obecné doporučení pro vzdělávání v oblasti bezpečnosti ICT

Historicky byl významným mezníkem ve vzdělávání v oblasti výpočetních věd rok 1968, kdy byl vydán dokument „Curriculum Committee on Computer Science“ asociací ACM (Association for Computing Machinery) známé jako „Curriculum 68“ (87). Dokument obsahuje doporučení několika základních kurzů, které by měly být zařazeny do studia informatiky (88). Téměř paralelně s tím, bylo vydáno obdobné doporučení zaměřené na počítačové inženýrství (87). Následně v roce 1977, vzdělávací výbor celosvětově uznávané členské organizace IEEE Computer Society věnující se výpočetním vědám a technologiím, vydal dokument „Model Curricula Subcommittee of the Education Committee“ (87). Ten se již zaměřoval na model vzdělávání, jehož jádro bylo vytvořeno pro oba vědní obory.

Během dalších dekád byla vytvářena další doporučení, a to ve spolupráci asociace ACM a členské organizace IEEE. Jako základní dokument vzniklo kurikulum „Computing Curricula 2005“ (CC2005) poskytující vysokoškolské učební osnovy pro definovaných pět subdisciplín výpočetních věd (89):

- Počítačové inženýrství (Computing Engineering),
- Počítačové vědy (Computer Science),
- Informační systémy (Information Systems),

- Informační technologie (Information Technology),
- Softwarové inženýrství (Software Engineering).[60]

V návaznosti na předchozí vývoj ICT a příchod nových technologických fenoménů v ruce s novou průmyslovou revolucí a rozvojem kybernetické bezpečnosti, vznikla v roce 2015 iniciativa sestavit pracovní skupinu, která by se věnovala vypracování komplexního doporučení pro vzdělávání v oblasti bezpečnosti ICT[61] (90). Postupně vzniká nové doporučení s názvem „Cybersecurity Curricula 2017" (CSEC2017). Dokument je v současnosti rozpracován v návrhu a nachází se v připomínkovém řízení. Kapitoly týkající se doporučených studijních plánů nejsou stále dopracovány (90). Cílovou skupinou doporučení jsou vysoké školy věnující se disciplínám založeným na výpočetních vědách, které by chtěly vytvořit studijní programy a obory zaměřené na bezpečnost ICT.

Doporučení je prozatím vytvořeno pro bakalářské obory, ale stále zůstává otázkou, zda bude studium bezpečnosti ICT rozloženo do tří či pěti let (90). Nicméně v této práci není cílem stanovit konkrétní studijní plány a osnovy předmětů a rozložit je na tří či pěti leté studium. Cílem je ukázat, jakou bázi znalostí by absolventi těchto oborů měli mít vzhledem k jejich uplatnitelnosti na trhu. Lze se tedy inspirovat kurikulem, jaké znalostní domény pokrýt. Do jaké úrovně by měly tyto domény pokryty, bude záležet zejména na přístupu jednotlivých VŠ, zda budou nabízet jak bakalářské, tak navazující magisterské studium, či pouze magisterské studium v tomto oboru. Kurikulum obsahuje velmi dobrý myšlenkový model, který strukturuje oblasti znalostí z oblasti bezpečnosti ICT na jednotlivé domény znalostí. Tento model lze využít při analýze magisterských studijních oborů uvedených v Tab. 6 v praktické části práce.

9.2.1. Charakteristika studijního programu dle CSEC2017

Cybersecurity Curricula 2017 (CSEC2017) je doporučení vydané prestižními organizacemi, jako je ACM, IEEE – CS, asociace AIS SIGSEC a IFIP WG 11.8 (90). Cílem dokumentu je dodat sadu globálních doporučení pro vzdělávání na VŠ v oblasti bezpečnosti ICT.

Doporučení říká, že každý studijní program by měl zahrnovat (90 s. 14):

- základy z výpočetních věd (např. informační systémy či informační technologie, atd.);

---

[60] Tato doporučení se snaží neustále reflektovat vývoj vědních oborů a příchod nových výpočetních disciplín tím, že jsou pravidelně aktualizována (89).

[61] V cizojazyčné literatuře se nejčastěji označuje jako cybersecurity/cyber security, avšak není chápáno pouze jako kybernetická bezpečnost, ale i počítačová bezpečnost, a nakonec i bezpečnost informací v digitálním prostředí.

- průřezové koncepty široce uplatnitelné napříč všemi specializacemi v oblasti bezpečnosti ICT;
- klíčové znalosti a dovednosti v oblasti bezpečnosti ICT;
- znalosti a dovednosti přímo cílené k určité specializaci;
- etický základ.

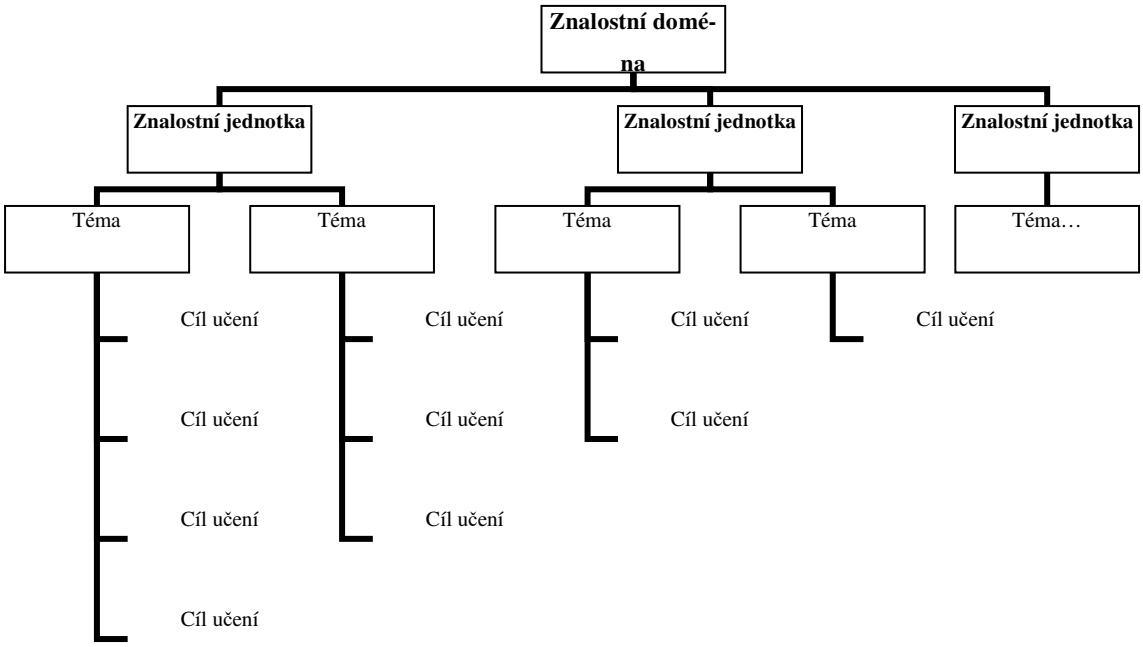
Základem bezpečnosti ICT dle kurikula jsou výpočetní vědy, které jsou popsány v rámci kurikula CC2005 (91 s. 115-122):

- **počítačové inženýrství** – obor zaměřený na konstrukci a návrh počítačů a systémů, zahrnuje studium HW, SW a komunikačních technologií od vývoje až po aplikaci teoretických poznatků, důraz je kladen především na HW;
- **počítačové vědy** – obor s velmi širokým rozsahem znalostí, zaměřený na oblast infrastruktury, systémů, ale také na robotiku, inteligentní systémy či bioinformatiku;
- **informační systémy** – obor zaměřený na integraci ICT do procesů organizací, zaměřuje se zejména na zpracování informací pomocí ICT v těchto procesech a na jejich případnou optimalizaci, zahrnuje v sobě znalosti matematiky, informatiky, marketingu, managmentu i IT;
- **informační technologie** – studium takového oboru se zaměřuje zejména na návrh, řízení a správu IT v organizacích, zde je nejvíce kladen důraz na provoz a údržbu SW, obnovu starých technologií, zajištění podpory pro práci s IT a bezpečnost, je velmi orientován na praxi;
- **softwarové inženýrství** – obor primárně zaměřený na návrh a vývoj SW produktů (aplikací, informační systémů, OS, aj.), důraz je kladen na kvalitu a bezpečnost vyvíjeného SW, prolíná se s počítačovými vědami, jeho studium zahrnuje jak teoretické poznatky, tak praxi.

Myšlenkový model kurikula CSEC 2017 definuje čtyři základní dimenze (90 s. 15):

- znalostní domény,
- průřezové koncepty,
- disciplinární zaměření,
- aplikační domény.

Obecnými požadavky jsou komunikační a aritmetické dovednosti a schopnost analytického myšlení (90 s. 15). Znalostní domény zahrnují znalostní jednotky, tj. kritické znalosti z výpočetních disciplín (90 s. 17). Obr. 5 naznačuje strukturu znalostní domény. Ta se může skládat z několika znalostních jednotek. Znalostní jednotky se dále skládají z jednotlivých tematických celků, jež jsou sdružovány na základě jednotlivých cílů učení (83 s. 17).



Obr. 5: Struktura znalostní domény dle myšlenkového modelu kurikula CSEC2017

Model má nadefinován šest znalostních domén: bezpečnost dat, bezpečnost software, systémová bezpečnost, bezpečnost osob, organizační bezpečnost a společenské zabezpečení (90 s. 18). Přičemž část znalostních domén je technicky zaměřená a druhá část zahrnuje netechnické znalosti. V praxi se to může projevit tak, že některé studijní programy budou zaměřeny více technicky a jiné méně. Nicméně je důležité, aby byly ve všech studijních programech věnující se bezpečnosti ICT (bez ohledu na disciplinární zaměření) zachovány všechny definované domény (90 s. 18).

- **Bezpečnost dat**

Doména se zaměřuje na ochranu dat z pohledu důvěrnosti, dostupnosti a integrity. Na rozdíl od ostatních je velmi úzce zaměřena. Vyžaduje schopnost aplikovat matematické a analytické algoritmy. Zahrnuje znalostní jednotky jako je kryptografie, důvěrnost a integrita dat (90 s. 19).

- **Bezpečnost software**

Doména se zaměřuje na vývoj a použití softwaru, zejména na jeho bezpečnostní vlastnosti a schopnosti, které by měly zajistit dostatečnou ochranu informací a systémů. Tato doména je nejvíce specializovaná. Obsahuje znalostní jednotky jako je vysoká spolehlivost softwaru, bezpečný vývoj softwaru, rozvoj a údržba, malware analýza. Vyžaduje porozumění bezpečnosti dat (90 s. 19).

- **Systémová bezpečnost**

Doména se zaměřuje na vytvoření a udržování bezpečnostních vlastností systémů zahrnujících různě propojené komponenty (data, software, hardwarová zařízení, sítě a lidi). Tato rozsáhlá znalostní doména obsahuje znalostní jednotky jako je dostupnost, autentizace, řízení přístupů, návrh bezpečného systému, forenzní analýza, atd. (90 s. 19)

- **Bezpečnost osob**

Doména se zaměřuje na ochranu osobních údajů a na ochranu soukromí. Zahrnuje studium lidského chování ve spojení s bezpečností ICT. Znalostní jednotky se zabývají tématy jako je identity management, sociální inženýrství[62], soukromí, bezpečnost na sociálních sítích (90 s. 19).

- **Organizační bezpečnost**

Doména se zaměřuje na ochranu organizace (bez ohledu na její zaměření) před kybernetickými hrozbami. Zahrnuje témata jako je řízení rizik, obnova činnosti a kontinuita činností organizace, hodnocení bezpečnosti a souladu s legislativou, budování bezpečnostního povědomí lidských zdrojů, atd. (90 s. 19)

- **Společenská bezpečnost**

Doména se zaměřuje na aspekty kybernetické bezpečnosti, které se mohou jakkoli dotknout celé společnosti. Zahrnuje témata jako kybernalita, kybernetické právo, etika, politologie, intelektuální vlastnictví, profesní spolehlivost a odpovědnost, společenská odpovědnost, atd. (90 s. 19)

Znalostní jednotky nemusí být nutně součástí pouze jedné domény, ale mohou být zahrnuty v rámci vícero znalostních domén. Průřezovými koncepty jsou míněny hlavní pilíře bezpečnosti ICT, tj. důvěrnost, dostupnost a integrita a dále riziko (90 s. 20). Průřezové koncepty by měly

[62] *„Způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace.“* (8 s. 93)

v závislosti na celkovém disciplinárním zaměření programu ovlivňovat úroveň hloubky výuky znalostních jednotek. Právě na podobu programu má vliv také samotné disciplinární zaměření, kdy každý z programů může být celkově koncepčně zaměřen na jednu konkrétní disciplínu (např. softwarové inženýrství). Teprve od toho by se dále měly odvíjet cíle každé znalostní jednotky a také hloubka jejího obsahu (90 s. 20). Znalostní jednotky a základní témata jsou uvedeny v Příloze A.

Aplikační domény, jako poslední dimenze myšlenkového modelu kurikula, jsou určité oblasti z praxe (např. vývoj, management, podniková architektura, aj.), kde je možné principy kurikula uplatnit pomocí využití vhodného frameworku pro stanovení úrovně potřebných kompetencí. Například „Cybersecurity Workforce Framework“ vytvořený organizací NICE či framework „Competency Models for Enterprise and Cybersecurity“ navrženého dle vzdělávací instituce University of Phoenix ve spolupráci s mezinárodní institucí ASIS International (92,93).

10. Kritéria vzdělávání v oblasti bezpečnosti ICT

Pro definování požadavků na znalosti a dovednosti odborníků v oblasti bezpečnosti ICT lze vycházet z doporučení kurikula CSEC2017 charakterizovaného v kap. 9.2.1. - „Charakteristika studijního programu dle CSCES2017“, ale také z existujících doporučení odborníků v oblasti bezpečnosti ICT (kompetenční frameworky, modely, apod.), analýzy požadavků pracovního trhu a analýzy současných magisterských studijních oborů definovaných v kap. 9. – „Vzdělávání v oblasti bezpečnosti ICT na VŠ“.

Cílem práce je definovat minimální požadavky na znalosti odborníků v oblasti bezpečnosti ICT a ukázat optimální skladbu těchto znalostí a dovedností, tj. optimální profil absolventa VŠ. Výsledné rozdíly mezi aktuální skladbou znalostí absolventů a požadavky na jejich znalosti vycházející z existujících doporučení a pracovního trhu, mohou významně přispět k rozvoji a zlepšení kvality jednotlivých studijních oborů v oblasti bezpečnosti ICT. Použitá metodika může vysokým školám zjednodušit přesnou identifikaci absolventských profilů. Výsledky analýzy budou použity jako vstup k formulaci strategie pro rozvoj vzdělávání v oblasti bezpečnosti ICT tak, jak je v této práci vymezena.

10.1 Použitá metodika

Základním východiskem pro definici požadavků na znalosti a dovednosti pracovníků v oblasti bezpečnosti ICT, je stanovení znalostních domén. Při jejich definici jsem vycházela zejména z doporučení uvedených v dokumentu CSEC2017, který byl popsán v kap. 9.2.1. – „Charakteristika studijního programu dle CSEC2017“ a Příloze A – „Základní znalostní jednotky a témata“. Dále z teoretických východisek, tj. základní okruhy znalostí z oblasti řízení bezpečnosti informací a kybernetické bezpečnosti, které byly nastíněny v kap. 3. - „Řízení bezpečnosti informací“ a kap. 4. – „Řízení kybernetické bezpečnosti“. V neposlední řadě byly při formulaci znalostních domén a znalostních jednotek zohledněny skutečné požadavky pracovního trhu (viz. Příloha B) a reálné plány studijních oborů na vybraných VŠ (viz. Příloha C).

Analyzováno bylo vybraných šest magisterských oborů, se zaměřením na bezpečnost ICT, jež uvádí Tab. 6 v kap. 9.1. – „Současný stav vzdělávání odborníků v bezpečnosti ICT“. Jedná se o obory vyučované na technických VŠ s různým disciplinárním zaměřením z oblasti výpočetních věd. Příloha C obsahuje studijní plány analyzovaných oborů dle doporučeného průchodu studiem. V plánech nejsou vypsány volitelné předměty, diplomová práce a obhajoba, státní

zkouška, tělesná výchova a cizí jazyky, tj. z pohledu tohoto hodnocení předměty nepodstatné[63]. Zahrnuty byly naopak povinně volitelné předměty, které u většiny oborů studentům umožňují prohloubit znalosti v problematice bezpečnosti ICT. U čistě volitelných předmětů se objevuje až přílišná diverzita v jednotlivých zaměřeních předmětů, a tak nelze zaručit, že studenti volí v rámci svého studia právě ty předměty, které by jim prohloubily znalosti v bezpečnosti ICT. Z tohoto důvodu nebyly hodnoceny.

Na základě analýz existujících zdrojů a na základě poznatků z kap. 11. – „Analýza požadavků pracovního trhu“ (Tab. 11, Tab. 12), byly určeny znalostní domény. Celkem bylo vytvořeno deset znalostních domén s označením ID 01-10, které je pro zjednodušení při hodnocení používáno. Znalostní domény jsou definovány pomocí znalostních jednotek uvedených v kap. 11.1. – „Definice znalostních domén“ (Tab. 13) a slouží k vymezení rozsahu a k namapování znalostí každého z hodnocených oborů na znalostní domény. Pro hodnocení znalostní základny jednotlivých studijních oborů bylo vymezeno a definováno celkem deset znalostních domén:

- 01 – Řízení bezpečnosti informací,
- 02 – Řízení kybernetické bezpečnosti,
- 03 – Softwarové inženýrství,
- 04 – Systémová bezpečnost,
- 05 – Síťová bezpečnost,
- 06 – Kybernalita,
- 07 – Právo,
- 08 – Etika,
- 09 – Trendy ICT,
- 10 – Odborná praxe.

Lze si povšimnout, že oproti kurikulu CSEC2017, kde bylo definováno šest znalostních domén, se jedná o jemnější rozlišení. Domény „Kybernalita“, „Právo“ a „Etika“ byly „vyděleny“ z domén definovaných CSEC2017 jako „Společenská bezpečnost“, „Organizační bezpečnost“ a „Bezpečnost lidských zdrojů“. Tímto byly zvýrazněny s ohledem na požadavky pracovního trhu. Díky jemnějšímu rozlišení lze snadněji ověřit, zda daný studijní obor danou oblast pokrývá, či nikoli. Častým problémem studijních oborů zaměřených na bezpečnost ICT, jež jsou vyu-

[63] Z toho důvodu součet kreditů v uvedených studijních plánech neodpovídá 120 ECTS kreditům, jež je požadováno pro absolvování magisterského studia.

čovány čistě na technicky zaměřených vysokých školách, je zejména absence výuky těchto znalostí. Z tohoto důvodu byly tyto okruhy znalostí osamoceny.

Důvodem, proč nebyly převzaty znalostní domény z návrhu kurikula CSEC2017, bylo příliš úzké vymezení domény „Bezpečnost dat“ a také fakt, že pokud by se hodnocení jednotlivých domén předložilo odborníkům z praxe k vyjádření, pravděpodobně by velmi obtížně kategorizovali oblasti jako právo či kybernetická bezpečnost, které se prolínají všemi doménami kurikula CSEC2017. Specifické oblasti jsou ve výše definovaných doménách vyděleny, a tak mohou být samostatně hodnoceny. Zároveň portfolio znalostních domén charakterizuje potřebu multidisciplinárního přístupu, který byl zmiňován v kap. 5 – „Bezpečnost ICT jako multidisciplinární obor“. Znalostní domény byly celkově redefinovány a z původních domén kurikula byly ponechány pouze „Systémová bezpečnost“ a „Bezpečnost software“, která byla přejmenována na „Softwarové inženýrství“. Naopak přidána a osamostatněna byla „Síťová bezpečnost“, která v poslední době nabývá na významu.

Jako poslední znalostní domény byly přidány „Trendy ICT“ a „Odborná praxe“. „Trendy ICT“ byly přidány z důvodu požadavků pracovního trhu, které orientaci v nich často požaduje a pro ověření, zda je akademické prostředí dostatečně reflektuje. Dle analýzy požadavků pracovního trhu je přehled o trendech v ICT základním požadavkem na pracovníky v oblasti bezpečnosti ICT. Obdobně je tomu u odborné praxe, kdy většina organizací vyžaduje alespoň minimální znalost prostředí a orientaci v něm. K tomu lze přispět povinnou odbornou praxí. Zde však může být problém s prací s informacemi, které nemusí být vždy určeny široké veřejnosti. Nicméně i sebemenší kontakt s praxí má pro budoucí absolventy obrovský přínos pro pozdější proces adaptace na pracovní prostředí Ten tak může být významně rychlejší a pro absolventa příjemnější.

Je zřejmé, že některé znalostní domény mohou být v rámci daného studijního oboru vyučovány pouze do určité úrovně znalostí, v závislosti na celkovém disciplinárním zaměření takového oboru. Domény „Řízení bezpečnosti informací“ a „Řízení kybernetické bezpečnosti“ by měly protínat napříč všechny tyto obory. Silněji však mohou být zastoupeny zejména v souvislosti s disciplínami jako „Informační systémy“ a „Informační technologie“. U domén „Softwarové inženýrství“, „Síťová bezpečnost“ a „Systémová bezpečnost“, se může úroveň dosažených znalostí významně lišit v závislosti na celkovém disciplinárním zaměření oboru. Úroveň dosažených znalostí se sice může lišit, ale měla by být alespoň vyvážená bez velmi výrazných výkyvů, tj. ideálně bez absence znalostí.

Každá znalostní doména byla následně rozložena na několik stěžejních znalostních jednotek. K tomu byl použit návrh v myšlenkovém modelu kurikula CSEC2017. Znalostní jednotka je v hodnocení považovaná za okruh několika témat znalostní domény. Z důvodu rozsahu práce,

nebyl v kap. 11.1. – „Definice znalostních domén“ proveden rozpad na jednotlivá témata a dílčí cíle učení. Témata a dílčí cíle učení jsou předmětem osnov jednotlivých studijních předmětů, které byly analyzovány. Při kategorizaci předmětů do znalostních domén, bylo pohlíženo na to, aby předmět svými tématy reflektoval některé ze znalostních jednotek (tematický okruh) definované znalostní domény. Zde se mohlo nejvíce projevit subjektivní hodnocení, nicméně snahou bylo najít vždy konkrétní téma osnovy, které je jednoznačně přiřaditelné k dané znalostní jednotce konkrétní domény. K tomu také napomohl výčet témat znalostních jednotek v Příloze A - „Základní znalostní jednotky a témata“. Studenti by tak vždy měli mít alespoň minimální přehled v dané problematice.

Pro analýzu studijních oborů a následnou definici a hodnocení absolventských profilů byly využity definované znalostní domény a příslušné znalostní jednotky. Nejprve bylo analyzováno pokrytí jednotlivých definovaných domén v rámci jednotlivých studijních oborů. To bylo provedeno pomocí namapování studijních předmětů hodnoceného oboru na příslušné znalostní domény. Předmět byl zařazen do příslušné domény, pokud v osnově zahrnoval téma přiřaditelné alespoň k jedné definované znalostní jednotce v rámci domény. Některé předměty mohly být zařazeny do znalostních domén vícekrát, protože zahrnovaly témata z vícero znalostních domén. Tam, kde neexistoval žádný předmět, který by v osnově obsahoval téma přiřaditelné k některé ze znalostních jednotek příslušné domény, vznikla mezera v komplexním učebním plánu. Komplexní studijní obory by, obdobně jako v návrhu CSEC2017, měly zahrnovat všechny definované znalostní domény.[64]

K definici absolventských profilů a hodnocení pokrytí znalostních domén, je zapotřebí nejprve stanovit kritéria pro hodnocení úrovně dosažených znalostí. Ke každé znalostní doméně bylo dále provedeno hodnocení úrovně získaných znalostí na základě definovaného kritéria, kde:

- **K – počet kreditů v kreditním systému** (ECTS), jež vyjadřuje obtížnost daného předmětu,1 kredit = 28 hodin studijní zátěže.

Každá znalostní doména je hodnocena jako součet všech kreditů těch studijních předmětů, které spadají do příslušné znalostní domény (dle zmiňovaných principů mapování znalostních jednotek). Protože některé předměty mohly být v rámci analýzy studijního oboru namapovány vícekrát, vypovídá výsledný součet kreditů o přibližné úrovni znalostí v rámci dané znalostní domény. Nikoli o definitivní a celkové úrovni znalostí v oblasti bezpečnosti ICT v rámci hodnoceného studijního oboru, která by byla měřitelná pomocí ECTS. Pro hodnocení úrovně znalostí

[64] I přesto se může úroveň dosažených znalostí velmi lišit. Jednak vzhledem k celkovému disciplinárnímu zaměření oboru a jednak vzhledem k tomu, zda studenti studují pouze magisterský, nebo i bakalářský obor. K tomuto bylo při nastavování úrovní z hlediska toho, co je a není dostačující, přihlíženo.

v dané doméně odpovídající skutečnosti, by bylo nutné vycházet z detailnějších informací, které nejsou běžně veřejnosti dostupné a lze je získat pouze prostřednictvím dotazování odpovědných zástupců vysokých škol, či absolvováním takového oboru. Pro poukázání na výrazné rozdíly v rozsahu znalostí a na mezery ve znalostech absolventů je však uvedená metodika hodnocení dostačující.

Odpovídající úroveň znalostí po součtu kreditů ECTS v dané znalostní doméně je vyjádřena na stupnici v Tab. 9.

Součet kreditů v rámci domény	**Odpovídající úroveň znalostí**
0	Žádné znalosti a dovednosti
1-5	Obecný přehled
6-10	Základní orientace v problematice
11-20	Pokročilá orientace v problematice
21 a více	Výjimečný přehled v problematice

Tab. 9: Kritéria hodnocení úrovně znalostí

Pro nastavení kritérií pro hodnocení úrovně vzdělávání lze vycházet z teoretických východisek a z požadavků pracovního trhu (viz. Příloha B). Zde se i u pracovních pozic jako je administrátor IT bezpečnosti, objevují požadavky na znalost bezpečnostních standardů v oblasti kybernetické bezpečnosti. Stěžejními doménami pro základní orientaci v problematice bezpečnosti ICT a pro uplatnitelnost absolventů na trhu práce jsou domény „Řízení bezpečnosti informací“ a „Řízení kybernetické bezpečnosti“.

- Pro domény s ID 01 a 02, by měla být požadovaná úroveň znalostí absolventů dle Tab. 9 minimálně na úrovni **základní orientace v problematice**. V oborech se zaměřením na informační systémy a informační technologie řízení, lze pravděpodobně očekávat úroveň vyšší.

Obdobně tomu je u domén „Softwarové inženýrství“, „Systémová bezpečnost“ a „Síťová bezpečnost“. To se projevuje také výrazně v požadavcích na znalosti specialisty bezpečnosti ICT, kterou mohou absolventi těchto oborů po ukončení studia vykonávat. Lze však očekávat úroveň znalostí vyšší, neboť vybrané studijní obory jsou vyučovány na technických školách se zaměřením na technické znalosti a dovednosti v oblasti bezpečnosti ICT.

- Pro domény s ID 03, 04 a 05, by měla být požadovaná úroveň znalostí absolventů dle Tab. 9 minimálně na úrovni **základní orientace v problematice**. V oborech

s větším zaměřením na technické znalosti a dovednosti v oblasti bezpečnosti ICT, lze očekávat úroveň vyšší.

Domény s ID 06-09 doplňují znalosti z oblasti bezpečnosti ICT o znalosti z jiných oborů a splňují tak požadavek multidisciplinárního přístupu. Jsou zde zahrnuty znalosti z oblastí jako je například právo, etika, kybernalita, atd., jejichž význam byl zmiňován v kap. 5. – „Bezpečnost ICT jako multidisciplinární obor“, kap. 6.2.1. – „Legislativa ČR“ nebo kap. 7. – „Trendy v bezpečnosti ICT“. Etický základ je doporučován kurikulem CSEC2017. Mimo jiné by studenti měli mít alespoň obecné povědomí o celkovém vývoji bezpečnosti ICT a o událostech, které tento vývoj determinovaly. Důležité však je, aby absolvent disponoval alespoň minimálními znalostmi z každé definované domény.

- Pro domény s ID 06, 07, 08 a 09 by měla být požadovaná úroveň znalostí absolventů dle Tab. 9 minimálně na úrovni **obecného přehledu**.

Pro znalostní doménu s ID 10 lze tolerovat i absenci, a to zejména z toho důvodu, že pro některé obory by bylo velmi obtížné zakomponovat odbornou praxi za 10 ECTS (280 hodin[65]) do učebního plánu tak, aby studenti splnili zároveň i základní učební osnovu. Nicméně s apelem na potřebu zlepšení kvality absolventů by bylo ideální propojit praxi a vzdělávání absolventů. To bylo ostatně i zmíněno v kap. 6 – „Situace na pracovním trhu v oblasti bezpečnosti ICT“.

- Pro doménu s ID 10, lze vzhledem k problematickému uchopení tolerovat **žádné znalosti a dovednosti.** Výhodu budou představovat ti absolventi, kteří budou mít alespoň obecný přehled.

Z navrženého modelu hodnocení je tak možné zjistit, jaký rozsah znalostí daný studijní obor pokrývá a jakou přibližnou úroveň znalostí v jednotlivých doménách poskytuje. Výsledkem byly unikátní absolventské profily jednotlivých oborů, kde každé úrovni znalostí odpovídá příslušná stupnice grafu dle Tab. 10.

[65] Při výuce v délce 13 týdnů (semestr) by bylo nutné absolvovat odbornou praxi v rozsahu 21,5 hodiny týdně.

Úroveň znalostí	Klasifikační stupnice v grafu
Žádné znalosti a dovednosti	0
Obecný přehled	1
Základní orientace v problematice	2
Pokročilá orientace v problematice	3
Výjimečný přehled v problematice	4

Tab. 10: Klasifikační stupnice úrovně znalostí v absolventských profilech

Pro celkové zhodnocení vzdělávání v oblasti bezpečnosti ICT v rámci analyzovaných magisterských oborů byl proveden čistý aritmetický průměr dle vzorce:

$$\bar{x} = \frac{1}{n} * \sum_{i=1}^{n} x_i .$$

Výsledky hodnocení byly uvedeny v Tab. 20. Výsledný rozsah a úroveň znalostí byly graficky znázorněny na Obr. 12, kde je možné vidět vzniklé mezery ve znalostech absolventů analyzovaných magisterských studijních oborů v oblasti bezpečnosti ICT. Kap. 13. – „Hodnocení vzdělávání v oblasti bezpečnosti ICT“ dále popisuje tyto mezery a celkový dopad z hlediska požadavků pracovního trhu a vzhledem k situaci na trhu. Výsledná zjištění z analýzy studijních oborů jsou vstupem SWOT analýzy, která shrnuje poznatky externí (situace na pracovním trhu) a poznatky z analýzy studijních oborů. Zde jsou zhodnoceny silné a slabé stránky současného vzdělávání v analyzovaných magisterských oborech zaměřených na oblast bezpečnosti ICT. Z externích poznatků jsou dále odvozeny příležitosti a hrozby pro současné vzdělávání v této oblasti.

10.1.1. Definice rolí a profesí v oblasti bezpečnosti ICT

Pro definici adekvátní profesní role v oblasti bezpečnosti ICT, kterou by absolventi vybraných oborů mohli zastávat, a ze které by bylo možné odvodit požadavky na znalosti a dovednosti odborníků v této oblasti, je nejprve nezbytné vůbec definovat, koho lze za pracovníka v oblasti bezpečnosti ICT považovat. ČSÚ používá ve svých statistikách klasifikaci CZ-ISCO vycházející z mezinárodní klasifikace zaměstnání ISCO-08, která byla zmiňována v kap. 8. – „Situace na pracovním trhu v oblasti bezpečnosti ICT“. Ačkoli se jedná o velmi podrobnou klasifikaci zaměstnání, pro oblast bezpečnosti ICT není zcela dostatečná.

Pro potřeby správné identifikace základny znalostí a dovedností pracovníků v oblasti bezpečnosti ICT, bylo zapotřebí nalézt vhodnější klasifikaci zaměstnání, dle které by bylo možné odvodit adekvátní profesní roli. Velmi kvalitně provedená klasifikace je klasifikace ANZSCO vytvořená organizacemi Australian Bureau of Statistics, Statistics of New Zeland a Department of Education, Employment and Workplace Relations a platná od července roku 2010 (94). K této klasifikaci byla vytvořena metodická příručka pro nalezení vazby na standard ISCO-08, ze které je patrné, že ANZSCO reaguje na současný vývoj pracovního trhu a rozlišuje zaměstnání daleko jemněji, než je tomu u ISCO-08 (95). Výhodou použití této klasifikace je, že vypsané volné pracovní pozice v ČR mají obdobné, někdy i stejné názvy, jež jsou v této klasifikaci uvedeny – např. „ICT Account Manager“, „ICT Security Specialist“, „ICT Business Analyst“, atd.

ANZSCO oproti ISCO-08 reflektuje vývoj pracovního trhu v oblasti ICT, což dokazuje samotné zahrnutí ICT projektových manažerů, IT servis manažerů a jiných pracovních pozic do struktury zaměstnání, které ISCO-08 prozatím postrádá (94). ANZSCO navíc reflektuje také vývoj v oblasti bezpečnosti ICT a definuje pro ni samostatnou roli „262112 - ICT Security Specialist“ (Specialista bezpečnosti ICT) (95). Alternativou této role je „Security Administrator“ (Administrátor bezpečnosti) (95). Role „ICT Security Specialist“ je zařazena v jednotce (tzv. unit group) definované jako „262100 - Database and Systems Administrators, and ICT Security Specialist“ (Administrátoři databází a systémů a Specialisté bezpečnosti ICT) (96). Specialista bezpečnosti ICT je zde definován jako pracovník, který ustanovuje, řídí a spravuje politiku bezpečnosti ICT v organizaci a postupy za účelem minimalizace bezpečnostních rizik (96). To je sice definice velmi obecná, ale oproti klasifikaci v CZ-ISCO není čistě technicky zaměřená a zmiňuje také oblast bezpečnostních politik a řízení rizik.

CZ-ISCO definuje pro tuto oblast kategorii „2529 - Specialisté v oblasti bezpečnosti dat a příbuzní pracovníci“, která zahrnuje specialisty v oblasti bezpečnosti informačních, komunikačních a telekomunikačních technologií (97). Příklady pracovní činnosti této kategorie pracovníků jsou však příliš technicky zaměřené a nepokrývají činnosti spojené například s tvorbou bezpečnostní dokumentace na úrovni bezpečnostních politik či řízením rizik tak, jako tomu bylo v ANZCO. Pracovníci této kategorie vykonávají dle popisu v klasifikaci činnosti jako například (97):

- *školení uživatelů a podpora povědomí o zabezpečení s cílem zajistit bezpečnost systému a zlepšit efektivnost serveru a sítě;*
- *monitorování nejnovějších zpráv o počítačových virech s cílem určit, kdy aktualizovat systémy antivirové ochrany;*

- *monitorování používání datových souborů a regulace přístupů za účelem bezpečnosti informací v počítačových souborech;*
- *kódování přenosu dat a budování "protipožárních stěn (firewalls)" pro skrytí důvěrných informací při přenosu a pro odmítnutí pochybných digitálních přenosů.“*

Třída 1 v klasifikaci ANZSCO zahrnuje obdobně jako ISCO-08 zejména řídící pracovníky na vrcholových úrovních. Zde jsou samostatně zmíněni manažeři ICT a „Chief Information Manager“ (Ředitel ICT) (98). Samotná pozice ředitele bezpečnosti ICT či manažera bezpečnosti ICT zde, stejně jako v ISCO-08, definována není. Nicméně předpokladem je, že studenti po absolvování studia nejprve získají několikaletou zkušenost v oblasti bezpečnosti ICT a teprve později se dopracují na pozice řídících pracovníků. Výchozí profesní role pro definici požadavků na znalosti a dovednosti absolventů magisterských oborů v oblasti bezpečnosti ICT tak budou pozice na úrovni třídy 2. Ty nejsou čistě zaměřené na řízení, ale působí zejména na operativní úrovni řízení. Absolventi některých oborů v oblasti bezpečnosti ICT mohou případně vykonávat pozice na úrovni třídy 3, kam jsou zahrnuti techničtí pracovníci. Na ně se však tato práce nezaměřuje. V provedených analýzách je zaměření pouze na vyšší třídu 2 – specialisté.

Ačkoli ANZSCO lépe rozlišuje pracovníky v oblasti bezpečnosti ICT než ISCO-08, požadavky na jejich znalosti jsou v ANZSCO popsány velmi stručně. Navíc klasifikace ANZSCO stále nepokrývá svou strukturou stávající poptávku na pracovním trhu, a to zejména absencí pracovních pozic jako je například auditor, konzultant, analytik, specialista v oblasti kybernetické bezpečnosti a v oblasti řízení bezpečnosti informací, specialista bezpečnostního dohledu, etický hacker (penetrační tester), projektový manažer v oblasti bezpečnosti, obchodník v oblasti bezpečnostních technologií a řešení, architekt v oblasti bezpečnosti, aj. Pro definici odpovídající profesní role specialisty bezpečnosti ICT musela být provedena analýza pracovního trhu. Ta byla provedena tak, že byly vyhledávány skrz pracovní portál pracovní pozice vypsané za poslední 3 měsíce[66], v jejichž názvu byly uvedeny slova „bezpečnost“ či „security“. Tím vznikl přehled pracovních pozic a kvalifikačních požadavků v Příloze B. Díky analýze bylo možné přiřadit k definované pracovní roli adekvátní profese.

K určení základních požadavků na znalosti specialistů bezpečnosti ICT, bylo vybráno doporučení uvedené v kompetenčním modelu „Competency Models for Enterprise and Cybersecurity“ navrženého vzdělávací institucí University of Phoenix ve spolupráci s mezinárodní institucí ASIS International. Model říká, že za specialistu v bezpečnosti ICT můžeme označit toho, kdo zejména (93):

[66] Analýza byla provedena v období 12/2016–02/2017. Pracovní portál dostupný z: http://www.jobs.cz/.

- řídí rizika;
- se zabývá právními aspekty v oblasti bezpečnosti;
- navrhuje a implementuje opatření související s kybernetickou bezpečností;
- navrhuje a implementuje opatření související s bezpečností informací;
- uplatňuje zásady krizového managementu;
- vyšetřuje bezpečnostní události a incidenty;
- se zabývá návrhem administrativních, fyzických, technických a technologických opatření;
- obsluhuje ICT prostředí a udržuje jeho dostupnost a bezpečnost;
- zajišťuje ochranu ICT prostředí před hrozbami;
- vyšetřuje bezpečnostní události a incidenty a vede jejich evidenci;
- shromažďuje informace o bezpečnosti ICT a podílí se na vývoji znalostní databáze;
- analyzuje dostupné informace o bezpečnosti ICT;
- dohleduje bezpečnost ICT prostředí;
- podílí se na vývoji bezpečnosti ICT;

Podle tohoto frameworku by měli pracovníci v oblasti bezpečnosti ICT disponovat potřebnými kompetencemi pro oblast řízení bezpečnosti ICT v organizaci v podobě znalosti základů v oblasti řízení bezpečnosti, měli by mít základní orientaci v podnikovém prostředí a také hlubší znalost matematiky a výpočetních věd (93). Stěžejním předpokladem pro specialisty v oblasti bezpečnosti ICT se zaměřením na organizační zabezpečení jsou dle frameworku znalosti zejména v oblasti řízení rizik, legislativy v oblasti bezpečnosti, znalosti z kybernetické bezpečnosti, z oblasti bezpečnosti informací, krizového managementu, vyšetřování bezpečnostních událostí a incidentů a Information Security Governance, technologie pro kybernetickou bezpečnost, atd. (93)

Specialisté v oblasti bezpečnosti ICT se zaměřením především na implementaci technického zabezpečení by měli být schopni navrhnout technická bezpečnostní opatření pro daný systém, dále provozovat a udržovat bezpečnost ICT, chránit ICT prostředí před hrozbami, vyšetřovat hrozby, shromažďovat informace a řídit proces bezpečnosti ICT, analyzovat informace a dohlížet na bezpečnost ICT (93). Dále záleží na charakteru organizace, ve které jsou pracovníci zaměstnáni. Zde hraje nejdůležitější roli odvětví, v němž organizace zajišťuje svou činnost. Požaduje se tak například znalost prostředí státních institucí, bankovních a finančních institucí, zdravotnických zařízení, dopravy, výroby a průmyslu, apod. Provedená analýza trhu však ukázala,

že jsou na tyto specialisty kladeny obdobné požadavky, jako na specialisty zaměřené na organizační zabezpečení (93) S ohledem na tato existující doporučení a požadavky pracovního trhu uvedené v Příloze B, byly v provedené analýze v kap. 11 – „Analýza požadavků pracovního trhu“ k definované profesní roli přiřazeny požadavky na znalosti a následně i dovednosti profesí vykonávající profesní roli specialisty bezpečnosti ICT.

11. Analýza požadavků pracovního trhu

Pro definici základních požadavků na znalosti specialistů v oblasti bezpečnosti ICT vymezených v kap. 10.1.1. – „Definice rolí a profesí v oblasti bezpečnosti ICT“, byla provedena analýza požadavků pracovního trhu dle uvedené metodiky ve zmiňované kapitole. Tyto požadavky na znalosti, byly zohledněny při definování dílčích znalostních domén uvedených v kap. 11.1. – „Definice znalostních domén“. Zde bylo snahou smysluplně rozložit jednotlivé požadavky do adekvátních tematických okruhů tak, aby odpovídaly požadavkům pracovního trhu.

Základní role a profese	**Požadavky na znalosti**
Specialista bezpečnosti ICT (ICT Security Specialist) Profese: *administrátor bezpečnosti ICT; analytik bezpečnosti ICT, penetrační tester, etický hacker, konzultant kybernetické bezpečnosti/bezpečnosti informací*	**Klíčové znalosti:** - základní pojmy z oblasti bezpečnosti informací a kybernetické bezpečnosti; - znalost sady norem ISO/IEC 27000; - znalost konceptu Information Security Governance; - řízení rizik; - organizační a technická bezpečnostní opatření; - znalost legislativy ČR a EU v oblasti bezpečnosti ICT; - krizový management; - znalost související legislativy v oblasti ICT; - principy soukromí; - řízení kontinuity činností a jejich obnova; - řízení bezpečnostních událostí a incidentů; - vyšetřování bezpečnostních událostí a incidentů; - bezpečnost lidských zdrojů; - programovací jazyky; - znalost a orientace v prostředcích technické a síťové bezpečnosti (např. SIEM, firewall, aj.); - OS, databáze, nástroje pro obnovu dat, nástroje pro ochranu dat z pohledu důvěrnosti a integrity; - trendy v bezpečnosti ICT; - kryptografické nástroje a algoritmy; - systémová bezpečnost a bezpečnost software; - přehled o hackerských technikách a testovacích nástrojích;

	- standardy pro testování (např. OWASP); - přehled o aktuálních hrozbách v ČR, ale i celosvětově; - principy etického hackingu.

Tab. 11: Klíčové znalosti specialisty bezpečnosti ICT

Základní role a profese	**Požadavky na dovednosti**
Specialista bezpečnosti ICT (ICT Security Specialist) Profese: *administrátor bezpečnosti;* *analytik bezpečnosti ICT,* *penetrační tester,* *etický hacker,* *konzultant kybernetické bezpečnosti/bezpečnosti informací*	**Klíčové dovednosti:** - návrh a implementace technických a organizačních bezpečnostních opatření, - řízení rizik; - návrh a podpora implementace bezpečnostních politik; - návrh bezpečné architektury ICT; - provoz a údržba bezpečnosti ICT; - zlepšování bezpečnosti ICT; - návrh, implementace, aktualizace a testování plánů obnovy; - návrh a implementace strategie pro řízení kontinuity činností; - návrh a implementace politiky zálohování; - administrace a správa databází; - administrace a správa síťových prvků; - administrace přístupů do systémů a aplikací; - provozní administrace IDS a dalších bezpečnostních prvků sítě; - provádění bezpečnostních testů včetně plánování; - provádění analýz síťového provozu; - monitoring úrovně bezpečnosti ICT prostředí pomocí dohledových nástrojů; - práce s nástroji prevence a detekce narušení bezpečnosti – SIEM, log management, aj.; - analýza a vyhodnocování auditních logů; - identifikace a správa bezpečnostních incidentů a hrozeb, návrh vhodných protiopatření a spolupráce na jejich řešení; - sběr podkladů pro podporu vyšetřování;

	- reporting stavu ICT bezpečnosti; - shromažďování a udržování znalostí v oblasti bezpečnosti ICT; - konzultace v oblasti bezpečnosti ICT; - spolupráce při interních a externích auditech; - zpracování zpráv z testování; - aktualizace a údržba bezpečnostní dokumentace; - budování bezpečnostního povědomí; - monitoring a hodnocení účinnosti zavedených bezpečnostních opatření; - spolupráce při zadávání zakázek v oblasti IT/ICT bezpečnosti; - řízení projektů v oblasti IT/ICT bezpečnosti; - reporting, hodnocení a prezentace stavu bezpečnosti informací v organizaci; - schopnost orientace v daném odvětví;

Tab. 12: Klíčové dovednosti specialisty bezpečnosti ICT

11.1. Definice znalostních domén

Na základě existujících doporučení (CSEC2017, Competency Models for Enterprise and Cybersecurity) a analýzy požadavků pracovního trhu, bylo definováno celkem deset níže definovaných domén.

ID	Znalostní doména	Znalostní jednotka
01	**Řízení bezpečnosti informací**	Bezpečnost informací – související standardy a legislativa
		Základy bezpečnosti informací (hrozba, zranitelnost, aktivum, důvěrnost, dostupnost, integrita, cyklus PDCA a fáze zpracování, atd.)
		Information Security Governance
		Řízení rizik
		Řízení přístupů a přístupových práv

		Organizace řízení bezpečnosti informací
		Bezpečnost lidských zdrojů
		Bezpečnost provozu
		Základy bezpečnosti dat a ochrany informací
		Ochrana osobních údajů
		Bezpečnostní mechanismy
		Základy kryptografie a kryptoanalýzy
		Základy síťové bezpečnosti
		Základy systémové bezpečnosti
		Řízení kontinuity činností
		Zvládání bezpečnostních incidentů
		Audit bezpečnosti informací
02	**Řízení kybernetické bezpečnosti**	Kybernetická bezpečnost – související standardy a legislativa
		Základy kybernetické bezpečnosti (hrozba, zranitelnost, aktivum, důvěrnost, dostupnost, integrita, cyklus PDCA a fáze zpracování, bezpečnostní role, povinné subjekty, kritická informační infrastruktura, povinnosti subjektů, atd.)
		Krizové řízení a národní strategie kybernetické bezpečnosti ČR
		Řízení rizik
		Řízení přístupů a přístupových práv
		Organizace řízení bezpečnosti informací
		Bezpečnost lidských zdrojů

		Bezpečnost provozu a komunikací
		Bezpečnost průmyslových a řídících systémů
		Základy bezpečnosti dat a ochrany informací
		Ochrana osobních údajů
		Bezpečnostní mechanismy
		Základy kryptografie a kryptoanalýzy
		Základy síťové bezpečnosti
		Základy systémové bezpečnosti
		Řízení kontinuity činností
		Zvládání bezpečnostních incidentů
		Audit kybernetické bezpečnosti
03	**Softwarové inženýrství**	Základní principy návrhu software
		Principy bezpečného programování
		Ochrana před ztrátou dat
		Testování bezpečnosti SW (penetrační testy, fuzz testy, testování zranitelnosti SW, aj.)
		Dokumentace softwarového produktu
04	**Systémová bezpečnost**	Řízení přístupů a správa identit
		Informační a komunikační technologie
		Autentizace
		Pokročilá kryptografie a kryptoanalýza
		Návrh bezpečné architektury systémů
		HW a SW bezpečnost

		Bezpečnost databázových systémů
		Bezpečnost průmyslových a řídících systémů
		Ochrana počítačových sítí
		Bezpečnostní technologie ochrany IS a možnosti útoku
		Testování zranitelností a penetrační testování IS
		Forenzní analýza OS, systémových souborů, aplikací, sítí, mobilních zařízení, aj.
05	**Síťová bezpečnost**	Pokročilá bezpečnost počítačových sítí a zabezpečení cloudu
		Provoz počítačových sítí
		Pokročilé síťové technologie
06	**Kybernalita**	Trestné chování v kyberprostoru
		Kyberterorismus
07	**Právo**	Legislativa v oblasti kybernetické bezpečnosti a v oblasti ochrany dat
		Související legislativa ČR a EU
		Softwarové právo
		Ochrana soukromí
08	**Etika**	Etický hacking
		Profesní etika a profesní odpovědnost
09	**Trendy ICT**	Sociální sítě
		IoT
		3D tisk
		Big data

		Biometrie
		Bezpečnostní hrozby, atd.
10	**Odborná praxe**	Odborná praxe s ohledem na celkové zaměření oboru

Tab. 13: Definované znalostní domény

Mimo znalosti zahrnuté v uvedených znalostních doménách, by absolventi měli disponovat základními znalostmi z výpočetních věd a matematických disciplín, které lze považovat za prerekvizity ve vzdělávání v oblasti bezpečnosti ICT. U každého z oborů pak lze očekávat doplnění znalostí s ohledem na konkrétní disciplinární zaměření oboru. Mezi další požadavky kladené na absolventy pracovním trhem, je velmi dobrá znalost anglického jazyka, schopnost pracovat v týmu, komunikační a prezentační dovednosti, schopnost vyjednávání a kreativita při řešení úkolů. Co se však neobjevilo v žádném z doporučení, ani v současných studijních oborech, jsou základní znalosti z projektového řízení, marketingu, financí, obchodu či managementu.

12. Analýza studijních oborů

Analýza studijních oborů byla provedena pro vybrané magisterské obory uvedené v Tab. 6 v kapitole 9.1. – „Současný stav vzdělávání odborníků v bezpečnosti ICT“. Zdrojem informací byly veřejně dostupné informace, zejména: studijní plány těchto oborů (viz. Příloha C), osnovy předmětů a výroční zprávy vysokých škol.

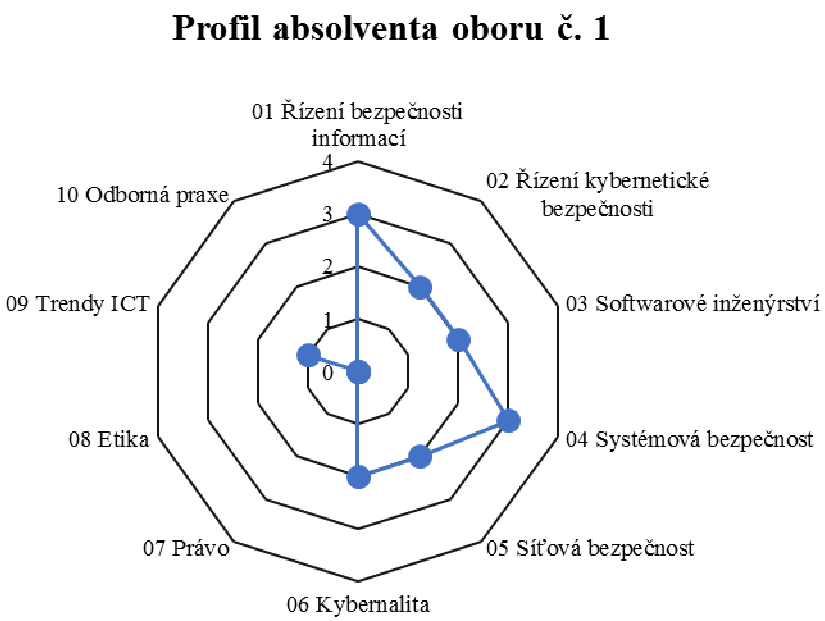
12.1. Studijní obor č. 1

Znalostní doména	**Odpovídající předměty**	**ECTS**
01 Řízení bezpečnosti informací	Systémová bezpečnost	**5**
	Síťová bezpečnost	**5**
	Informační bezpečnost	**2**
	Součet ECTS kreditů:	**12**
Celková úroveň znalostní domény 01:	***Pokročilá orientace v problematice***	
02 Řízení kybernetické bezpečnosti	Systémová bezpečnost	**5**
	Síťová bezpečnost	**5**
	Součet ECTS kreditů:	**10**
Celková úroveň znalostní domény 02:	***Základní orientace v problematice***	
03 Softwarové inženýrství	Paralelní a distribuované programování	**5**
	Pokročilá kryptologie	**5**
	Součet ECTS kreditů:	**10**
Celková úroveň znalostní domény 03:	***Základní orientace v problematice***	
04 Systémová bezpečnost	Systémová bezpečnost	**5**
	Reverzní inženýrství	**5**

	Hardwarová bezpečnost	**5**
	Pokročilá kryptologie	**5**
	Součet ECTS kreditů:	**20**
Celková úroveň znalostní domény 04:	***Pokročilá orientace v problematice***	
05 Síťová bezpečnost	Síťová bezpečnost	**5**
	Moderní technologie Internetu	**5**
	Součet ECTS kreditů:	**10**
Celková úroveň znalostní domény 05:	***Základní orientace v problematice***	
06 Kybernalita	Síťová bezpečnost	**5**
	Kybernalita	**3**
	Součet ECTS kreditů:	**8**
Celková úroveň znalostní domény 06:	***Základní orientace v problematice***	
07 Právo	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 07:	***Žádné znalosti a dovednosti***	
08 Etika	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 08:	***Žádné znalosti a dovednosti***	
09 Trendy ICT	Moderní technologie Internetu	**5**
	Součet ECTS kreditů:	**5**
Celková úroveň znalostní domény 09:	***Obecný přehled***	
10 Odborná praxe	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 10:	***Žádné znalosti a dovednosti***	

Tab. 14: Pokrytí znalostních domén oboru č. 1

Profil absolventa dle uvedené metodiky:



Obr. 6: Profil absolventa č. 1

Shrnutí hodnocení:

Oboru dominuje znalostní doména s ID 04, kde stejnojmenný předmět pokrývá základní znalostní jednotky domény tématy jako například autentizace, hardwarová bezpečnost, ochrana počítačových sítí, bezpečnostní technologie ochrany informačních systémů, možnosti útoku na informační systémy, aj. Další předmět spadající do této domény je „Reverzní inženýrství“, kde se studenti setkávají s postupy forenzního vyšetřování a forenzní analýzou. V neposlední řadě je výuka prohloubena o pokročilé kryptografické metody a kryptografickou analýzu, které jsou využitelné nejen při návrhu informačních systémů, ale i softwarových programů. Znalosti z předmětů, které se věnují síťové a systémové bezpečnosti jsou aplikovatelné při realizaci bezpečnostních opatření zejména technického charakteru v rámci zavádění, provozu a zlepšování ISMS, ale také systému řízení kybernetické bezpečnosti.

Problematiku domény s ID 01 je možné prohloubit o znalosti z povinně volitelného předmětu „Informační bezpečnost“, kterým lze získat základní znalosti z řízení bezpečnosti informací a řízení bezpečnosti IS/ICT – např. IT Governance, základní normy a standardy v těchto oblastech, legislativa ČR, řízení rizik, řízení kontinuity činností a obnova činnosti, audit, atd. Protože se však jedná o povinně volitelný předmět, je rozsah výuky menší než u povinných předmětů oboru. Na pokročilou orientaci v dané problematice to celkově nestačí. S čímž koresponduje také absence předmětů, které by se do větší hloubky věnovaly právu v bezpečnosti ICT. Opět je

zde možnost doplnit si chybějící znalosti v rámci povinně volitelného předmětu „Kybernalita“, nicméně někteří studenti mohou volit i jinak zaměřené předměty.

Závěr: Převažuje technické zaměření absolventa na počítačovou bezpečnost s pokročilou znalostí z oblasti řízení bezpečnosti informací, bez právního a etického základu a bez pokročilejších znalostí z oblasti řízení kybernetické bezpečnosti. Základní kontext z oblasti kybernality. V rámci oboru není povinná praxe.

- Vzhledem k celkovému zaměření studijního oboru je základní orientace v problematice domén s ID 01 a 02 dostatečná.
- Dle očekávání jsou znalosti v doménách s ID 03-05 vyšší, a tedy i dostatečné. Pokročilá orientace v problematice domény s ID 04 je výhodná zejména pro absolventy, kteří chtějí obsadit čistě technicky zaměřené profese.
- Jako velmi problematická, se jeví absence alespoň obecného přehledu v rámci domény s ID 08, neboť je velmi pravděpodobné, že absolvent takového oboru může v praxi provádět penetrační testování či testy zranitelností. Bez znalostí etického kodexu a znalostí z etického hackingu to lze považovat za velmi rizikové.
- Za rizikové lze považovat i absenci znalostí z domény s ID 07 a to z důvodu, že se absolvent takového oboru může v praxi podílet na ochraně kritických informačních systémů, kde je alespoň obecný přehled o ZKB a ZKŘ nezbytným předpokladem.
- Chybí možnost odborné praxe, kde by se budoucí absolventi mohli setkat se skutečnými problémy z reálného prostředí. Kladně lze hodnotit výuku současných trendů v ICT.
- V rámci oboru je nedostatek povinně volitelných předmětů. Oproti jiným oborům tak absolventi nedisponují hlubší znalostí vztahující se k bezpečnosti ICT.
- Přidanou hodnotou k povinným předmětům je možnost volby povinně volitelného předmětu „Kybernalita“, který zajišťuje potřebný kontext s prostředím bezpečnosti ICT.

12.2. Studijní obor č. 2

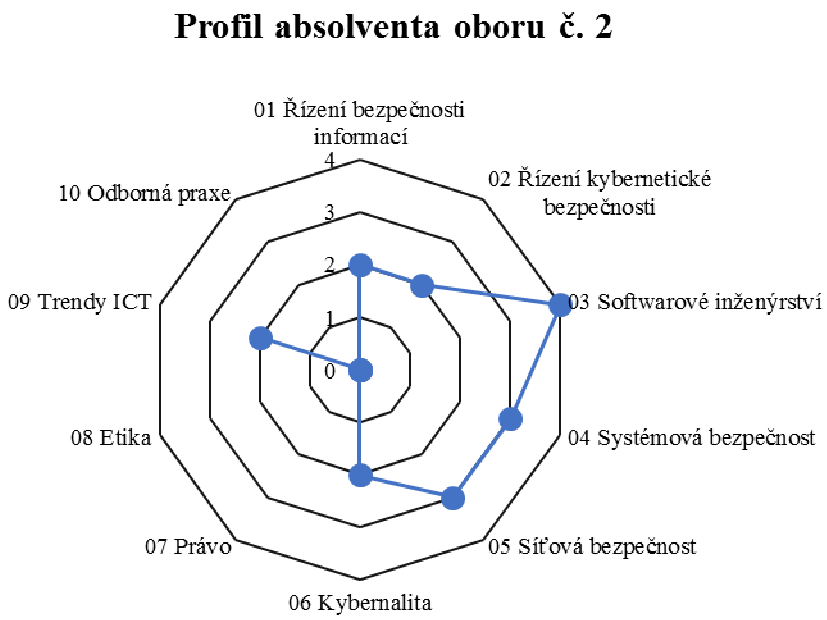
Znalostní doména	**Odpovídající předměty**	**ECTS**
01 Řízení bezpečnosti informací	Komunikační bezpečnost	**6**
	Součet ECTS kreditů:	**6**
Celková úroveň znalostní domény 01:	***Základní orientace v problematice***	

02 Řízení kybernetické bezpečnosti	Komunikační bezpečnost	**6**
	Součet ECTS kreditů:	**6**
Celková úroveň znalostní domény 02:	***Základní orientace v problematice***	
03 Softwarové inženýrství	Bezpečnost systémů	**6**
	Kombinatorická optimalizace	**6**
	Statistická analýza dat	**6**
	Zajištění kvality software	**6**
	Součet ECTS kreditů:	**24**
Celková úroveň znalostní domény 03:	***Výjimečný přehled v problematice***	
04 Systémová bezpečnost	Bezpečnost systémů	**6**
	Komunikační bezpečnost	**6**
	Součet ECTS kreditů:	**12**
Celková úroveň znalostní domény 04:	***Pokročilá orientace v problematice***	
05 Síťová bezpečnost	Pokročilé síťové technologie	**6**
	Bezpečnost systémů	**6**
	Součet ECTS kreditů:	**12**
Celková úroveň znalostní domény 05:	***Pokročilá orientace v problematice***	
06 Kybernalita	Komunikační bezpečnost	**6**
	Součet ECTS kreditů:	**6**
Celková úroveň znalostní domény 06:	***Základní orientace v problematice***	
07 Právo	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 07:	***Žádné znalosti a dovednosti***	

08 Etika	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 08:	***Žádné znalosti a dovednosti***	
09 Trendy ICT	Bezpečnost systémů	**6**
	Součet ECTS kreditů:	**6**
Celková úroveň znalostní domény 09:	***Základní orientace v problematice***	
10 Odborná praxe	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 10:	***Žádné znalosti a dovednosti***	

Tab. 15: Pokrytí znalostních domén oboru č. 2

Profil absolventa dle uvedené metodiky:



Obr. 7: Profil absolventa č. 2

Shrnutí hodnocení:

V hodnoceném oboru dominuje doména s ID 03, kterou pokrývají předměty jako například „Zajištění kvality software“. Celkově se však většina povinných předmětů oboru zaměřuje více úzce na celkové disciplinární zaměření oboru bez výrazných návazností na bezpečnost (např. „Kombinatorická optimalizace“). Jedinými předměty, které se v rámci oboru bezpečnosti věnují jsou „Komunikační bezpečnost“ a „Bezpečnost systémů“. Ty absolventům poskytují technický základ pro zajištění bezpečnosti informací či kybernetické bezpečnosti například té-

maty jako je anonymita, popřitelnost, identifikace a autentifikace, zajištění důvěrnosti a integrity, síťová bezpečnost, zaznamenávání logů, apod.

Předmět „Bezpečnost systémů“ pokrývá znalostní jednotky jako je psaní bezpečného kódu či řízení přístupů a přístupových práv. Zároveň svou osnovou předmět pokrývá doménu s ID 09, neboť se poměrně intenzivně věnuje zranitelnostem mobilních aplikací, mobilních operačních systémů a jejich zabezpečení. Komunikační bezpečnost pak zahrnuje v osnově i typické útoky (například na finanční systémy) a dotýká se tak zlehka oblasti kybernality.

Závěr: Převažuje technické zaměření absolventa na bezpečnost software bez právního a etického základu a bez pokročilejších znalostí z oblasti řízení bezpečnosti informací a z oblasti řízení kybernetické bezpečnosti. Základní kontext z oblasti kybernality. V rámci oboru není povinná praxe.

- Vzhledem k celkovému zaměření studijního oboru je základní orientace v problematice domén s ID 01 a 02 přijatelná.
- Jako velmi problematická, se jeví absence domény s ID 08, neboť je velmi pravděpodobné, že absolvent takového oboru může v praxi provádět penetrační testování či testy zranitelností. To může být bez znalostí etického kodexu a znalostí z etického hackingu velmi rizikové.
- Za rizikové lze také považovat absenci znalostí z domény s ID 07 a to z toho důvodu, že se absolvent takového oboru může v praxi podílet na ochraně kritických informačních systémů, kde je minimální základní znalost ZKB a ZKŘ nezbytným předpokladem.
- Ačkoli je zde snaha naučit studenty aplikovat získané znalosti v rámci cvičení v laboratořích, chybí možnost odborné praxe, kde by se studenti mohli seznámit s reálnými problémy z praxe.
- Nevýhodu může představovat absence bloku předmětů, které by byly povinně volitelné a vztahovaly by se k bezpečnosti ICT. Oproti jiným oborům tak studenti nezískávají hlubší znalosti vztahující se k bezpečnosti ICT.
- Kladně lze hodnotit snahu propojit výuku předmětů se současnými trendy v ICT.

12.3. Studijní obor č. 3

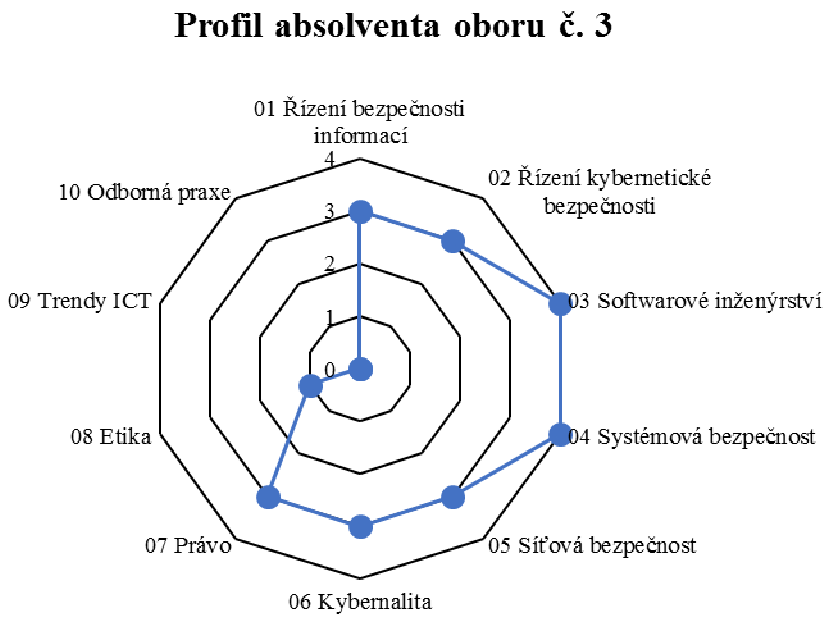
Znalostní doména	**Odpovídající předměty**	**ECTS**
01 Řízení bezpečnosti informací	Pokročilá témata v bezpečnosti informačních technologií	**6**
	Řízení informační bezpečnosti	**4**
	Aplikovaná kryptografie	**5**
	Úvod do práva ICT II	**4**
	Součet ECTS kreditů:	**19**
Celková úroveň znalostní domény 01:	***Pokročilá orientace v problematice***	
02 Řízení kybernetické bezpečnosti	Pokročilá témata kybernetické bezpečnosti	**5**
	Pokročilá témata v bezpečnosti informačních technologií	**6**
	Aplikovaná kryptografie	**5**
	Úvod do práva ICT II	**4**
	Součet ECTS kreditů:	**20**
Celková úroveň znalostní domény 02:	***Pokročilá orientace v problematice***	
03 Softwarové inženýrství	Systémové ověření a ujištění	**8**
	Pokročilá témata kybernetické bezpečnosti	**5**
	Principy a praktiky bezpečného kódování	**8**
	Laboratoř bezpečnosti a aplikované kryptografie	**3**
	Součet ECTS kreditů:	**24**

Celková úroveň znalostní domény 03:	***Výjimečný přehled v problematice***	
04 Systémová bezpečnost	Real-time systémy	**4**
	Systémové ověření a ujištění	**8**
	Pokročilá témata kybernetické bezpečnosti	**5**
	Pokročilá témata v bezpečnosti informačních technologií	**6**
	Aplikovaná kryptografie	**5**
	Součet ECTS kreditů:	**28**
Celková úroveň znalostní domény 04:	***Výjimečný přehled v problematice***	
05 Síťová bezpečnost	Pokročilé síťové technologie	**4**
	Pokročilá témata kybernetické bezpečnosti	**5**
	Pokročilá témata v bezpečnosti informačních technologií	**6**
	Součet ECTS kreditů:	**15**
Celková úroveň znalostní domény 05:	***Pokročilá orientace v problematice***	
06 Kybernalita	Specifika online komunikace	**4**
	Kyberkriminalita a kybernetická bezpečnost	**3**
	Úvod do práva ICT II	**4**
	Součet ECTS kreditů:	**11**
Celková úroveň znalostní domény 06:	***Pokročilá orientace v problematice***	
07 Právo	Teorie a metoda práva ICT	**3**
	Úvod do práva ICT I	**4**
	Úvod do práva ICT II	**4**

	Součet ECTS kreditů:	**11**
Celková úroveň znalostní domény 07:	***Pokročilá orientace v problematice***	
08 Etika	Postgraduální seminář o IT bezpečnosti a kryptografii	**4**
	Součet ECTS kreditů:	**4**
Celková úroveň znalostní domény 08:	***Obecný přehled***	
09 Trendy ICT	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 09:	***Žádné znalosti a dovednosti***	
10 Odborná praxe	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 10:	***Žádné znalosti a dovednosti***	

Tab. 16: Pokrytí znalostních domén oboru č. 3

Profil absolventa dle uvedené metodiky:



Obr. 8: Profil absolventa č. 3

Shrnutí hodnocení:

Profil absolventa oboru se, oproti předchozím hodnoceným oborům, otevírá do větší šíře. To je dáno zejména tím, že zahrnuje povinně volitelné předměty zaměřené na témata vztahující se přímo k bezpečnosti ICT, které mohou prohloubit znalosti některé z domén – softwarové inženýrství, systémová bezpečnost či síťová bezpečnost. Podmínkou pro splnění studijního plánu je absolvování vždy minimálně jednoho předmětu z každé domény. To je důvodem, proč absolventi takového oboru dosahují minimálně pokročilé orientace v klíčových oblastech nejen v doménách s ID 01 a 02, ale také s ID 06 a 07.

Obor, oproti předchozím hodnoceným oborům, zahrnuje navíc předměty přímo specializované na témata ze znalostních domén s ID 01 a 02 Na ně dále navazuje předměty z dalších znalostních domén jako například z domény s ID 07 či 04. To se projevilo v uplatnění některých předmětů ve vícero znalostních doménách, neboť se tyto znalostní domény smysluplně svou osnovou propojovaly a navazovaly na sebe. Příkladem může být předmět „Pokročilá témata v bezpečnosti informačních technologií“, který se zabýval řízením rizik, bezpečnostními politikami, ale také bezpečností kritické informační infrastruktury, biometrickou autentizací a bezpečností sítí.

Studenti jsou navíc povinni absolvovat několik předmětů v oblasti práva ICT. Tyto předměty jsou navíc strukturované do jednotlivých úrovní a postupně na sebe nabalují různou problematiku z oblasti bezpečnosti ICT – od elektronického podpisu, ochrany dat, duševního vlastnictví po kybernetickou bezpečnost, kybernalitu a datové schránky. Na předměty následně volně navazuje předmět „Kyberkriminalita a kybernetická bezpečnost“. Zde však byla patrná absence návaznosti na současné trendy v ICT – např. ransomware útoky, phishing, aj. Phishing je pouze lehce nastíněn v osnově povinně volitelného předmětu „Specifika online komunikace“.

Závěr: Vyvážený profil absolventa se zaměřením jak na zajištění bezpečnosti ICT z organizačního hlediska, tak z technického hlediska s pokročilou orientací v oblasti práva a s minimálním etickým základem. Doplněn hlubším kontextem z oblasti kybernality. V rámci oboru není povinná praxe.

- Oproti předchozím hodnoceným oborům, je úroveň znalostí získaných v doménách s ID 01 a 02 velmi dobrá a tedy dostačující.
- Vyvážený absolventský profil je více univerzální, než v předchozích hodnocených oborech. To umožňuje uplatnění absolventa v čistě technicky zaměřených profesích, ale také v profesích, kde je vyžadována například konzultační činnost v oblasti kybernetické bezpečnosti. Nevýhodu může představovat pro absolventy, kteří usilují převážně o technicky zaměřené profese.

- Minimální úroveň znalostí získaných z domény s ID 08 snižují riziko, že by se absolvent takového oboru mohl v praxi chovat neeticky v rámci pracovních činností jako je například penetrační testování či testy zranitelností. Z tohoto pohledu je úroveň znalostí absolventů dostačující.
- Za velmi příznivou lze považovat pokročilou znalost práva v oblasti ICT a bezpečnosti ICT. Tyto znalosti rozšiřují uplatnitelnost absolventa, který může být zaměstnán například jako specialista kybernetické bezpečnosti, kde jednou z jeho primárních činností může být posuzování „compliance“ s právními předpisy z oblasti kybernetické bezpečnosti.
- Obdobně jako u předchozích oborů i navzdory tomu, že se projevuje snaha naučit studenty aplikovat získané znalosti v rámci cvičení v laboratořích, chybí možnost odborné praxe, kde by studenti mohli seznámit s reálnými problémy z praxe.
- Velkou výhodu představují vhodně složené bloky předmětů zaměřené na bezpečnost ICT v rámci jednotlivých znalostních domén jako například softwarové inženýrství, systémová bezpečnost či síťová bezpečnost. Oproti jiným oborům studenti získávají hlubší znalosti vztahující se k bezpečnosti ICT.
- Velmi kladně lze hodnotit propojenost a návaznost studijních předmětů v rámci jednotlivých domén.
- Vytknout lze menší zaměření na současné trendy v ICT, než tomu bylo u předchozích hodnocených oborů.

12.4. Studijní obor č. 4

Znalostní doména	**Odpovídající předměty**	**ECTS**
01 Řízení bezpečnosti informací	Nadstandardní prvky objektové bezpečnosti	**4**
	Bezpečnostní technologie ochrany informačních systémů	**3**
	Elektronické zabezpečovací a přístupové systémy	**4**
	Kamerové systémy	**4**

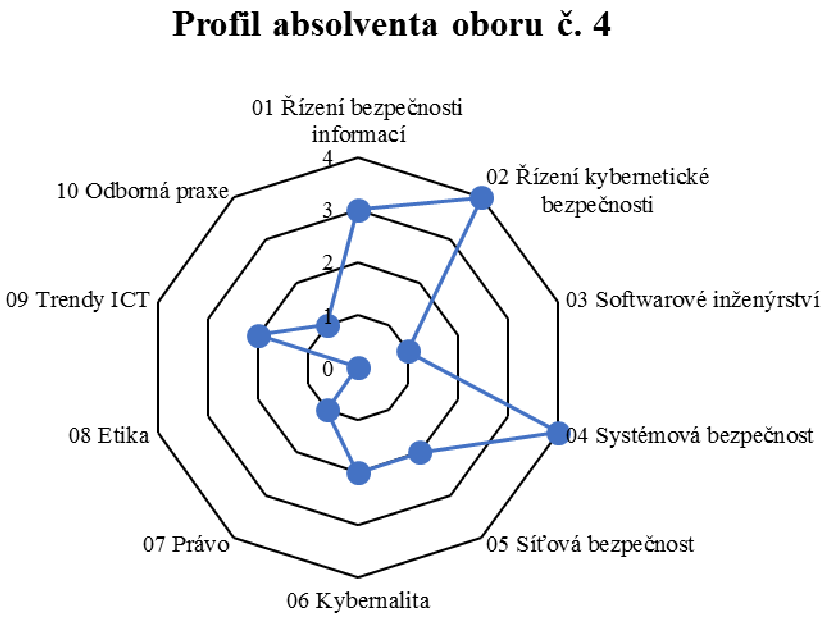
	Součet ECTS kreditů:	**15**
Celková úroveň znalostní domény 01:	***Pokročilá orientace v problematice***	
02 Řízení kybernetické bezpečnosti	IZS státu, krizový a informační management	**5**
	Nadstandardní prvky objektové bezpečnosti	**4**
	Bezpečnostní technologie ochrany informačních systémů	**3**
	Kybernetická bezpečnost	**4**
	Modelování krizových situací	**6**
	Elektronické zabezpečovací a přístupové systémy	**4**
	Kamerové systémy	**4**
	Součet ECTS kreditů:	**30**
Celková úroveň znalostní domény 02:	***Výjimečný přehled v problematice***	
03 Softwarové inženýrství	Počítačové viry a bezpečnost	**3**
	Součet ECTS kreditů:	**3**
Celková úroveň znalostní domény 03:	***Obecný přehled***	
04 Systémová bezpečnost	Počítačové viry a bezpečnost	**3**
	Robotika	**6**
	Telekomunikační systémy	**4**
	Bezpečnostní technologie ochrany informačních systémů	**3**
	Informační systémy	**5**

	Forenzní vědy	**5**
	Projektování integrovaných systémů	**6**
	Součet ECTS kreditů:	**32**
Celková úroveň znalostní domény 04:	***Výjimečný přehled v problematice***	
05 Síťová bezpečnost	Provoz počítačových sítí	**4**
	Počítačové viry a bezpečnost	**3**
	Bezpečnostní technologie ochrany informačních systémů	**3**
	Součet ECTS kreditů:	**10**
Celková úroveň znalostní domény 05:	***Základní orientace v problematice***	
06 Kybernalita	Kriminologie	**4**
	Forenzní vědy	**5**
	Součet ECTS kreditů:	**9**
Celková úroveň znalostní domény 06:	***Základní orientace v problematice***	
07 Právo	Podnikatelské právo v průmyslu komerční bezpečnosti	**4**
	Součet ECTS kreditů:	**4**
Celková úroveň znalostní domény 07:	***Obecný přehled***	
08 Etika	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 08:	***Žádné znalosti a dovednosti***	
09 Trendy ICT	Geografické informační systémy	**4**
	Bezpečnostní technologie ochrany informačních systémů	**3**

	Počítačové viry a bezpečnost	**3**
	Součet ECTS kreditů:	**10**
Celková úroveň znalostní domény 09:	***Základní orientace v problematice***	
10 Odborná praxe	Odborná praxe	**5**
	Součet ECTS kreditů:	**5**
Celková úroveň znalostní domény 10:	***Obecný přehled***	

Tab. 17: Pokrytí znalostních domén oboru č. 4

Profil absolventa dle uvedené metodiky:



Obr. 9: Profil absolventa č. 4

Shrnutí hodnocení:

Obor je skladbou předmětů více zaměřen na systémovou bezpečnost, kterou pokrývá předměty jako například „Bezpečnostní technologie ochrany informačních systémů“, „Informační systémy“, „Telekomunikační systémy“ či „Robotika“ aj. Kde předmět „Bezpečnostní technologie ochrany informačních systémů“ svou osnovou pokrývá vícero znalostních domén. Zahrnuje témata jako bezpečnost informačních systémů a prvků IS, autentizaci, bezpečnost provozu, zabezpečení sítí, ale také bezpečnost cloudu, čímž reaguje na současné trendy v bezpečnosti ICT.

Zajímavým doplňkem je zaměření na geografické informační systémy, které rozšiřují portfolio znalostí domény.

Velmi významné je propojení systémové bezpečnosti s forenzními vědami, která obsahuje znalosti z práce s digitálními stopami. Ojedinělá je také specializace na kamerové systémy a elektronické zabezpečovací a přístupové systémy (tzv. EZS), což jsou systémy velmi důležité pro zajištění fyzické bezpečnosti ICT prostředí. Tyto systémy jsou vyžadovány ZKB, a tak byly zařazeny do domény s ID 02, ale také do domény s ID 01 (vzhledem k tomu, že ta požadavek na zajištění fyzické bezpečnosti také zahrnuje). Mimo to, že střeží majetek organizace a kontrolují vstup osob do budov organizace, zabezpečují fyzický přístup k ICT technologiím a tím také informace, které jsou v nich zpracovávány.

V absolventském profilu dále velmi dominuje znalostní doména s ID 02 a to díky předmětům jako „IZS státu, krizový a informační management“, „Kybernetická bezpečnost“ a „Modelování krizových situací“. Zde jsou součástí osnov předmětů stěžejní témata kybernetické bezpečnosti, například kritická infrastruktura ČR, krizový management a krizové řízení, ochrana obyvatelstva, ale také bezpečnostní strategie ČR a ochrana kritické informační infrastruktury. Součástí osnovy je také nezbytné právní minimum.

Široce uplatnitelný předmět v rámci vícero znalostních domén byl předmět „Počítačová bezpečnost a viry“. Ten zahrnoval jednak znalosti z oblasti tvorby a generování počítačových virů, ale také metody infekce a prevenci bezpečnostních incidentů. Zohledněny byly taktéž současné trendy v bezpečnosti ICT (např. phishing).

Závěr: Vyvážený profil absolventa se zaměřením jak na zajištění bezpečnosti ICT z organizačního hlediska, tak z technického hlediska s úzkou specializací na kybernetickou bezpečnost a systémovou bezpečnost, s právním základem a bez etického základu. Doplněn základním kontextem z oblasti kybernality. V rámci oboru je povinná praxe.

- Oproti úvodním hodnoceným oborům (studijní obory č. 1 a č. 2), je úroveň znalostí získaných v doménách s ID 01 a 02 velmi dobrá a tedy dostatečná. V doméně s ID 02 až výjimečná.
- Vyvážený absolventský profil je více univerzální, než v úvodních hodnocených oborech (studijní obory č. 1 a č. 2). Oproti studijnímu oboru č. 3 je však tento obor více technicky zaměřen. Předpokládá se uplatnění ve spíše technicky zaměřených profesích.
- Jako velmi problematická se jeví absence domény s ID 08, neboť je velmi pravděpodobné, že absolvent tohoto oboru může v praxi provádět penetrační testování či testy zranitelností. To může být bez znalostí etického kodexu a znalostí z etického hackingu velmi rizikové. V této doméně jsou znalosti absolventa hodnoceny jako nedostatečné.

- Za rizikové lze také považovat absenci hlubších znalostí z domény s ID 07. Zejména absence návaznosti ZKŘ na ZKB a další související předpisy. Absolvent tohoto oboru se bude v praxi s velkou pravděpodobností podílet na ochraně kritických informačních systémů, ideálně by tak měl disponovat znalostmi minimálně na úrovni základní orientace v problematice, aby se zvýšila jeho uplatnitelnost na trhu práce. Přesto lze vzhledem k počátečním kritériím hodnotit úroveň znalostí jako dostatečnou.
- Obor nezahrnuje povinně volitelné předměty, které by rozšiřovaly znalosti v oblasti bezpečnosti ICT.
- Velmi kladně lze hodnotit povinnost odborné praxe, která připravuje studenta na pracovní prostředí a usnadňuje pozdější proces adaptace.
- Pozitivně lze hodnotit zahrnutí unikátních předmětů zaměřených na zajištění fyzické bezpečnosti a na krizový management.
- Jako vhodné se jeví zakomponování současných trendů v ICT do osnov vybraných předmětů.

12.5. Studijní obor č. 5

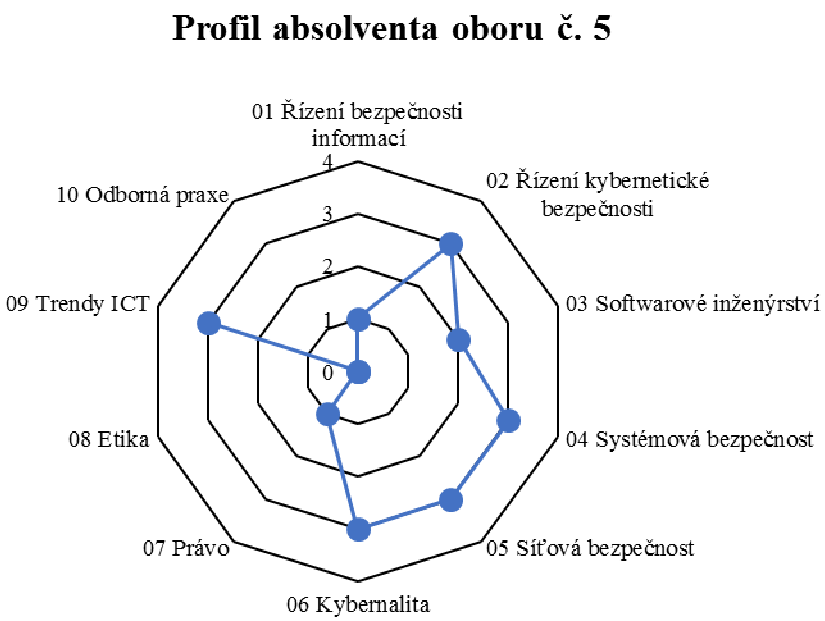
Znalostní doména	**Odpovídající předměty**	**ECTS**
01 Řízení bezpečnosti informací	Kryptografie a počítačová bezpečnost	**4**
	Součet ECTS kreditů:	**4**
Celková úroveň znalostní domény 01:	***Obecný přehled***	
02 Řízení kybernetické bezpečnosti	Bezpečnost v komunikacích	**4**
	Kryptografie a počítačová bezpečnost	**4**
	Kyberkriminalita	**3**
	Bezpečnost počítačových sítí datových center a cloudových služeb	**4**
	Součet ECTS kreditů:	**15**
Celková úroveň znalostní domény 02:	***Pokročilá orientace v problematice***	

03 Softwarové inženýrství	Počítačové viry a bezpečnost počítačových systémů	**4**
	Počítačová obrana a útok	**4**
	Součet ECTS kreditů:	**8**
Celková úroveň znalostní domény 03:	***Základní orientace v problematice***	
04 Systémová bezpečnost	Počítačové viry a bezpečnost počítačových systémů	**4**
	Kryptografie a počítačová bezpečnost	**4**
	Počítačová obrana a útok	**4**
	Součet ECTS kreditů:	**16**
Celková úroveň znalostní domény 04:	***Pokročilá orientace v problematice***	
05 Síťová bezpečnost	Multimediální komunikace a zabezpečení obsahu	**4**
	Bezpečnost v komunikacích	**4**
	Počítačová obrana a útok	**4**
	Bezpečnost počítačových sítí datových center a cloudových služeb	**4**
	Součet ECTS kreditů:	**16**
Celková úroveň znalostní domény 05:	***Pokročilá orientace v problematice***	
06 Kybernalita	Bezpečnost v komunikacích	**4**
	Počítačová obrana a útok	**4**
	Kyberkriminalita	**4**
	Součet ECTS kreditů:	**12**

Celková úroveň znalostní domény 06:	***Pokročilá orientace v problematice***	
07 Právo	Kyberkriminalita	**4**
	Součet ECTS kreditů:	**4**
Celková úroveň znalostní domény 07:	***Obecný přehled***	
08 Etika	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 08:	***Žádné znalosti a dovednosti***	
09 Trendy ICT	Multimediální komunikace a zabezpečení obsahu	**4**
	Bezpečnost v komunikacích	**4**
	Počítačové viry a bezpečnost počítačových systémů	**4**
	Počítačová obrana a útok	**4**
	Součet ECTS kreditů:	**16**
Celková úroveň znalostní domény 09:	***Pokročilá orientace v problematice***	
10 Odborná praxe	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 10:	***Žádné znalosti a dovednosti***	

Tab. 18: Pokrytí znalostních domén oboru č. 5

Profil absolventa dle uvedené metodiky:



Obr. 10: Profil absolventa č. 5

Shrnutí hodnocení:

V oboru převažují znalostní domény s ID 02, 04, 05 a 06. Obor je výrazně zaměřen na síťovou bezpečnost, kde jsou v rámci studijního plánu zahrnuty předměty jako „Bezpečnost v komunikacích“ a „Bezpečnost počítačových sítí datových center a cloudových služeb“ či „Počítačová obrana a útok“. Ta zahrnuje v osnově téma DDoS útoků a obranu proti nim. „Bezpečnost v komunikacích“ zase vhodně navazuje na témata kybernetické bezpečnosti (bezpečnostní týmy CSIRT a CERT, řízení bezpečnostních incidentů, atd.). Navíc se předmět věnuje zabezpečení bezdrátových sítí, jež nabývá v posledních letech vlivem IoT stále více na významu.

Obdobně jako ve studijním oboru č. 4, byla i zde pozornost věnována trendům v souvislosti s počítačovými viry. Předmět „Počítačové viry a bezpečnost počítačových systémů“ je opět předmětem, který svou osnovou naplňuje vícero znalostních domén. Věnuje se bezpečnosti od škodlivého kódu, tvorby a generování virů až po forenzní analýzu. V rámci předmětu „Kryptografie a počítačová bezpečnost“ jsou pak znalosti doplněny v doméně s ID 06. Obdobně široce uplatnitelný je předmět „Počítačová obrana a útok“, který byl zmíněn ve spojení se síťovou bezpečností, avšak jeho osnova zahrnuje i principy testování softwaru (penetrační testování, testování zranitelností, atd.), ale také forenzní analýzu a současné trendy v kybernetických útocích (např. vyděračský škodlivý software CryptoLocker).

Stěžejním předmětem oboru, který dává teoretický základ v oblasti kybernetické bezpečnosti je předmět „Kyberkriminalita“, který nezahrnuje pouze přehled kybernetických útoků a zmínku

o trestném chování v kyberprostoru, ale zaměřuje se také na znění ZKŘ a ZKB a činnost CSIRT a CSERT týmů. Zároveň dává obecný přehled o souvisejících právních normách, ochraně soukromí a ochraně autorských práv.

Závěr: Převažuje technické zaměření absolventa na zajištění kybernetické bezpečnosti bez etického základu a bez pokročilejších znalostí z oblasti řízení bezpečnosti informací. Doplněn hlubším kontextem z oblasti kybernality. V rámci oboru není povinná praxe.

- Oproti úvodním hodnoceným oborům (studijní obory č. 1 a č. 2), je úroveň znalostí v doméně s ID 02 velmi dobrá a tedy dostačující.
- Zcela nevhodná je absence domény s ID 01. Mezi doménou 01 a 02 existuje vztah, kdy doména 02 vychází z domény 01 a je od ní prakticky neoddělitelná. Úroveň znalostní domény 01 je z tohoto důvodu nedostatečná.
- Absencí požadované minimální úrovně znalostí v doméně s ID 01 je narušena komplexnost absolventského profilu a znalosti absolventů v doméně s ID 02 mohou vykazovat určité nedostatky.
- Jako velmi problematická se jeví absence domény s ID 08, neboť je velmi pravděpodobné, že absolvent tohoto oboru může v praxi provádět penetrační testování či testy zranitelností, což může být bez znalostí etického kodexu a znalostí z etického hackingu velmi rizikové. Zde je úroveň znalostí hodnocena jako nedostatečná.
- Za rizikové lze považovat absenci hlubších znalostí z domény s ID 07 a to z toho důvodu, že absolvent tohoto oboru se bude v praxi s velkou pravděpodobností podílet na ochraně kritických informačních systémů. V rámci oboru je sice minimální základní znalost ZKB a ZKŘ, nicméně bylo by vhodné disponovat znalostí na vyšší úrovni (například doplnění znalostí z ochrany osobních údajů, duševního vlastnictví, datových schránek, apod.). Přesto je vzhledem k počátečním definovaným kritériím úroveň dosažených znalostí absolventa dostatečná.
- Obor nezahrnuje povinně volitelné předměty, které by přímo rozšiřovaly znalosti v oblasti bezpečnosti ICT.
- V rámci oboru chybí možnost odborné praxe, kde by se studenti mohli seznámit s reálnými problémy z praxe.
- Jako obzvláště vhodné, se jeví zakomponování současných trendů v ICT do osnov vybraných předmětů.

- Velmi pozitivně lze hodnotit zaměření síťové bezpečnosti na zabezpečení cloudu a datových center, čímž jsou reflektovány současné trendy v ICT.
- Kladně lze hodnotit výuku současných trendů v kybernetických útocích a výuku obrany proti nim.

12.6. Studijní obor č. 6

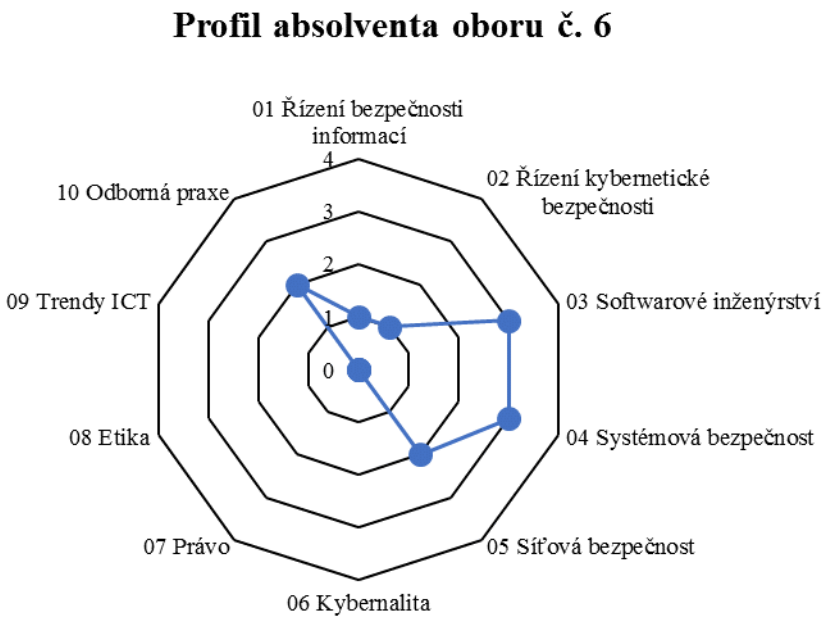
Znalostní doména	**Odpovídající předměty**	**ECTS**
01 Řízení bezpečnosti informací	Bezpečnost informačních systémů	**5**
	Součet ECTS kreditů:	**5**
Celková úroveň znalostní domény 01:	***Obecný přehled***	
02 Řízení kybernetické bezpečnosti	Bezpečnost informačních systémů	**5**
	Součet ECTS kreditů:	**5**
Celková úroveň znalostní domény 02:	***Obecný přehled***	
03 Softwarové inženýrství	Hardware/Software Codesign	**5**
	Funkcionální a logické programování	**5**
	Kódování a komprese dat	**5**
Součet ECTS kreditů:		**15**
Celková úroveň znalostní domény 03:	***Pokročilá orientace v problematice***	
04 Systémová bezpečnost	Hardware/Software Codesign	**5**
	Biometrické systémy	**5**
	Kryptografie	**5**
	Návrh, správa a bezpečnost	**5**
	Součet ECTS kreditů:	**20**

Celková úroveň znalostní domény 04:	***Pokročilá orientace v problematice***	
05 Síťová bezpečnost	Přenos dat, počítačové sítě a protokoly	**5**
	Návrh, správa a bezpečnost	**5**
	Součet ECTS kreditů:	**10**
Celková úroveň znalostní domény 05:	***Základní orientace v problematice***	
06 Kybernalita	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 06:	***Žádné znalosti a dovednosti***	
07 Právo	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 07:	***Žádné znalosti a dovednosti***	
08 Etika	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 08:	***Žádné znalosti a dovednosti***	
09 Trendy ICT	Není odpovídající předmět	**0**
Celková úroveň znalostní domény 09:	***Žádné znalosti a dovednosti***	
10 Odborná praxe	Odborná praxe	**6**[67]
Celková úroveň znalostní domény 10:	***Žádné znalosti a dovednosti***	

Tab. 19: Pokrytí znalostních domén oboru č. 6

[67] Předmět není hodnocen kredity. Pro potřeby hodnocení byl přepočítán na kredity a zaokrouhlen směrem nahoru.

Profil absolventa dle uvedené metodiky:



Obr. 11: Profil absolventa č. 6

Shrnutí hodnocení:

V rámci oboru jsou dominantně zastoupeny domény s ID 03 a 04. Doménu 03 znalostně naplňují předměty jako „Hardware/Software Codesign“ (zaměřeno na návrh a optimalizaci software či celých systémů) či „Funkcionální a logické programování“. V rámci těchto předmětů však chybí užší návaznost na bezpečnost ICT. Naopak u domény 03 se objevovaly předměty více spjaté s oblastí bezpečnosti ICT. Příkladem je předmět „Bezpečnost informačních systémů“, který zahrnoval témata jako kritéria hodnocení bezpečnosti informačních systémů, bezpečnost databází, bezpečnost operačních systémů, atd. Tento předmět taktéž pokrýval domény s ID 01 a 02 se základními pojmy v oblasti bezpečnosti ICT (hrozby, zranitelnosti, bezpečnostní opatření, aj.) a analýzou rizik.

Obor postrádal hlubší rozvinutí znalostí v doménách s ID 01 a 02 a vůbec celkovou návaznost ostatních domén na tyto domény. Ostatní povinné předměty neměly ve své osnově jasnou návaznost na bezpečnost ICT, ale spíše sloužily pro prohloubení znalostí právě v dominantních doménách s ID 03 a 04. Obor navíc postrádal možnost doplnit studijní plán o povinně volitelné předměty, které by chybějící znalosti z oblasti bezpečnosti ICT prohloubily.

Závěr: Převažuje technické zaměření absolventa na bezpečnost software a systémovou bezpečnost bez základních znalostí z řízení bezpečnosti informací a řízení kybernetické bezpečnosti a bez právního a etického základu. Bez kontextu z oblasti kybernality. V rámci oboru je povinná praxe.

- Úroveň znalostí v doménách s ID 01 a 02 je nedostatečná.
- Absencí požadované minimální úrovně znalostí v doménách s ID 01 a 02 je narušena vyváženost absolventského profilu a obor se tak stává méně univerzální.
- Jako velmi problematická se jeví absence domény s ID 08, neboť je velmi pravděpodobné, že absolvent tohoto oboru může v praxi provádět penetrační testování či testy zranitelností, což může být bez znalostí etického kodexu a znalostí z etického hackingu velmi rizikové. Úroveň dosažených znalostí absolventa v této doméně je hodnocena jako nedostatečná.
- Za nedostatečné a rizikové lze také považovat absenci hlubších znalostí z domény s ID 07 a to z toho důvodu, že absolvent tohoto oboru se může v praxi setkat s kritickými informačními systémy. V rámci oboru je minimální základní znalost ZKB a ZKŘ nezbytná.
- Obor nezahrnuje povinně volitelné předměty, které by rozšiřovaly znalosti v oblasti bezpečnosti ICT.
- V rámci oboru je zahrnuta praxe. Ta není zahrnuta v kreditním systému, nicméně je podmínku pro úspěšné absolvování oboru.
- V rámci oboru chybí zakomponování současných trendů v ICT do osnov předmětů.
- V rámci oboru chybí kontext z oblasti kybernality.

13. Hodnocení vzdělávání v oblasti bezpečnosti ICT

Pro nalezení mezer v současném vzdělávání v bezpečnosti ICT, byly výsledné absolventské profily analyzovaných oborů vloženy do jednoho grafu (viz. Obr. 12). Pro každou doménu byl spočítán průměr dle uvedené metodiky v kap. 10.1. – „Použitá metodika“. Výsledky hodnocení lze vidět v Tab. 20. Dle uvedených kritérií v použité metodice lze říci, že znalosti získané z analyzovaných oborů v doménách s ID 01 a 02 jsou dostačující a poskytují absolventům základní orientaci v problematice. Absolventi získávají základní přehled v doménách kybernetické bezpečnosti a bezpečnosti informací tématy jako například IT Governance, bezpečnost kritické informační infrastruktury, bezpečnostní politiky, řízení bezpečnostních incidentů, krizový management, krizové řízení a ochrana obyvatelstva, ale také bezpečnostní strategie ČR.

V těchto doménách v převážné většině chybělo pokrytí znalostních jednotek jako je „Řízení rizik“, „Řízení kontinuity činností“ a také pokrytí stěžejních znalostních jednotek „Základy bezpečnosti informací“ a „Základy kybernetické bezpečnosti“. V osnovách předmětů se téměř nikde neobjevily pojmy jako hrozba, aktivum, PDCA cyklus a ISMS, které byly definovány v teoretické části práce.

Obor	**Znalostní domény**									
	ID 01	**ID 02**	**ID 03**	**ID 04**	**ID 05**	**ID 06**	**ID 07**	**ID 08**	**ID 09**	**ID 10**
č. 1	3	2	2	3	2	2	0	0	1	0
č. 2	2	2	4	3	3	2	0	0	2	0
č. 3	3	3	4	4	3	3	3	1	0	0
č. 4	3	4	1	4	2	2	1	0	2	1
č. 5	1	3	2	3	3	3	1	0	3	0
č. 6	1	1	3	3	2	0	0	0	0	2
Průměr	2,2	2,5	2,7	3,3	2,5	2	0,8	0,2	1,3	0,5

Tab. 20: Hodnocení znalostních domén

Průměrná úroveň domén s ID 03 a 05 je vzhledem k počátečním kritériím dostačující a reflektuje původní očekávání, že úroveň domén bude o něco vyšší. Obdobně je tomu u domény 04, která byla celkově ve všech oborech nejdominantnější. To zejména z toho důvodu, že obsahově je schopna alespoň minimálně pokrýt témata jak softwarové, tak síťové bezpečnosti. Zabezpečení informačních systémů bez základních znalostí v síťové bezpečnosti a bezpečnosti software by nebylo zcela možné. Zejména důležité jsou pak témata jako řízení přístupů v informačních systémech, autentizace a kryptografie, na které je kladen důraz v ZKB. Velmi pozitivně lze hodnotit zařazení tématu forenzní analýzy do osnov studijních předmětů u převážné většiny oborů. V síťové bezpečnosti zase dominovala témata bezpečné komunikace, ochrany počítačových sítí pomocí firewallů, možnosti útoků, apod.

Velmi dobře v hodnocení dopadla doména s ID 06. Ta se téměř v každém studijním oboru vyskytovala napříč všemi předměty. To bylo také dáno poměrně velkým zaměřením na témata jako počítačové viry, metody útoku a obrana proti nim, páchání trestné činnosti prostřednictvím dark webů, vyšetřování trestné činnosti v kyberprostoru, apod. V osnovách chybělo naopak téma sociálního inženýrství. To bylo pouze v některých případech lehce nastíněno v souvislosti s phishingem. A v neposlední řadě lze zmínit i obsah znalostí v předmětech těchto oborů o kybernetické bezpečnosti na mezinárodní úrovni.

Velmi slabé byly domény s ID 07 a 08. Právní předpisy a aspekty práva obecně v ICT, ale také v bezpečnosti ICT u mnoha studijních oborů chyběly. Pouze jediný obor (obor č. 3) rozvíjel tyto znalosti do větší hloubky, čímž oproti ostatním naprosto vynikal. Také absolventský profil tohoto oboru se jevil jako více vyvážený (oproti ostatním) s větším rozsahem znalostí a vyšší úrovní znalostí. To bylo způsobeno především vhodným zakomponováním povinně volitelných předmětů do studijního plánu oboru, které byly zaměřeny na větší rozvinutí znalostí z oblasti bezpečnosti ICT. Studenti se tak například mohli věnovat pokročilým síťovým technologiím pro ochranu počítačových sítí.

U dvou oborů (obor č. 4 a č. 5) byl v rámci oboru poskytován obecný přehled v právu ICT a bezpečnosti ICT. Ten lze vzhledem k úvodním nastaveným kritériím tolerovat, nicméně absence hlubších znalostí z oblasti práva je velmi zarážející zejména v oborech profilující se zaměřením na kybernetickou bezpečnost a taktéž z hlediska požadavků praxe (viz. Příloha B). Pozorována byla také absence pojmu jako je ochrana osobních údajů, která bude vzhledem k brzké účinnosti GDPR dalším z požadavků na znalosti z hlediska pracovního trhu. Průměrně však tyto obory nedosahují ani obecného přehledu, z tohoto pohledu je současné vzdělávání v této doméně nedostačující.

Nejvíce krizová pak byla doména s ID 08, kde pouze jediný obor (obor č. 3) poskytoval alespoň obecný přehled o etickém chování v rámci kyberprostoru ale spíše zobecněně. Celkově je tak

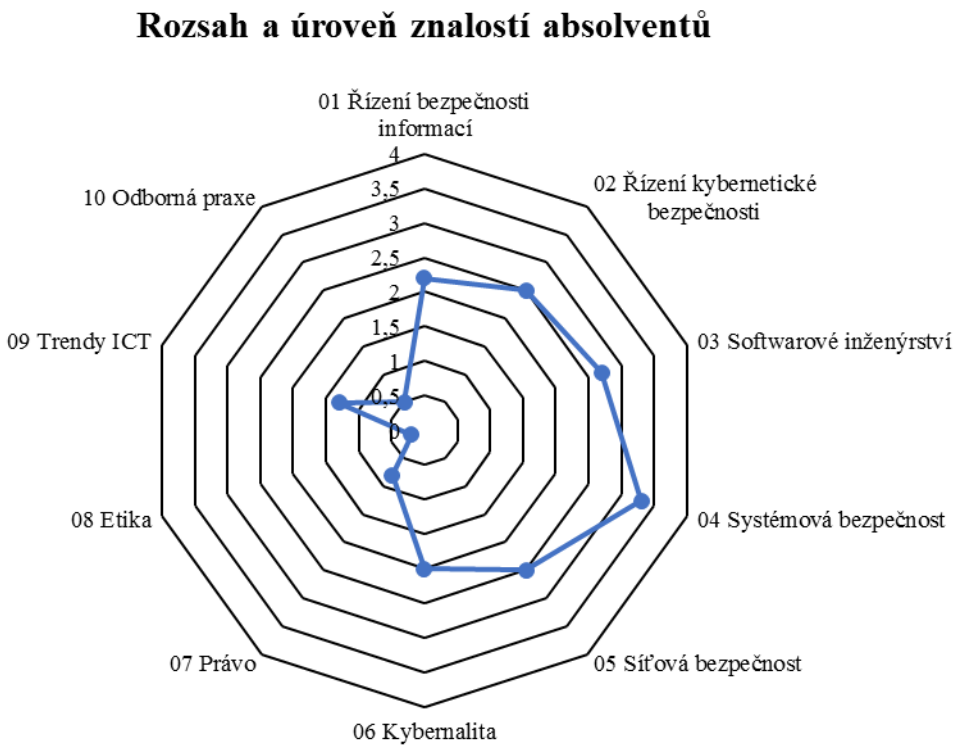
hodnoceno vzdělání v této doméně jako nedostačující. Přičemž v této znalostní doméně jde především o to, představit studentům základní principy profesní etiky a etiky hackingu. Současné vzdělávání tyto principy nedostatečně prosazuje, což může představovat poměrně velké bezpečnostní riziko.

Co lze považovat za pozitivum a co vyvrací zobecňování v tom smyslu, že v akademickém prostředí a výuce studentů chybí reflektování současných trendů v bezpečnosti ICT, je v těchto oborech alespoň obecný přehled o trendech v ICT. V rámci analýzy se ukázalo, že převážná většina analyzovaných oborů současné trendy v této oblasti reflektuje a pokud je to možné, snaží se do osnov většiny předmětů zakomponovat různá populární témata. Častým příkladem je biometrie a její využití pro autentizaci. Nebo také zabezpečení cloudu, ransomwarové útoky a jejich vývoj v čase, ale také phishing. V osnovách naopak chyběly trendy jako zabezpečení IoT, 3 D tisku či aspekty rozšířené reality. Doménu lze z hlediska nastavených kritérií hodnotit jako dostačující.

Poslední doména s ID 10 byla pokryta v rámci dvou studijních oborů (obor č. 4 a č. 6). U oboru č. 6 byla však časová dotace daleko vyšší, ačkoli předmět nebyl zahrnut do kreditního systému, ale jeho splnění bylo podmínkou pro úspěšné zakončení studijního oboru. Absolventi jsou díky tomu lépe připraveni na řešení konkrétních reálných problémů z praxe, přičemž lze očekávat, že jejich následná adaptace na pracovní prostředí bude po nástupu do zaměstnání rychlejší, než u absolventů ostatních oborů. Studenti navíc získávají možnost seznámit se s bezpečností v konkrétním prostředí – například finance, zdravotnictví, apod.

Vzniklé mezery, výsledný rozsah a průměrnou úroveň znalostí absolventů VŠ oborů v oblasti bezpečnosti ICT lze vidět na Obr. 12. Na základě provedené analýzy lze říci, že absolventi analyzovaných oborů svými znalostmi pokrývají stěžejní znalostní domény v dostačujícím rozsahu. Nicméně je potřeba napravit mezery v osnovách některých předmětů a zakomponovat pokrytí znalostních jednotek jako je „Řízení rizik“, „Řízení kontinuity činností“ a také pokrytí stěžejních znalostních jednotek „Základy bezpečnosti informací“ a „Základy kybernetické bezpečnosti“. Z výsledků je také zřejmá absence multidisciplinárního přístupu u mnoha oborů. Zejména téměř nulovou úrovní dosažených znalostí v oblasti etiky a velmi nízkou úrovní znalostí v oblasti práva.

Celkovou výuku by VŠ měly zaměřovat nejen na technická bezpečnostní opatření, ale také organizační bezpečnostní opatření. Tím zajistí absolventům větší uplatnitelnost na trhu práce. Absolventi mohou být v současnosti absencí těchto znalostí limitováni (např. nemohou být zaměstnáni jako konzultant kybernetické bezpečnosti). Studenti se v současnosti profilují více na technicky zaměřené profese (jako například administrátor bezpečnosti ICT).



Obr. 12: Rozsah a úroveň znalostí absolventů

Z pohledu požadavků pracovního trhu je nežádoucí absence právního a etického základu. Například pro pozici jako je penetrační tester či tester zranitelností může být absolvent bez povědomí o etickém hackingu a etického kodexu velmi rizikový. Ne však z pohledu, že by prováděl penetrační testování a ponechal zadní vrátka „kolegovi“, ale svou nevědomostí může ohrozit bezpečnost informací organizace například tím, že korektně neuzavře takové testování. Etický základ by tak měl vhodně doplnit stěžejní domény zaměřené na síťovou a systémovou bezpečnost a bezpečnost software.

V neposlední řadě se může negativně projevit absence hlubší znalosti v oblasti práva bezpečnosti ICT (např. při ucházení o pozice ve státní správě či u dodavatelů ICT bezpečnostního řešení pro státní správu za účelem ochrany kritické informační infrastruktury). Lze navíc očekávat s účinností GDPR, že budou požadavky na znalost právních předpisů ze strany pracovního trhu navýšeny. Další regulace, vzhledem ke kontinuálnímu vymezování hranic kyberprostoru, v budoucnu nelze s jistotou vyloučit. Předpokládat lze naopak větší nátlak na multidisciplinární přístup a mezioborové vzdělání (např. spojení studia práva a bezpečnosti ICT).

V prohloubení znalostí a zejména k získání klíčových znalostí, které byly kladeny na specialisty v bezpečnosti ICT v kap.11. – „Analýza pracovního trhu“, mohou pomoci povinné odborné praxe. V některých současných oborech se vyskytuje model, kdy povinná praxe není součástí kreditního systému, ale pro splnění studijního plánu a pro absolvování magisterského studia je

podmínkou. Studenti jí musí povinně absolvovat nad rámec standardního studijního plánu. Studenti tak mají možnost setkat se s bezpečností ICT v konkrétním prostředí. Problém v realizaci mohou představovat informace, které nejsou určeny široké veřejnosti. S těmi se lze setkat v praxi bezpečnosti ICT poměrně často.

13.1. SWOT analýza

Uvedená zjištění z hodnocení vzdělávání v oblasti bezpečnosti ICT lze využít jako vstupní informace pro SWOT analýzu. Ta se zaměřuje na zhodnocení silných a slabých stránek současného vzdělávání v oblasti bezpečnosti ICT v oborech, jež uvádí Tab. 6. Zároveň jsou v analýze shrnuty příležitosti a hrozby vyplývající se současného stavu.

SILNÉ STRÁNKY

1. V hodnocených oborech dominují znalostní domény zaměřené převážně na technické znalosti.
2. V hodnocených oborech jsou převážně reflektovány současné trendy v bezpečnosti ICT.
3. Většina absolventů má minimálně obecný přehled z oblasti forenzní analýzy.
4. Většina absolventů chápe minimální kontext bezpečnosti prostředí ICT a kybernality.
5. Existuje studijní obor, v rámci kterého studenti získávají hlubší znalosti z oblasti práva.
6. Některé studijní obory zahrnují povinnou odbornou praxi.

SLABÉ STRÁNKY

1. V hodnocených oborech chybí základní znalosti a některá teoretická východiska pro řízení bezpečnosti informací a řízení kybernetické bezpečnosti.
2. Některé hodnocené studijní obory nejsou dostatečně vyvážené z pohledu technického a organizačního zajištění bezpečnosti ICT.
3. V hodnocených oborech chybí základní znalosti z oblasti řízení rizik v bezpečnosti ICT.
4. Některé hodnocené studijní obory nezahrnují povinně volitelné předměty, které by prohlubovaly znalosti v oblasti bezpečnosti ICT.
5. Většina hodnocených studijních oborů zahrnuje pouze volitelné předměty vyznačující se velkou diverzitou.
6. Absolventi hodnocených oborů mají nedostatečné znalosti z oblasti práva.
7. Absolventi hodnocených oborů nemají etický základ v oblasti bezpečnosti ICT.

PŘÍLEŽITOSTI	HROZBY
1. Absolventi mohou být díky své specializaci kvalitními odborníky pro oblast bezpečnosti ICT se zaměřením na technické zabezpečení prostředí ICT.	1. Absolventi mohou být při svém uplatnění na pracovním trhu limitováni užším rozsahem znalostí (přílišnou specializací).
2. Znalosti studentů mohou být prohloubeny také o praktické dovednosti získané odbornou praxí.	2. Absolventi mohou být při svém uplatnění na pracovním trhu limitováni absencí alespoň obecného přehledu v právní problematice bezpečnosti ICT.
3. Odborná praxe může být zakomponována nad rámec studijního plánu. K tomu by bylo vhodné studenty dostatečně motivovat.	3. Absolventi mohou být při svém uplatnění na pracovním trhu limitováni absencí obecného přehledu v etice bezpečnosti ICT. Díky absenci obecného povědomí o etickém hackingu mohou představovat pro budoucí zaměstnavatele velké riziko.
4. Obory věnující se právním aspektům v bezpečnosti ICT do větší hloubky, mohou svými osnovami inspirovat ostatní.	5. K prohloubení nedostatků ve znalostech z oblasti práva mohou přispět změny v právních předpisech a příchod nových právních předpisů.
5. Studenti se společně s odborníky z akademického prostředí mohou podílet na návrhu etického kodexu pro oblast bezpečnosti ICT.	
6. Stávající výuka může být v oborech rozšířena o etiku a jiné související disciplíny.	

V neposlední řadě lze zmínit ohrožení těchto oborů a celkové produkce absolventů v důsledku poklesu zájmu o IT obory obecně. Na základě identifikovaných silných a slabých stránek současného vzdělávání v analyzovaných oborech a na základě identifikace příležitostí a hrozeb pro oblast vzdělávání v bezpečnosti ICT, by se strategie analyzovaných oborů měla zaměřit zejména na:

- **potlačení slabých stránek**
  - vyvážením studijních plánů, kde by znalosti byly rovnoměrně rozloženy mezi doménami zaměřenými na řízení bezpečnosti ICT, tj. domény s ID 01, 02 a na technické zajištění bezpečnosti ICT, tj. domény 03, 04 a 05;
  - doplněním základních znalostí a teoretických východisek v doménách s ID 01 a 02, které v současném vzdělávání v těchto oborech převážně chybí;
  - posílením znalostí v doméně s ID 07, u které lze předpokládat že poroste na významu;

- doplněním znalostí v doméně s ID 08 a zařazení etického základu do studijních osnov některých předmětů, případně vytvořit samostatný předmět zaměřený na spojení etiky a bezpečnosti ICT.

- **eliminaci hrozeb**
  - nižší uplatnění absolventů v důsledku užšího rozsahu znalostí (přílišné specializaci);
  - nižší uplatnění absolventů v důsledku absence alespoň obecného přehledu v právní problematice týkající se ICT a bezpečnosti ICT;
  - nižší uplatnění absolventů v důsledku absence etického základu, který je pracovním trhem požadován.

- **využití příležitostí**
  - obory mohou zakomponovat do svých studijních osnov minimální etický základ, zejména s důrazem na etické principy při testování bezpečnosti ICT;
  - obory mohou zakomponovat do svých studijních osnov právní problematiku a mohou se nechat inspirovat oborem, který absolventům poskytuje hlubší znalosti v právní problematice ICT a bezpečnosti ICT, a to dokonce na několika úrovních;
  - akademičtí pracovníci by se mohli společně se studenty podílet na tvorbě etického rámce pro oblast bezpečnosti ICT;
  - současná výuka by navíc mohla být prohloubena o získání praktických dovedností díky povinné odborné praxi.

K poslednímu bodu by bylo vhodné navázat užší spolupráci s komerční sférou. Zde by velmi pravděpodobně odborná výuka musela být nad rámec standardního studijního plánu a k jejímu absolvování by měli být studenti dostatečně motivováni. Zároveň by musel být vyřešen problém s přístupem k informacím, které nejsou určeny veřejnosti.

14. Závěr

Cílem práce bylo definovat minimální požadavky na znalosti a dovednosti pracovníků v oblasti bezpečnosti ICT a na základě analýzy současných magisterských studijních oborů věnující se této oblasti, stanovit strategii pro rozvoj vzdělávání v bezpečnosti ICT na technických vysokých školách. Požadavky na minimální klíčové znalosti a dovednosti pracovníků v oblasti bezpečnosti ICT byly na základě stanovené metodiky v kap. 10.1.1. – „Definice rolí a profesí v oblasti bezpečnosti ICT“ stanoveny v kap. 11. – „Analýza požadavků pracovního trhu“. Výsledkem byl popis profesní role „Specialista bezpečnosti ICT“ vhodná pro čerstvé absolventy věnující se oblasti bezpečnosti ICT. Definice této role, klíčové znalosti a dovednosti vycházejí z provedené analýzy požadavků pracovního trhu, z klasifikace zaměstnání dle standardu ANZSCO, z kompetenčního modelu „Competency Models for Enterprise and Cybersecurity“ a z teoretických východisek této práce.

Pro analýzu vybraných studijních oborů věnující se oblasti bezpečnosti ICT a nalezení mezer v současném vzdělávání v této oblasti, bylo nutné definovat kritéria hodnocení a základní znalostní domény, které byly v modelu hodnocení použity. Kritéria hodnocení vzdělávání v oblasti bezpečnosti ICT ve vybraných studijních oborech byla popsána v kap. „10. – Kritéria vzdělávání v oblasti bezpečnosti ICT“. Zvolená kritéria hodnocení brala v úvahu současné požadavky pracovního trhu. Pro hodnocení analyzovaných studijních oborů věnující se této oblasti byly definovány znalostní domény popsané v kap. 11.1. – Definice znalostních domén“. Struktura znalostních domén vycházela z požadavků pracovního trhu (viz. Příloha B) a analýzy provedené v kap. 11. – „Analýza požadavků pracovního trhu“, z doporučení kurikula CSEC2017 popsaného zejména v kap. „9.2.1. – Charakteristika studijního programu dle CSEC2017“ a z teoretických východisek této práce.

Dle nastavených kritérií hodnocení, bylo vzdělávání v současných oborech se zaměřením na bezpečnost ICT hodnoceno z hlediska úrovně pokrytí jednotlivých znalostních domén. Právě zde se projevily rozdíly v rozsahu znalostí absolventů analyzovaných studijních oborů, kde některé studijní obory byly až příliš úzce zaměřené na zajištění bezpečnosti ICT zejména z technického hlediska, bez základních znalostí z méně technicky zaměřených domén. To poukazuje na absenci multidisciplinárního přístupu, který bezpečnost ICT vyžaduje. Taktéž se projevily mezery ve znalostních doménách „Řízení bezpečnosti informací“ a „Řízení kybernetické bezpečnosti“. Zde chybělo pokrytí znalostních jednotek jako jsou „Základy bezpečnosti informací“ a „Základy kybernetické bezpečnosti“, „Řízení rizik“. Byla zaznamenána úplná absence základních pojmů jako riziko, hrozba, zranitelnost, PDCA cyklus.

Další výrazné mezery v osnovách studijních oborů vznikly ve znalostních doménách „Právo“ a „Etika“. Vzhledem k tomu, že i pracovní trh požaduje pokrytí těchto znalostních domén, byly chybějící znalosti hodnoceny jako nedostačující pro vzdělávání odborníků v bezpečnosti ICT. Právní oblast byla až nad očekávání pokryta pouze v rámci jednoho studijního oboru, který může svou studijní osnovou inspirovat zbylé studijní obory. Ten se stává příležitostí pro zlepšení v této oblasti. Dalším nedostatkem byla absence etického základu v naprosté většině analyzovaných studijních oborů. Etický základ je požadován zejména u pracovních profesí, jejichž primární činností je testování zranitelností či penetrační testování. Znalosti principů etického hackingu, jsou nezbytným předpokladem pro uplatnění absolventa. Nedostačující úroveň znalostí v těchto doménách snižují uplatnitelnost absolventů, zejména v oblasti kybernetické bezpečnosti, kde jsou základy práva a etických principů nepostradatelné.

U analyzovaných oborů se projevila snaha doplnit výuku v doménách jako „Softwarové inženýrství“, „Systémová bezpečnost“ či „Síťová bezpečnosti“ o kontext ze znalostní domény „Kybernalita“ a „Trendy ICT“. Absolventi se mohli seznámit s typickými útoky na bezpečnost ICT a s charakteristikou trestného chování v rámci kyberprostoru, stejně tak jako se současnými trendy nejen v ICT, ale také v bezpečnosti ICT. Zde se výuka soustřeďovala na vývoj hackerských technik a škodlivých kódů, ale také na biometrii a její využití v autentizaci či zabezpečení datových center a cloudů. Výsledné hodnocení tak vyvrátilo zobecňování typu, že akademické prostředí dostatečně nereflektuje současný vývoj trendů v ICT.

V analýze se také ukázalo, že některé analyzované studijní obory zahrnují ve svých studijních plánech odbornou praxi. Ta byla v rámci jednoho studijního oboru zařazena, vzhledem k časové náročnosti, nad rámec studijního plánu a vydělena z kreditového systému ECTS. Její absolvování bylo však jednou z podmínek pro úspěšné ukončení magisterského studia. Ukazuje se tak, že existuje snaha propojit akademickou a komerční sféru. To může výrazně přispět k pokročilejší orientaci absolventů v problematice bezpečnosti ICT, ale také k rychlejší adaptaci po nástupu do pracovního prostředí po ukončení studia. V případě zakomponování odborné praxe do studijních plánů, je nezbytné počítat s dostatečnou motivací studentů k absolvování praxe nad rámec studia a brát v úvahu problematiku týkající se zveřejňování informací, které nejsou určeny běžné veřejnosti.

V závěru práce byly výsledky hodnocení zaneseny do SWOT analýzy, která v kap. „13.1. – SWOT analýza“ hodnotí základní poznatky týkající se silných a slabých stránek současného vzdělávání v analyzovaných studijních oborech se zaměřením na bezpečnost ICT. Zde byly identifikovány hlavní příležitosti a hrozby, které z těchto nedostatků mohou plynout. K tomu byla dána základní doporučení pro nastavení strategie pro rozvoj vzdělávání v oblasti bezpečnosti ICT v magisterských studijních oborech věnující se této oblasti. Cílem strategie je potlačit

slabé stránky a eliminovat hrozby, a naopak využít příležitostí, které za současné situace v oblasti vzdělávání bezpečnosti ICT vznikají. Zejména se jedná o zakomponování minimálního etického základu do osnov těchto oborů, s důrazem na etické principy při testování bezpečnosti ICT. Taktéž zakomponování právní problematiky, kde se mohou tyto obory nechat inspirovat oborem, který absolventům poskytuje hlubší znalosti v právní problematice ICT a bezpečnosti ICT.

Seznam literatury

(1) LONG, Ju a Garry WHITE. On the global knowledge components in an information security curriculum–a multidisciplinary perspective. *Education and Information Technologies* [online]. 2010, 15(4), 317-331 [cit. 2017-11-11]. DOI: 10.1007/s10639-010-9121-0. ISSN 1360-2357. Dostupné z: http://link.springer.com/10.1007/s10639-010-9121-0

(2) EUROPEAN UNION. *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).* In: Brussels: European Parliament, Council of the European Union, 2016. Dostupné také z: http://eur-lex.europa.eu/eli/reg/2016/679/oj

(3) ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů*. 2014, ročník 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

(4) ČESKÁ REPUBLIKA. Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů.* 2014, ročník 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-316

(5) DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

(6) LUKÁŠ, Luděk. TEORIE BEZPEČNOSTI A TYPOLOGIE DRUHŮ BEZPEČNOSTI. *21. medzinárodná vedecká konferencia: Riešenie krízových situácií v špecifickom prostredí* [online]. Žilina: Fakulta bezpečnostného inžinierstva UNIZA, 2016, 324-331 [cit. 2017-02-12]. Dostupné z: http://fbiw.uniza.sk/rks/2016/articles/Lukas.pdf

(7) BOZP a PO: *Bezpečnost práce moderně a efektivně* [online]. Praha: CRDR spol. s r.o., 2017 [cit. 2017-02-12]. Dostupné z: http://www.bozp.cz/

(8) JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: první oficiální verze slovníku kybernetické bezpečnosti.* Vyd. 1. elektronické. Praha: Policejní akademie České republiky, 2012. ISBN 978-80-7251-377-2.

(9) Bezpečnost: Miroslav Mareš. Mendelova univerzita v Brně: *Elektronické studijní materiály* [online]. Brno: Mendelova univerzita v Brně [cit. 2017-02-12]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511

(10) *ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary.* International Organization for Standardization, International Electrotechnical Commission, 2016.

(11) Systém řízení informační bezpečnosti: Information security management system. *CyberSecurity.cz: Kybernetická bezpečnost* [online]. CyberSecurity.cz, c2010-2016 [cit. 2017-04-12]. Dostupné z: http://www.cybersecurity.cz/data/srib.pdf

(12) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(13) *ISO/IEC 27001:2013 - Information Security Management Systems – Requirements.* International Organization for Standardization, International Electrotechnical Commission, 2013.

(14) *ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security controls.* International Organization for Standardization, International Electrotechnical Commission, 2013.

(15) Transition guide: *Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013.* BSI group [online]. 2013 [cit. 2016-03-14]. Dostupné z: http://www.bsigroup.com/LocalFiles/en-GB/iso-iec-27001/resources/BSI-ISO27001-transition-guide-UK-EN-pdf.pdf

(16) *ISO/IEC 27005:2011 - Information technology - Security techniques - Information security risk management.* International Organization for Standardization, International Electrotechnical Commission, 2011.

(17) *ISO/IEC 27002:2005 - Information technology - Security techniques - Code of practice for information security management.* International Organization for Standardization, International Electrotechnical Commission, 2005.

(18) Normy ISO/IEC 27001 a 27002: Katalog opatření ISMS – oblasti bezpečnosti informací. *Vysoké učení technické v Brně* [online]. Brno: Vysoké učení technické v Brně, 2014 [cit. 2017-02-12]. Dostupné z: https://www.vutbr.cz/www_base/priloha.php?dpid=85292

(19) ČESKÁ REPUBLIKA. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. In: *Sbírka zákonů*. 2014. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-317

(20) ČESKÁ REPUBLIKA. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. In: *Sbírka zákonů*. 2010. Dostupné také z: https://www.zakonyprolidi.cz/cs/2010-432

(21) ČESKÁ REPUBLIKA. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In: *Sbírka zákonů*. 2000. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-240

(22) ČESKÁ REPUBLIKA. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: *Sbírka zákonů.* 2005. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-127

(23) *Národní centrum kybernetické bezpečnosti: Co je NCKB.* GovCERT.cz [online]. [cit. 2016-11-13]. Dostupné z: https://www.govcert.cz/

(24) *Národní bezpečnostní úřad* [online]. Národní bezpečnostní úřad [cit. 2016-11-13]. Dostupné z: https://www.nbu.cz/cs/

(25) ČESKÁ REPUBLIKA. Zákon č. 412/2005 o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů*. 2005. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

(26) RFC 2350 STANDARD: POPIS VLÁDNÍHO CERT ČESKÉ REPUBLIKY. *Národní centrum kybernetické bezpečnosti* [online]. Národní centrum kybernetické bezpečnosti, 2016 [cit. 2016-11-13]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/rfc-2350-standard/

(27) CSIRT: Úvod. *CSIRT.cz* [online]. [cit. 2016-11-13]. Dostupné z: https://www.csirt.cz/

(28) Bezpečnostní role: a jejich začlenění v organizaci. *Národní centrum kybernetické bezpečnosti* [online]. NBÚ, 2016 [cit. 2016-11-24]. Dostupné z: https://www.govcert.cz/download/kii-vis/container-nodeid-574/bezpecnostnirolev41.pdf

(29) JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. ISBN 978-80-247-1561-2.

(30) MAYEROVÁ, Iveta. *Zákon Sarbanes-Oxley, Interné kontroly nad finančným vykazovaním.* nám. Winstona Churchilla 1938/4, 130 67 Praha 3, 2006. Diplomová práce. Vysoká škola ekonomická v Praze. Vedoucí práce Prof. Ing. Jiří Dvořáček, CSc.

(31) PONEMON INSTITUTE LLC. 2016 Cost of Data Breach Study: Global Analysis. *IBM Offering Information.* 2016, 1.

(32) MARCHANT, Anne. Teaching ethics in the context of IT and globalization. In: *Proceedings of the 5th conference on Information technology education - CITC5 '04* [online]. New York, New York, USA: ACM Press, 2004, s. 227- [cit. 2017-04-16]. DOI: 10.1145/1029533.1029589. ISBN 1581139365. Dostupné z: http://portal.acm.org/citation.cfm?doid=1029533.1029589

(33) ČESKÁ REPUBLIKA. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů.* 2000. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-101

(34) MORGAN, Steve. IBM's CEO On Hackers: 'Cyber Crime Is The Greatest Threat To Every Company In The World'. *Forbes* [online]. 2015 [cit. 2017-03-18]. Dostupné z: https://www.forbes.com/sites/stevemorgan/2015/11/24/ibms-ceo-on-hackers-cyber-crime-is-the-greatest-threat-to-every-company-in-the-world/#5bb4fb2073f0

(35) Trocha historie. PŘIKRYL, Jan. *Jemný úvod do kryptografie* [online]. 2013, s. 3-5 [cit. 2017-03-21]. Dostupné z: http://euler.fd.cvut.cz/predmety/y2kk/kzk-krypto-uvod.pdf

(36) Historie Internetu v České republice. *Fakulta informatiky Masarykovy univerzity* [online]. [cit.2017-03-18]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/2000/xchlad.htm

(37) Cyber Threats and Dangers on the Deep (Dark) Web: Defining the Deep/Dark Web. *Kaspersky Lab* [online]. AO Kaspersky Lab., ©2017 [cit. 2017-03-18]. Dostupné z: https://usa.kaspersky.com/internet-security-center/threats/deep-web#.WM1tmjs1_IU

(38) DRASTICH, Martin. *Systém managementu bezpečnosti informací.* Grada Publishing, 2011. ISBN 9788024776163.

(39) *TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA*. United States: DEPARTMENT OF DEFENSE, 1983.

(40) *ISO/IEC 15408-1:2009 - Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model.* International Organization for Standardization, International Electrotechnical Commission, 2009.

(41) *ISO/IEC 17799:2000 - Information technology - Code of practice for information security management.* International Organization for Standardization, International Electrotechnical Commission, 2000.

(42) *ČSN ISO/IEC 17799:2001 - Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.* Český normalizační institut, 2001.

(43) *THE NATIONAL STRATEGY TO SECURE CYBERSPACE* [online]. Washington: THE WHITE HOUSE WASHINGTON, 2003 [cit. 2017-04-13]. Dostupné z: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

(44) *STRATEGIE PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY NA OBDOBÍ 2012 - 2015* [online]. Národní bezpečnostní úřad, 2012 [cit. 2017-04-13]. Dostupné z: https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieprooblastkbnbu.pdf

(45) *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* [online]. Národní bezpečnostní úřad, 2012 [cit. 2017-04-13]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf

(46) EU. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* In: Brussels: European Parliament and the Council of the European Union, 2016. Dostupné také z: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

(47) *Návrh na změnu zákona o kybernetické bezpečnosti - transpozice směrnice NIS* [online]. Národní bezpečnostní úřad, 2016 [cit. 2017-04-13]. Dostupné z: https://www.nbu.cz/cs/aktualne/1161-navrh-na-zmenu-zakona-o-kyberneticke-bezpecnosti-transpozice-smernice-nis/

(48) ČESKÁ REPUBLIKA. Zákon č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.In: *Sbírka zákonů.* 1992. Dostupné také z: https://www.psp.cz/sqw/sbirka.sqw?cz=256&r=1992

(49) Historie Úřadu pro ochranu osobních údajů. *Úřad pro ochranu osobních údajů: The Office for Personal Data Protection* [online]. Úřad pro ochranu osobních údajů, c2013 [cit. 2017-04-13]. Dostupné z: https://www.uoou.cz/historie-uradu-pro-ochranu-osobnich-udaju/ds-1061/archiv=0&p1=1059

(50) ČESKÁ REPUBLIKA. Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů.* 2005. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

(51) ČESKÁ REPUBLIKA. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů. In: *Sbírka zákonů.* 2000. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-365

(52) ČESKÁ REPUBLIKA. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). In: *Sbírka zákonů České republiky*. Ministerstvo vnitra ČR, 2005. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-127

(53) ČESKÁ REPUBLIKA. Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. In: *Sbírka zákonů České republiky*. Ministerstvo vnitra ČR, 1999. Dostupné také z: https://www.zakonyprolidi.cz/cs/1999-106

(54) MACDOUGALL, William. *INDUSTRIE 4.0: Smart Manufacturing for the Future* [online]. Berlin: Germany Trade and Invest, 2014 [cit. 2017-03-25]. Dostupné z: https://www.gtai.de/GTAI/Content/EN/Invest/_SharedDocs/Downloads/GTAI/Brochures/Industries/industrie4.0-smart-manufacturing-for-the-future-en.pdf

(55) MAŘÍK, Vladimír et al. *NÁRODNÍ INICIATIVA PRŮMYSL 4.0* [online]. Praha: Ministerstvo obchodu a průmyslu, 2015 [cit. 2017-03-25]. Dostupné z: http://www.spcr.cz/images/priloha001-2.pdf

(56) Avast cyber security predictions for 2017. *AVAST Software, Inc. [US]: Blog* [online]. AVAST Software, Inc. [US], 2017 [cit. 2017-03-25]. Dostupné z: https://blog.avast.com/avast-cyber-security-predictions-for-2017

(57) Emory Healthcare hit by ransomware, data of over 200,000 patients hacked. *Healthcare IT news: Privacy & Security* [online]. 2017 [cit. 2017-03-25]. Dostupné z: http://www.healthcareitnews.com/news/emory-healthcare-hit-ransomware-data-over-200000-patients-hacked

(58) Free Ransomware Decryptors. *Kaspersky Lab* [online]. Kaspersky Lab, c1997-2017 [cit. 2017-04-16]. Dostupné z: https://noransom.kaspersky.com/

(59) O nás: Statistiky řešených incidentů. *CSIRT.CZ* [online]. CSIRT.CZ, 2017 [cit. 2017-03-25]. Dostupné z: https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/.

(60) TOP 25 nejpoužívanějších hesel roku 2015. *Globe24.cz* [online]. Globe24.cz, 2016 [cit. 2017-04-13]. Dostupné z: https://globe24.cz/technika/14546-top-25-nejpouzivanejsich-hesel-roku-2015

(61) *McAfee Labs 2017 Threats Predictions* [online]. McAfee Labs, 2016 [cit. 2017-04-13]. Dostupné z: https://www.mcafee.com/us/resources/reports/rp-threats-predictions-2017.pdf

(62) Cloud Security Alliance Establishes New Third-Party Consultancy Program to Ensure Best Practices in Secure Cloud Implementation. *CSA - Cloud Security Alliance* [online]. San Francisco: Cloud Security Alliance, 2017 [cit. 2017-04-16]. Dostupné z: https://cloudsecurityalliance.org/media/news/cloud-security-alliance-establishes-new-third-party-consultancy-program-to-ensure-best-practices-in-secure-cloud-implementation/

(63) CHMELAŘ, Aleš a kol. *Dopady digitalizace na trh práce v ČR a EU: Příspěvek k vývoji hospodářského modelu ČR* [online]. Praha: Úřad vlády České republiky, c2015, s. 10-11 [cit. 2017-04-16]. Dostupné z:https://www.vlada.cz/assets/evropske-zalezitosti/analyzy-EU/Dopady-digitalizace-na-trh-prace-CR-a-EU.pdf

(64) 2017 Global Information Security Workforce Study [online]. Frost & Sullivan [cit. 2017-04-13]. Dostupné z: https://iamcybersafe.org/research_millennials/

(65) Odvětví informační ekonomiky. *Český statistický úřad* [online]. Český statistický úřad [cit. 2017-04-17]. Dostupné z: https://www.czso.cz/csu/czso/odvetvi-informacni-ekonomiky

(66) Definice a vymezení ICT sektoru. *Český statistický úřad* [online]. Český statistický úřad [cit. 2017-04-17]. Dostupné z: https://www.czso.cz/documents/10180/20561137/970711_e.pdf/cac3d9f8-d9f5-46fb-88bd-7af0504d8327?version=1.0

(67) *Cybersecurity Professional Trends: A SANS Survey* [online]. SANS Institute, 2014 [cit. 2017-04-13].Dostupné z:https://www.sans.org/reading-room/whitepapers/analyst/cybersecurity-professional-trends-survey-34615

(68) Klasifikace zaměstnání (CZ-ISCO). *Český statistický úřad* [online]. Český statistický úřad, 2017 [cit. 2017-04-13]. Dostupné z: https://www.czso.cz/csu/czso/klasifikace_zamestnani_-cz_isco-

(69) SDĚLENÍ Českého statistického úřadu: ze dne 16. června 2010 o zavedení Klasifikace zaměstnání (CZ-ISCO). *Český statistický úřad* [online]. Český statistický úřad, 2017 [cit. 2017-04-13]. Dostupné z: https://www.czso.cz/documents/10180/23164307/sdeleni_csu_206_2010.pdf/63f1f15d-793c-4ecc-aeb8-240b75aca6d5?version=1.0

(70) Informační ekonomika v číslech - 2016. *Český statistický úřad* [online]. Český statistický úřad, 2017 [cit. 2017-04-13]. Dostupné z: https://www.czso.cz/csu/czso/informacni-ekonomika-v-cislech

(71) USD průměrné kurzy 2013, historie kurzů měn. *Kurzy.cz* [online]. Český statistický úřad, c2000-2017 [cit. 2017-04-13]. Dostupné z:http://www.kurzy.cz/kurzy-men/historie/USD-americky-dolar/2013/

(72) Statistiky: ICT odborníci. *Český statistický úřad* [online]. ČSÚ, 2016 [cit. 2017-04-16]. Dostupné z: https://www.czso.cz/csu/czso/ict-odbornici

(73) I v roce 2016 bude nedostatek IT odborníků. *BusinessIT* [online]. 2016 [cit. 2017-04-13]. Dostupné z: http://www.businessit.cz/cz/i-v-roce-2016-bude-nedostatek-it-odborniku.php

(74) *PLATOVÝ PRŮZKUM HAYS PRACOVNÍ TRH V ROCE 2016: Přehled platů a motivace zaměstnanců na českém trhu v roce 2016* [online]. Hays, 2016 [cit. 2017-04-13]. Dostupné z: https://www.hays.cz/cs/groups/hays_common/@cz/@content/documents/digitalasset/hays_1602080.pdf

(75) ISPV - Informační systém o průměrných výdělcích: Aktuální výsledky podle zaměstnání za rok 2016. Ministerstvo práce a sociálních věcí [online]. Praha: *Ministerstvo práce a sociálních věcí.* [cit.2017-04-05]. Dostupné z: http://www.mpsv.cz/ISPV.php?sfera=1&sz=2&txt=&ok=Najdi

(76) Co ovlivňuje přijímání absolventů v sektoru informací, financí a vzdělávání. *Informační systém o uplatnění absolventů škol na trhu práce* [online]. 2014 [cit. 2017-04-13]. Dostupné z: http://www.infoabsolvent.cz/Temata/ClanekAbsolventi/4-1-19/Co-ovlivnuje-prijimani-absolventu-v-sektoru-/26

(77) DOLEŽALOVÁ, Mgr. Gabriela. *Potřeby zaměstnavatelů a připravenost absolventů škol – šetření v kvartérním sektoru* [online]. Praha: Národní ústav pro vzdělávání, školské poradenské zařízení a zařízení pro další vzdělávání pedagogických pracovníků, 2014 [cit. 2017-04-13]. Dostupné z:file:///C:/Users/sulan/Downloads/F-9.0.92_Potreby_zamestnavatelu_a_pripravenost_absolventu_skol__setreni_v_kvarternim_sektoru__2014.pdf

(78) Share of the population by level of educational attainment, by selected age groups and country, 2015. Eurostat Statistics Explained [online]. *Eurostat*, 2017 [cit. 2017-04-05]. Dostupné z: http://ec.europa.eu/eurostat/statisticsexplained/index.php/File:Share_of_the_population_by_level_of_educational_attainment,_by_selected_age_groups_and_country,_2015_(%25).png

(79) Osoby s terciárním vzděláním, studenti a absolventi terciárního vzdělávání: Analýza: Osoby s terciárním vzděláním v České republice (2000–2015). *Český statistický úřad: Statistiky* [online]. Český statistický úřad, 2017 [cit. 2017-04-05]. Dostupné z: https://www.czso.cz/csu/czso/osoby-s-terciarnim-vzdelanim-studenti-a-absolventi-vysokych-skol

(80) SIMS 2.0: Sdružené informace matrik studentů. *Ministerstvo školství, mládeže a tělovýchovy* [online]. MŠMT ČR, ÚVT MU [cit. 2017-04-13]. Dostupné z: https://sims.msmt.cz/Default.aspx?pozadovanaStranka=Default.aspx

(81) Metodika - Mezinárodní klasifikace vzdělání ISCED 97. *Český statistický úřad* [online]. Český statistický úřad [cit. 2017-04-13]. Dostupné z: https://www.czso.cz/csu/czso/metodika_mezinarodni_klasifikace_vzdelani_isced_97

(82) Osoby s terciárním vzděláním, studenti a absolventi terciárního vzdělávání. *Český statistický úřad* [online]. Český statistický úřad [cit. 2017-04-13]. Dostupné z: https://www.czso.cz/csu/czso/osoby-s-terciarnim-vzdelanim-studenti-a-absolventi-vysokych-skol

(83) Studenti a absolventi vysokoškolského studia v oboru Informatika. *Český statistický úřad* [online]. Český statistický úřad [cit. 2017-04-13]. Dostupné z: https://www.czso.cz/csu/czso/studenti_a_absolventi_vysokoskolskeho_studia_v_oboru_informatika

(84) Výroční zprávy: Výroční zpráva za rok 2015. *Fakulta informačních technologií: Vysokého učení technického v Brně* [online]. Vysoké učení technické v Brně, 2015 [cit. 2017-04-05]. Dostupné z: http://www.fit.vutbr.cz/FIT/vz/

(85) VŠ OBORY V OBLASTI KYBER BEZPEČNOSTI. *Národní centrum kybernetické bezpečnosti* [online]. NCKB [cit. 2017-04-13].
Dostupné z: https://www.govcert.cz/cs/vzdelavani/vs-obory-v-oblasti-kyber-bezpecnosti/

(86) DATA O STUDENTECH, POPRVÉ ZAPSANÝCH A ABSOLVENTECH VYSOKÝCH ŠKOL. *Ministerstvo školství, mládeže a tělovýchovy* [online]. MŠMT [cit. 2017-04-13]. Dostupné z: http://www.msmt.cz/vzdelavani/skolstvi-v-cr/statistika-skolstvi/data-o-studentech-poprve-zapsanych-a-absolventech-vysokych

(87) ENGEL, GERALD L. a OSCAR N. GARCIA. *Computer science and computer engineering: A review and overview of curriculum development* [online]. National Computer Conference, 1978 [cit. 2017-03-21]. Dostupné z:
https://www.computer.org/csdl/proceedings/afips/1978/5086/00/50861197.pdf

(88) ATCHISON, William F., Earl J. SCHWEPPE, William VIAVANT, et al. Curriculum 68: Recommendations for academic programs in computer science. *Communications of the ACM* [online]. 11(3), 151-197 [cit. 2017-03-21]. DOI: 10.1145/362929.362976. ISSN00010782. Dostupné z: http://portal.acm.org/citation.cfm?doid=362929.362976

(89) Education: Curricula Recommendations. *Association for Computing Machinery* [online]. ACM, c2017 [cit. 2017-03-21]. Dostupné z:http://www.acm.org/education/curricula-recommendations

(90) *Cybersecurity Curricula 2017: Curriculum Guidelines for Undergraduate Degree Programs in Cybersecurity* [online]. ACM, IEEE-CS, 2017 [cit. 2017-04-13]. Dostupné z: https://media.wix.com/ugd/895bd2_2d799fac868643a4a4e6902d9fe77e7f.pdf

(91) DOUCEK, Petr. *Lidské zdroje v ICT: analýza nabídky a poptávky po IT odbornících v ČR.* Praha: Professional Publishing, 2007. ISBN 978-80-86946-51-1.

(92) DRAFT NICE Cybersecurity Workforce Framework (NCWF): National Initiative for Cybersecurity Education. *NIST - National Institute of Standards and Technology* [online]. National Institute of Standards and Technology, U.S. Department of Commerce, 2016 [cit. 2017-04-13]. Dostupné z: http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf

(93) Competency Models for Enterprise Security and Cybersecurity: Research-Based Frameworks for Talent Solutions. *ASIS Foundation* [online]. Apollo Education Group, c2015 [cit. 2017-04-13]. Dostupné z: https://foundation.asisonline.org/Documents/Competency%20Models%20for%20Enterprise%20and%20Cybersecurity.pdf

(94) 1220.0 - ANZSCO - Australian and New Zealand Standard Classification of Occupations, First Edition, Revision 1. *Australian Bureau of Statistics* [online]. Computer Hope [cit. 2017-04-13]. Dostupné z: http://www.abs.gov.au/ausstats/abs@.nsf/Previousproducts/1220.0Search0First%20Edition,%20Revision%201

(95) 1220.0 - ANZSCO - Australian and New Zealand Standard Classification of Occupations, First Edition, Revision 1: UNIT GROUP 2621 DATABASE AND SYSTEMS ADMINISTRATORS, AND ICT SECURITY SPECIALISTS. *Australian Bureau of Statistics* [online]. [cit. 2017-04-14]. Dostupné z: http://www.abs.gov.au/ausstats/abs@.nsf/Product+Lookup/1220.0~First+Edition,+Revision+1~Chapter~UNIT+GROUP+2621+Database+and+Systems+Administrators,+and+ICT+Security+Specialists

(96) 1220.0 - ANZSCO - Australian and New Zealand Standard Classification of Occupations, First Edition, Revision 1. *Australian Bureau of Statistics* [online]. Computer Hope [cit. 2017-04-13]. Dostupné z: http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/1220.0First%20Edition,%20Revision%201?OpenDocument

(97) 2529 Specialisté v oblasti bezpečnosti dat a příbuzní pracovníci. *CZ-ISCO: Klasifikace zaměstnání ISCO* [online]. CZ-ISCO, c2017 [cit. 2017-04-14]. Dostupné z: http://www.cz-isco.cz/isco/2529-specialiste-v-oblasti-bezpecnosti-dat-a-pribuzni-pracovnici/

(98) UNIT GROUP 1351 ICT MANAGERS. *CZISCO: Klasifikace zaměstnání ISCO* [online]. CZ-ISCO, c2017 [cit. 2017-04-14]. Dostupné z: http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/7F69EDFAC48B7D3DCA257B960020A809?opendocument

(99) Bezpečnost (Miroslav Mareš). *Mendelova univerzita v Brně* [online]. Mendelova univerzita v Brně [cit. 2017-04-13]. Dostupné z: https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=69511

(100) Modely řízení přístupu. *IBM Knowledge Center* [online]. IBM [cit. 2017-04-13]. Dostupné z:
https://www.ibm.com/support/knowledgecenter/cs/SSTFWV_5.1.0/com.ibm.itim.doc/cpt/cpt_ic_plan_role_issues_models_acc.html

(101) Symetrická kryptografie. *Mendelova univerzita v Brně* [online]. Mendelova univerzita v Brně [cit. 2017-04-13]. Dostupné z:
https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=7026

(102) Algoritmus RSA. *Algoritmy.net* [online]. Jan Neckář, c2016 [cit. 2017-04-05]. Dostupné z: https://www.algoritmy.net/article/4033/RSA

(103) Základy kryptografie pro manažery: hashovací funkce. *Clever and smart* [online]. Miroslav Čermák, c2008-2017 [cit. 2017-04-05]. Dostupné z:
http://www.cleverandsmart.cz/zaklady-kryptografie-pro-manazery-hashovaci-funkce/

(104) Úvod do kryptologie: Digitální podepisování pomocí asymetrické kryptografie. *Kmlinux* [online]. Mendelova univerzita v Brně, 2010 [cit. 2017-04-13]. Dostupné z: https://kmlinux.fjfi.cvut.cz/~balkolub/Vyuka/Digitalni_podpis.pdf

(105) ČESKÁ REPUBLIKA. Zákon č. 227/2000 Sb., o elektronickém podpisu. In: *Sbírka zákonů* České republiky. Ministerstvo vnitra České republiky, 2000. Dostupné také z:
http://www.mvcr.cz/clanek/zakon-c-227-2000-sb-o-elektronickem-podpisu.aspx

(106) Key Management. *Microsoft: TechNet* [online]. Microsoft, c2017 [cit. 2017-04-05]. Dostupné z: https://technet.microsoft.com/en-us/library/cc961626.aspx

(107) *Kryptografické protokoly* [online]. 2011 [cit. 2017-04-13]. Dostupné z:
http://www.obluda.cz/iprednasky/15_proto.pdf

(108) Úvod do kryptologie. *Mendelova univerzita v Brně* [online]. Mendelova univerzita v Brně [cit. 2017-04-13]. Dostupné z:
https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=21331

(109) Teorie čísel. *FJFI* [online]. [cit. 2017-04-13]. Dostupné z:
http://people.fjfi.cvut.cz/pelanedi/SpolecnaTeorieCisel090409.pdf

(110) Pravděpodobnost. *Fakulta elektrotechniky a komunikačních technologií VUT v Brně: Ústav matematiky* [online]. Fakulta elektrotechniky a komunikačních technologií VUT v Brně [cit. 2017-04-13]. Dostupné z:
http://www.umat.feec.vutbr.cz/~hlavicka/vyuka/BMA3_predn/prednaska01.pdf

(111) Definice pravděpodobnosti. *ČVUT Fakulta elektrotechnická: Katedra matem*atiky [online]. ČVUT Fakulta elektrotechnická [cit. 2017-04-13]. Dostupné z:
https://math.feld.cvut.cz/ftp/prucha/m3c/predn/pravd/u2.pdf

(112) Přenos informace: Systémy pro sběr a přenos dat. *ČVUT Fakulta elektrotechnická: Katedra měření* [online]. ČVUT Fakulta elektrotechnická [cit. 2017-04-13]. Dostupné z: http://measure.fel.cvut.cz/system/files/files/cs/vyuka/predmety/A4B38DSP/4_Information_Theory_cz.pdf

(113) Virtuální privátní sítě. *Microsoft: TechNet* [online]. Microsoft, c2017 [cit. 2017-04-05]. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd469653(v=ws.11).aspx)

(114) Objektově orientované programování (1): O co se vlastně jedná. *Populárně naučný portál: Popular* [online]. [cit. 2017-04-05]. Dostupné z: http://popular.fbmi.cvut.cz/it/Stranky/OOP1---O-co-jde.aspx

(115) Moduly a knihovny. *VUT v Brně: Fakulta informačních technologií* [online]. VUT v Brně [cit. 2017-04-13]. Dostupné z: http://www.fit.vutbr.cz/~martinek/clang/modules.html

(116) Architektura klient/server a třívrstvá architektura. *VUT v Brně: Fakulta informačních technologií* [online]. VUT v Brně [cit. 2017-04-13]. Dostupné z: http://www.fit.vutbr.cz/study/courses/DSI/public/pdf/nove/10_clsrv.pdf

(117) Dekompozice problému, rekurze. *Edux.fit.cvut.cz* [online]. ČVUT, 2016 [cit. 2017-04-13]. Dostupné z: https://edux.fit.cvut.cz/courses/BI-PA1/_media/lectures/l10-recursion-cz.pdf

(118) What is open source? *Opensource.com* [online]. Opensource.com [cit. 2017-04-13]. Dostupné z: https://opensource.com/resources/what-open-source

(119) 2. díl - UML - Use Case Diagram. *Itnetwork.cz* [online]. itnetwork.cz, c2017 [cit. 2017-04-05]. Dostupné z: http://www.itnetwork.cz/navrhove-vzory/uml/uml-use-case-diagram

(120) BEHRINGER, Michael H. End-to-End Security: *The Internet Protocol Journal. The Internet Protocol Journal* [online]. Cisco Systems, 12(3) [cit. 2017-04-13]. Dostupné z: http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-45/123-security.html

(121) Defense In Depth. *SANS Information Security Training* [online]. c2000-2017 [cit. 2017-04-13]. Dostupné z: https://www.sans.org/reading-room/whitepapers/basics/defense-in-depth-525

(122) Specifikace požadavků dle IEEE standardu. *VUT v Brně: Fakulta informačních technologií* [online]. VUT v Brně [cit. 2017-04-13]. Dostupné z: http://www.fit.vutbr.cz/study/courses/RPS/public/pro-vytah.html

(123) Bezpečnost a bezpečné programování. *Edux.fit.cvut.cz: Fakulta informačních technologií* [online]. ČVUT [cit. 2017-04-13]. Dostupné z: https://edux.fit.cvut.cz/oppa/MI-BPR/prednasky/bpr-1.pdf

(124) Bezpečnost a bezpečné programování. *Edux.fit.cvut.cz: Fakulta informačních technologií* [online]. ČVUT [cit. 2017-04-13]. Dostupné z: https://edux.fit.cvut.cz/oppa/MI-BPR/prednasky/bpr-1.pdf

(125) Zranitelnost desetiletí aneb když přeteče zásobník…. *Computer World* [online]. IDG Czech Republic [cit. 2017-04-05]. Dostupné z: http://computerworld.cz/securityworld/zranitelnost-desetileti-aneb-kdyz-pretece-zasobnik-46243

(126) Softwarové inženýrství I: Ověřování správnosti softwaru. *VŠFS - Veřejné služby Informačního systému* [online]. [cit. 2017-04-13]. Dostupné z: https://is.vsfs.cz/el/6410/zima2013/N_SWI_1/um/beam004.txt

(127) Ochrana před ztrátou dat – systémy DLP. SystemOnLine.cz: *S přehledem ve světě informačních technologií* [online]. CCB, c2001-2017 [cit. 2017-04-05]. Dostupné z: https://www.systemonline.cz/it-security/ochrana-pred-ztratou-dat-systemy-dlp.htm

(128) Testování bílé a černé skříňky (white box, black box, grey box). *Testování softwaru* [online]. [cit. 2017-04-05]. Dostupné z: http://testovanisoftwaru.cz/tag/white-box/

(129) Penetrační testy. *Linux Services* [online]. Linux Services, c2017 [cit. 2017-04-05]. Dostupné z: https://www.linuxservices.cz/penetracni-testy

(130) Řešení pro výkonnostní a bezpečnostní testování Spirent CyberFlood. *TR instruments: Měřicí přístroje a systémy* [online]. Brno: TR instruments [cit. 2017-04-05]. Dostupné z: http://www.trinstruments.cz/spirent-cyberflood

(131) Bezpečnost PHP [1] - *SQL Injection. PHP-Fusion* [online]. PHP-Fusion, c2002-2017 [cit. 2017-04-05]. Dostupné z: http://www.phpfusion.cz/articles.php?article_id=31

(132) Výjimky. *Výuka programování a softwarového inženýrství na KIT VŠE* [online]. [cit. 2017-04-13]. Dostupné z: https://java.vse.cz/pdf/skripta-vyjimky.pdf

(133) Autentizační metody založené na biometrických informacích. *Access server* [online]. ČVUT FEL, 2010 [cit. 2017-04-13]. Dostupné z: http://access.feld.cvut.cz/view.php?cisloclanku=2010110002

(134) Vícefaktorová autentizace: Jak vypadá praxe? *Computer World* [online]. IDG Czech Republic [cit. 2017-04-05]. Dostupné z: http://computerworld.cz/securityworld/vicefaktorova-autentizace-jak-vypada-praxe-51923

(135) Systémový bezpečnostní audit. *SystemOnLine.cz: S přehledem ve světě informačních technologií* [online]. CCB, c2001-2017 [cit. 2017-04-05]. Dostupné z: https://www.systemonline.cz/clanky/systemovy-bezpecnostni-audit.htm

(136) IDS: základní informace. *Computer World* [online]. IDG Czech Republic [cit. 2017-04-05]. Dostupné z: http://computerworld.cz/securityworld/ids-zakladni-informace-46154

(137) Internet of Things: propojená budoucnost. Svět hardware: Vše ze světa počítačů [online]. oXy Online, c1998-2015 [cit. 2017-04-05]. Dostupné z: http://www.svethardware.cz/internet-of-things-propojena-budoucnost/39560

(138) Forenzní analýza dat. *Mgr. Martin Ludma: Soudní znalec IT od r. 2007* [online]. Olomouc [cit. 2017-04-08]. Dostupné z: http://www.martinludma.cz/forenzni-analyza-dat

(139) Identity and Access Management (IAM). *Gartner* [online]. Gartner, c2017 [cit. 2017-04-08]. Dostupné z: http://www.gartner.com/it-glossary/identity-and-access-management-iam

(140) Digital Footprint. *The Tech Terms Computer Dictionary* [online]. Sharpened Productions, c2017 [cit. 2017-04-08]. Dostupné z: https://techterms.com/definition/digital_footprint

(141) ČESKÁ REPUBLIKA. Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). In: *Sbírka zákonů České republiky*. 2000. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-121

(142) Code of Ethics. *ASIS International: Advancing Security Worldwide* [online]. Virginia: ASIS International, c2017 [cit. 2017-04-08]. Dostupné z: https://www.asisonline.org/About-ASIS/Pages/Code-of-Ethics.aspx

(143) What is ethical hacking and ethical hacker? *Computer Hope* [online]. Computer Hope [cit. 2017-04-13]. Dostupné z: http://www.computerhope.com/jargon/e/ethihack.htm

(144) *NET4GAS, s.r.o.* [online]. NET4GAS, c2016 [cit. 2017-04-17]. Dostupné z: http://www.net4gas.cz/cz/kontakty/

(145) *Československá obchodní banka a.s.* [online]. ČSOB, c2017 [cit. 2017-04-17]. Dostupné z: https://www.csob.cz/portal/

(146) *Komerční banka, a.s.* [online]. Komerční banka, c2017 [cit. 2017-04-17]. Dostupné z: https://www.kb.cz/

(147) *O2 Czech Republic a.s.* [online]. [cit.2017-04-17]. Dostupné z: https://www.o2.cz/osobni/

(148) *Delloitte Advisory s.r.o.* [online]. Delloitte, c2017 [cit. 2017-04-17]. Dostupné z: https://www2.deloitte.com/cz/cs.html

(149) *Waldviertler Sparkasse Bank AG* [online]. WALDVIERTLER SPARKASSE BANK, c2016 [cit. 2017-04-17]. Dostupné z: https://www.wspk.cz/

(150) *Siemens, s.r.o.* [online]. Siemens, c1996-2017 [cit. 2017-04-17]. Dostupné z: https://www.siemens.com/cz/cz/home.html

(151) *Equa bank a. s.* [online]. Equa bank, c2011-2017 [cit. 2017-04-17]. Dostupné z: https://www.equabank.cz/

(152) *Fakulta informačních technologií ČVUT* [online]. [cit. 2017-04-17]. Dostupné z: https://www.fit.cvut.cz/

(153*) ČVUT – Fakulta elektrotechnická* [online]. [cit. 2017-04-17]. Dostupné z: https://www.fel.cvut.cz/cz/

(154) *Fakulta informatiky Masarykovy univerzity* [online]. [cit. 2017-04-18]. Dostupné z: https://www.fi.muni.cz/

(155) *Univerzita Tomáše Bati ve Zlíně: Fakulta aplikované informatiky* [online]. [cit. 2017-04-18]. Dostupné z: http://www.utb.cz/fai

(156) *Vysoká škola báňská – Technická univerzita Ostrava: Fakulta elektrotechniky a informatiky* [online]. [cit. 2017-04-18]. Dostupné z: https://www.fei.vsb.cz/cs/index.html

(157) *VUT v Brně: Fakulta elektrotechniky a komunikačních technologií* [online]. VUT FEKT Brno, c2007 [cit. 2017-04-18]. Dostupné z: http://www.feec.vutbr.cz/fakulta/home.php.cz

(158) *VUT v Brně: Fakulta informačních technologií* [online]. Fakulta informačních technologií VUT v Brně [cit. 2017-04-18]. Dostupné z: http://www.fit.vutbr.cz/.cs

Seznam obrázků

Seznam tabulek

Seznam zkratek

Název zkratky	Popis
ACM	Association for Computing Machinery
AFOI	Asociace firem pro ochranu dat a informací
AIS SIGSEC	Association for Information Systems Special Interest Group on Security
ANZSCO	Australian and New Zealand Standard Classification of Occupations
BOZP	Bezpečnost a ochrana zdraví při práci
CC	Common Criteria (Společná kritéria pro hodnocení bezpečnosti informačních technologií)
CC2005	Computing Curricula 2005
CEO	Chief Executive Officer (Výkonný ředitel/ka)
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer (Manažer/ka bezpečnosti informací)
CMM	Capability Maturity Model
CERT	Computer Emergency Response Team
CSEC2017	Cybersecurity Curricula 2017
CSIRT	Computer Security Incident Response Team
CSO	Chief Security Officer (Manažer/ka bezpečnosti)
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria (Kanadská kritéria hodnocení bezpečnosti počítačových produktů)
CZ-ISCO	Česká verze převzatého mezinárodního standardu ISCO-08
ČR	Česká republika

ČSN	Československá státní norma
ČSÚ	Český statistický úřad
ČTÚ	Český telekomunikační úřad
ČVUT	České vysoké učení technické v Praze
DDoS	Distributed denial of service (Distribuované odmítnutí služby)
DHS	Department of Homeland Security (Ministerstvo vnitřní bezpečnosti)
DLP	Data Loss Prevention
DMS	Data Security Management
DNS	Domain Name System
ECTS	European Credit Transfer and Accumulation System (Kreditní systém školství)
ERP	Enterprise Resource Planning
EU	Evropská unie
EUR	Euro
EZS	Elektronická zabezpečovací signalizace
FAI	Fakulta aplikované informatiky
FBI	Federal Bureau of Investigation (Federální úřad pro vyšetřování)
FC	Federal Criteria (Federální kritéria pro bezpečnost informačních technologií)
FEI	Fakulta elektrotechniky a informatiky
FEKT	Fakulta elektrotechniky a komunikačních technologií
FEL	Fakulta elektrotechnická
FI	Fakulta informatiky
FIT	Fakulta informačních technologií

GDPR	General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů)
HR	Human Resources (Lidské zdroje)
HW	Hardware
ICT	Information and Communication Technologies (Informační a komunikační technologie)
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IEEE - CS	IEEE Computer Society
IFIP WG 11.8	International Federation for Information Processing Technical Committee on Information Security Education
IoT	Internet of Things (Internet věcí)
IS	Information System (Informační systém)
IS KII	Informační systém kritické informační infrastruktury
IS o ISVS	Informační systém o informačních systémech veřejné správy
ISACA	Information Systems Audit and Control Asociation
ISCED 97	Mezinárodní klasifikace vzdělání
ISCO-08	International Standard Classification of Occupations (Mezinárodní standard pro klasifikaci zaměstnání)
ISG	Information Security Governance (Správa a řízení bezpečnosti informací)
ISMS	Information Security Management System (Systém řízení bezpečnosti informací)
ISO	International Organization for Standardization

ISPV	Informační systém o průměrných výdělcích
IT	Information Technology (Informační technologie)
ITG	IT Governance (Správa a řízení IT)
ITSEC	Information Technology Security Evaluation Criteria (Kritéria hodnocení bezpečnosti informačních systémů)
IZS	Integrovaný záchranný systém
KB	Kybernetická bezpečnost
KS	Komunikační systém
KS KII	Komunikační systém kritické informační infrastruktury
MŠMT	Ministerstvo školství, mládeže a tělovýchovy ČR
MU	Masarykova Univerzita
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NICE	National Initiative for Cybersecurity Education
NIS	The Directive on security of network and information systems (Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii)
NIST	National Institute of Standards and Technology
NKI	Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
NSA	National Security Agency
OECD	Organisation for Economic Cooperation and Development (Organizace pro ekonomickou spolupráci a rozvoj)
OS	Operation System (Operační systém)

PLC	Programovatelný logický automat
SCADA	Supervisory Control Ans Data Acquisition
SIEM	Security Information and Event Management
SIMS	Sdružené informace matrik studentů
SQL	Structured English Query Language
SW	Software
TCSEC	Trusted Computer Security Evaluation Kriteria (Kritéria hodnocení důvěryhodných výpočetních systémů)
UML	Unified Modeling Language (Unifikovaný modelovací jazyk)
ÚOOÚ	Úřad pro ochranu osobních údajů
USA	United States of America (Spojené státy americké)
USD	Americký dolar
UTB	Univerzita Tomáše Bati ve Zlíně
VIS	Významný informační systém
VKB	Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
VPN	Virtual Private Networks (Virtuální privátní sítě)
VŠ	Vysoká škola
VŠB-TUO	Vysoká škola báňská – Technická univerzita Ostrava
VUT	Vysoké učení technické v Brně
VVIS	Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
ZEK	Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunika-

	cích)
ZKB	Zákon č. 181/2014 S., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
ZKŘ	Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)

Příloha A – Základní znalostní jednotky a témata

Pro identifikaci klíčových znalostí a dovedností odborníků v oblasti bezpečnosti ICT je možné částečně vycházet z definice kurikula CSEC2017 a ním definovaných témat v rámci znalostních jednotek. Klíčové znalosti a dovednosti jsou zachyceny ve struktuře myšlenkového modelu uvedeného v kap. 9.2.1. – „Charakteristika studijního programu dle CSEC2017“. Základní znalostní jednotky a příslušná témata, které definuje kurikulum CSEC2017 jsou popsány níže (90).

A.1: Znalostní doména – Bezpečnost dat

Znalostní jednotka	**Téma**
Základy bezpečnosti informací	Hrozba
	Zranitelnost a hodnocení rizik
	Základy kryptografie
	Základy bezpečnosti dat
	Modely řízení přístupů k datům
	Bezpečnostní mechanismy
Kryptografie	Symetrické šifrování
	Asymetrické šifrování
	Hashovací funkce
	Elektronický podpis
	Key Management
	Typy kybernetických útoků
	Kryptografické protokoly
	Vývoj šifrovacích algoritmů
	Bezpečnostní funkce
	Teorie čísel

	Pravděpodobnost a statistika
	Kryptoanalýza
	VPN

Tab. 21: Základní znalostní jednotky a témata domény "Bezpečnost dat"

Vysvětlivky:

Hrozba - *„Hrozba je akce nebo událost, která může ohrozit bezpečnost. Hrozba je zneužitím zranitelnosti“*. (5 s. 61)

Zranitelnost - *„Zranitelností rozumíme jakékoliv slabé místo aktiva včetně bezpečnostních procedur, kontrolních míst.“* (5, s. 62)

Hodnocení rizik – „*Celkový proces analýzy a vyhodnocení rizik.“* (5, s. 99) V rámci procesu probíhá analýza rizik a vyhodnocení rizika.

Analýza rizik – *„Proces pochopení povahy rizika a stanovení úrovně rizika.“* (8, s. 13)

Vyhodnocení rizik – *„Proces porovnání odhadnutého rizika vůči daným kritériím pro určení jeho významu“*. (5, s. 99)

Kryptografie – Obor, který zkoumá různé metody šifrování zpráv (99).

Bezpečnost dat – *„Počítačová bezpečnost aplikovaná na data. Zahrnuje například řízení přístupů, definování politik a procesů a zajištění integrity dat.“* (8 s. 18)

Modely řízení přístupů – Modely, které se používají pro centralizovanou správu identit. Existuje několik typů, z nichž nejznámější jsou: řízení přístupu dle rolí (RBAC), volitelné řízení přístupu (DAC), povinné řízení přístupu (MAC) (100).

Bezpečnostní mechanismus - „*Je opatřením nebo algoritmem, který je implementován v technických nebo programových řešeních.*“ (5 s. 59) Například autorizace, autentizace, audit přístupů, aj.

Autorizace - *„Proces udělení práv subjektu pro vykonávání určených aktivit v informačním systému.“* (8 s. 17)

Autentizace - *„Proces ověření identity subjektu.“* (8 s. 16)

Symetrické šifrování – Je proces šifrování, kdy se pro šifrování i dešifrování dat používá tentýž klíč (101).

Asymetrické šifrování – Proces šifrování, kdy jsou data zašifrována pomocí veřejného klíče a mohou být dešifrována pouze držitelem privátního klíče (102).

Hashovací funkce – Jednosměrná funkce k vytvoření tzv. hashe, neboli otisku, ze vstupního řetězce dat. Z výstupu funkce nelze získat původní vstup. Funkce se používá zejména pro ověření integrity dat (103).

Elektronický podpis – *„Elektronickým podpisem se rozumí údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které umožňují ověření totožnosti podepsané osoby*

ve vztahu k datové zprávě.“ (104) Použití elektronické podpisu je definováno v zákoně č. 227/2000 Sb., o elektronickém podpisu a o změně některých zákonů (zákon o elektronickém podpisu) (105).

Key management – Správa šifrovacích klíčů. Je vhodným nástrojem pro údržbu privátních šifrovacích klíčů. Zahrnuje generování, ukládání, výměnu a náhradu šifrovacích klíčů (106).

Kybernetický útok – *„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace.“* (8 s. 59)

Kryptografické protokoly – Zajišťují bezpečný přenos dat na základě předem stanovených pravidel (např. Kerberos) (107).

Šifrovací algoritmus – Algoritmus je *„konečná uspořádaná množina úplně definovaných pravidel pro vyřešení nějakého problému“*. (8 s. 12) *„Šifrování je kombinací transpozice, substituce a XORování s klíčem.“* (108) Aplikací šifrovacího algoritmu na otevřený text získáme šifrovaný text, který lze rozklíčovat pouze za předpokladu znalosti šifrovacího algoritmu (např. AES, DES, RSA, aj.).

Bezpečnostní funkce - *„Funkce daného systému nebo produktu, která přispívá k jeho bezpečnosti.“* Například ochrana dat, integrita dat, autentizace, aj. (5 s. 59)

Teorie čísel – Disciplína matematiky, jež se zabývá vlastnostmi čísel (například dělitelnost čísel) (109).

Pravděpodobnost a statistika – *„Pravděpodobnost zkoumaného jevu vyjadřuje míru naděje, že tento jev nastane.“* (110) Statistika se zabývá studiem zákonitosti výskytu těchto jevů (111).

Kryptoanalýza – Věda zabývající se dešifrováním zašifrovaných zpráv (112)

VPN (Virtual Private Networks) – Virtuální privátní sítě. Zajišťují důvěryhodné připojení a umožňují zabezpečenou komunikaci mezi koncovými body (113).

A.2: Znalostní doména – Bezpečnost software

Znalostní jednotka	**Téma**
Základní principy návrhu software	Objektové modelování
	Modulární programování
	Vícevrstvá architektura software
	Dekompozice
	Otevřený návrh
	Použitelnost
	End-to-End bezpečnost

	Obrana do hloubky (Defense in depth)
Praxe	Specifikace bezpečnostních požadavků
	Principy bezpečného programování
	Validace vstupů
	Přetečení zásobníku
	Statická a dynamická analýza
	Ochrana před ztrátou dat
	Životní cyklus vývoje software
	Testování software
	Penetrační testování
	Fuzz testování
	SQL injection
	Ošetření výjimek a chyb
Dokumentace	Tvorba dokumentace

Tab. 22: Základní znalostní jednotky a témata domény "Bezpečnost software"

Vysvětlivky:

Objektové modelování – *„Objektově orientované jazyky jsou postaveny na tzv. objektech, které odpovídají jednotlivým prvkům modelované reality. Objekty si pamatují svůj stav a navenek poskytují operace (v závislosti na konkrétním jazyku se jedná o tzv. zprávy či metody).“* (114) Je založeno na paradigmatech – objekty, abstrakce, skládání, delegování, dědičnost a polymorfismus.

Modulární programování – Je založeno na návrhu „shora-dolů“, kdy se funkcionality programu dekomponují do nezávislých modulů, což zvyšuje přehlednost kódu a případnou znovupoužitelnost, umožňuje skrýt určité části kódu a zjednodušuje práci s kódem (115).

Vícevrstvá architektura software – Znamená vrstvení aplikace na vícero spolupracujících vrstev. V softwarovém inženýrství se používá zejména třívrstvá architektura s rozdělením na prezentační, aplikační a datovou vrstvu, která umožňuje snadnější správu aplikace a snadnější rozšiřitelnost (116).

Dekompozice – Princip zjednodušování návrhu software, kdy jsou komplexní problémy rozloženy na jednodušší (triviální) podproblémy (117). Ty se vyřeší obdobným způsobem pomocí rekurze, tj. opakovaným použitím obdobného algoritmu.

Otevřený návrh – Používá se pro tvorbu tzv. open source software. Jedná se o veřejně přístupný software, který může být modifikován či rozšiřován (118).

Použitelnost – Použitelnost software se při návrhu definuje pomocí případů užití. K modelování případů užití může být použit modelovací jazyk UML (Unified Modeling Language) (119).

End-to-End bezpečnost – Bezpečnost na koncových bodech (komunikace klient-server, popřípadě klient-klient), tj. zajištění absolutně bezpečné komunikace mezi těmito body (120).

Obrana do hloubky (Defense in depth) - Koncept ochrany počítačové sítě s řadou obranných mechanismů. V případě, že jeden z mechanismů selže, je nahrazen jiným (121).

Specifikace bezpečnostních požadavků – Specifikace bezpečnostních požadavků by se měla řídit zvoleným standardem – např. IEEE 830-1984 (122). Požadavky lze dělit na funkční, které musí daný systém splňovat a nefunkční – tj. možná omezení (122).

Principy bezpečného programování – Jsou zaměřeny na správný postup vývoje softwarového produktu: návrh bezpečného produktu, implementaci vlastností, testování vlastností a bezpečnosti, opravu chyb a teprve potom zveřejnění SW produktu (123). Přičemž platí principy SD3: bezpečný návrh (Secure Design), výchozí instalace je nejvíce bezpečná (Secure by Default) a zabudování nastavení bezpečnosti přímo v softwarovém produktu (Secure in Deployment) (123).

Validace vstupů – Znamená zabezpečení validity vstupů od uživatele (datový typ, délka znaků, aj.) (124).

Přetečení zásobníku (Buffer Overflow) – Stav, kdy program zapíše data za konec alokované části paměti. V důsledku toho dochází k nekorektnímu chování programu – např. spuštění virů, atd. Jedná se o velmi častou zranitelnost programů (125).

Statická a dynamická analýza kódu – Analýza softwaru, která se spouští na nespuštěné (statická analýza) či spuštěné (dynamická analýza) počítačové programy. Používá se zejména pro odladění chyb a zranitelností, zvýšení spolehlivosti a výkonnosti SW a samotné zkvalitnění kódu (126).

Ochrana před ztrátou dat (Data Loss Prevention - DLP) – Jsou systémy schopné identifikovat, monitorovat a chránit data před jejich ztrátou (únikem). Význam těchto systémů narůstá s příchodem GDPR (127).

Životní cyklus vývoje software – Začíná zachycením požadavků na software, přes analýzu, návrh, implementaci, testování, udržování software a provoz a v neposlední řadě stažení software z užívání.

Testování software – Slouží k ověřování kvality software, odladění nedostatků a odstranění chyb. Rozlišují se na white box testy, kdy má tester zdrojový kód k dispozici a zná tak vnitřní funkce softwaru a black box testy, kdy tester nemá přístup ke kódu a vnitřní funkce softwaru jsou před ním skryty (128).

Penetrační testování – Testování se zaměřením na odhalení zranitelností testovaného softwaru či systému (129).

Fuzz testování – Fuzz testování je prováděno tak, že se na vstup posílají špatná, neočekávaná či náhodná data (130). Následně se ověřuje stav počítačového programu, případné spadnutí či jeho „zamrznutí“.

SQL injection – *„Je druh napadení webu, kdy může útočník přes nezabezpečené formuláře posílat příkazy databázi, která je poté vykoná“*. (131) Útočník se může například přihlásit jako jakýkoliv uživatel či přímo může smazat údaje v databázi (131).

Ošetření výjimek a chyb – Ošetření chybového stavu programu pomocí mechanismu výjimek (132).

Tvorba dokumentace – Popis detailního návrhu SW (obsahuje zejména požadavky na daný software, případy použití, sekvenci úkolů, digram interakce, návrh architektury atd.) a popis skutečného provedení.

A.3: Znalostní doména – Systémová bezpečnost

Znalostní jednotka	**Téma**
Dostupnost	Dostupnost systému
	Útoky zaměřené na dostupnost
Autentizace	Prostředky autentizace
	Autentizace na základě biometrických údajů
	Vícefaktorová autentizace
Řízení přístupů	Bezpečnostní politika
	Modely řízení přístupů
	Systémový audit
Bezpečný návrh systémů	Bezpečná architektura
Ochrana počítačových sítí	Firewall
	Systém prevence průniku (Intrusion Prevention System)
	Systém detekce průniku (Intrusion Detection System)
	Honeypot
Bezpečnost fyzických zařízení	Internet věcí
	Hrozby a zranitelnosti
Forenzní analýza	Forenzní analýza OS, systémových souborů, aplikací, sítí, mobilních zařízení

Tab. 23: Základní znalostní jednotky a témata domény "Systémová bezpečnost"

Vysvětlivky:

Dostupnost – *„Vlastnost přístupnosti a použitelnosti na žádost autorizované entity.“* (8 s. 35)

Útoky zaměřené na dostupnost – Například DDoS útoky. *„Distribuované odmítnutí služby (Distributed denial of service) je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele, a to útokem mnoha koordinovaných útočníků.“* (8 s. 33)

Prostředky autentizace – hesla, klíče, karty, certifikáty.

Autentizace na základě biometrických údajů – Proces autentizace s využitím biometrických údajů o uživateli – např. otisky prstů, rozpoznání rysů obličeje, duhovky, aj. (133).

Vícefaktorová autentizace – Proces autentizace založený na kombinaci zabezpečení ve třech oblastech (faktorech): znalost (něco, co uživatel zná), vlastnictví (něco, co uživatel vlastní) a biometrie (biometrické znaky uživatele) (134).

Bezpečnostní politika – *„Na úrovni organizace základní dokument, který vymezuje strukturu bezpečnostního rizika, odpovědnost za ochranu informací v organizaci, úroveň ochrany informací. Na úrovni systému soubor pravidel a praktik, které specifikují nebo regulují, jak systém (nebo organizace) poskytuje bezpečnostní služby, aby chránil/a citlivé nebo kritické zdroje systému.“* (8 s. 21) Pro řízení přístupů obsahuje pravidla přidělování přístupů k informačním a komunikačním systémům v organizaci. (5 s. 132).

Systémový audit – funkcionalita systémů, která umožňuje zaznamenávat události a stavy systému během provozu. Používá se pro zaznamenávání činností uživatelů v systému (135).

Bezpečná architektura – Zajišťuje, že informace obsažené v informačních systémech jsou chráněny z pohledu důvěrnosti, dostupnosti a integrity (5).

Firewall – HW či SW, který může být pomocí sady pravidel nakonfigurován tak, aby zabránil neoprávněnému přístupu k počítači či službám v síti (8 s. 38).

Systém prevence průniku (Intrusion Prevention System) - Systém detekce průniku do systému, jenž umožňuje aktivní reakci (je aktivní) (8 s. 98).

Systém detekce průniku (Intrusion Detection Systém - IDS) - Systém, který se používá pro kontrolu, zda došlo k pokusu o průnik, či k němu přímo došlo (136). Oproti IPS je pasivní a nezajišťuje aktivní reakci.

Honeypot – Návnada lákající útočníka (malware). Po zachycení podezřelého SW dochází k automatické analýze škodlivého kódu. (8 s. 42)

Internet věcí (Internet of Things) – *„Množina jednoznačně rozpoznatelných zařízení, která pracují v rámci vlastní sítě či internetové infrastruktury.“* (137)

Forenzní analýza – *„Forenzní analýza dat je investigativní zkoumání a vyšetřování dat uložených v nejrůznějších podobách, kterou je možné využít při zpracování digitálních důkazů – zajištění, výběr, identifikace, analýza, interpretace, dokumentace.“* (138) Může zkoumat OS, servery, datová uložiště, mobilní telefony, atd. Využívá se k vyšetřování páchání trestné činnosti s využitím právě těchto technických prostředků (kybernality).

A.4: Znalostní doména – Bezpečnost lidských zdrojů

Znalostní jednotka	Téma
Identity management	Řízení aktiv
	Identifikace a autentizace osob
	Útoky na přístupové kontroly
	Zajišťování životního cyklu identit a přístupů
Sociální inženýrství	Útoky na soukromí a anonymitu
	Politika soukromí
Sociální sítě	Základní koncepty

Tab. 24: Základní znalostní jednotky a témata domény "Bezpečnost lidských zdrojů"

Vysvětlivky:

Identity management – Správa identit je disciplína v oblasti bezpečnosti ICT, která zajišťuje práva identit v systémech k určitým zdrojům po určitý čas a pro určitý účel (139).

Řízení aktiv – zajištění přiměřené míry ochrany hmotných i nehmotných aktiv, udržování evidence a stanovení odpovědnosti za udržování přiměřené míry ochrany (garantem aktiv) (5 s. 131).

Identifikace uživatele – *„Znakový řetězec nebo vzorec používaný systémem zpracování dat k identifikaci uživatele.“* (8 s. 44)

Útoky na přístupové kontroly – Například „brute force“ útok (útok hrubou silou). *„Metoda k zjišťování hesel, kdy útočící program zkouší jako možné heslo všechny existující kombinace znaků, dokud nezjistí skutečné heslo.“* (8 s. 105)

Zajišťování životního cyklu identit a přístupů – Od přidělování přístupů na základě schvalovacího procesu k jejich odebrání, například z důvodu odchodu zaměstnance ze zaměstnání (5). Řízení životního cyklu identit a přístupů by mělo být pravidelně přezkoumáváno v rámci auditní činnosti.

Sociální inženýrství – *„Způsob manipulace lidí za účelem provedení určité akce nebo získání určité informace.“* (8 s. 93) Zejména využívá technik emocionálního nátlaku na oběť útoku – např. „jestliže nepotvrdíte správné heslo, bude tento uživatelský účet zablokován“.

Útoky na soukromí a anonymitu – Zejména metoda phishing *„usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtů apod. za účelem jejich následného zneužití“*. (8 s. 70)

Politika soukromí – Stanovení celkové politiky ochrany osobních údajů, jež organizace zpracovává. Základní požadavky na ochranu osobních údajů uvádí zákon č. 101/2000 Sb., o ochraně osobních údajů

a změně souvisejících zákonů (zákon o ochraně osobních údajů) a dále také nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), tzv. GDPR (2,33).

Sociální síť – *„Propojená skupina lidí, kteří se navzájem ovlivňují.“* (8 s. 93) Příkladem jsou sociální sítě Facebook, LinkedIn, aj.

A.5: Základní doména – Organizační bezpečnost

Znalostní jednotka	**Téma**
Bezpečnostní politika a Information Security Governance	Soukromí
	Organizace bezpečnosti
	Právo, etika a „compliance“
	Organizační kontext
	Řízení kontinuity činností (Business Continuity Management)
	Obnova po havárii (Disaster Recovery)
	Reporting
Budování bezpečnostního povědomí – školení a trénink	
Řízení rizik	Hodnocení a analýza rizik
	Metodiky pro analýzu rizik
	Mitigace rizik

Tab. 25: Základní znalostní jednotky a témata domény "Organizační bezpečnost"

Vysvětlivky:

Infomation Security Governance – Správa a řízení bezpečnosti informací, je součástí Enterprise Governance (správy a řízení na úrovni organizace) a musí mít vazbu na IT Governance (správa a řízení na úrovni IT). (5 s. 40-44).

Soukromí – Pravidla ochrany před neoprávněným zasahováním do soukromí stanovuje zákon č. 101/2000 Sb., o ochraně osobních údajů a změně souvisejících zákonů (zákon o ochraně osobních údajů) (33).

Organizace bezpečnosti – Stanovuje bezpečnostní opatření pro interní organizaci řízení bezpečnosti informací a pravidla pro zajištění bezpečnosti u externích subjektů (např. dodavatelů). (5 s. 134-135).

Právo, etika a „compliance" – Organizační bezpečnost vyžaduje znalost legislativních požadavků, které jsou na danou organizaci kladeny v návaznosti na oblast, ve které organizace působí a dále vyžaduje respektování základních etických pravidel podnikání (5). K tomu je nezbytné zajistit kontinuální proces kontroly shody s právními a jinými požadavky, které jsou na danou organizaci kladeny.

Organizační kontext – Pro řízení bezpečnosti ICT je nezbytné vnímat celkový kontext organizace – předmět podnikání, zákazníky, konkurenci, zaměstnance, atd. (5)

Řízení kontinuity činností organizace (Business Continuity Management) – *„Procesy a/nebo postupy k zajištění nepřetržitého chodu organizace."* (8 s. 53)

Obnova po havárii (Disaster Recovery) - Obnova činností organizace po havárii, kdy dochází k přerušení kontinuity činností organizace (8 s. 72). Pro takové situace se připravují plány obnovy, tj. záložní postupy při havárii a postup obnovy normálního chodu organizace.

Reporting - Dle ZKB a VKB mají správci VIS a správci IS KII a KS KII povinnost reportovat bezpečnostní incidenty. K tomu je nezbytné znát strukturu a náležitosti takového hlášení a také proces, který říká, kdy a jak takové hlášení podávat (3).

Budování bezpečnostního povědomí – Dle ZKB a sady norem ISO/IEC 27000 mají odpovědné subjekty prohlubovat bezpečnostní povědomí svých zaměstnanců formou pravidelných tréninků a školení (4). Jedná se o jedno z bezpečnostních opatření spadající do bezpečnosti z hlediska lidských zdrojů (5 s. 131).

Řízení rizik – *„Koordinované činnosti sloužící k řízení a kontrole organizace s ohledem na rizika."* (5 s. 99). Skládá se z fáze hodnocení rizik, fáze zvládání rizik, kdy jsou navržena příslušná bezpečnostní opatření a fáze akceptace rizika.

Metodiky pro analýzu rizik – Analýza rizik by měla být prováděna vždy v souladu se zvolenou metodikou (např. uvedená metodika ve VKB) (4).

Mitigace rizik – Pro mitigaci rizik se používá plán zvládání rizik, který popsuje cíle vybraných opatření pro eliminaci bezpečnostního rizika (5 s. 107).

A.6: Znalostní doména – Společenská bezpečnost

Znalostní jednotka	Téma
Kybernalita	Trestné chování v kyberprostoru
	Kyberterorismus
	Digitální stopa
	Motivace útočníků
	Dark web/Deep web
Právo	Legislativa v oblasti kybernetické bezpečnosti a v oblasti ochrany dat
	Související legislativa ČR a EU
	Duševní vlastnictví
Etika	Profesní etika a etické kodexy
Politologie	Kybernetická válka a národní strategie kybernetické bezpečnosti
	Mezinárodní politika kybernetické bezpečnosti a její vývoj
Profesní odpovědnost	
Sociální odpovědnost	Etický hacking

Tab. 26: Základní znalostní jednotky a témata domény "Společenská bezpečnost"

Vysvětlivky:

Kybernalita - *„Kybernalitou rozumíme takovou činnost, kterou je porušován zákon nebo je v rozporu s morálními pravidly společnosti.“* (29 s. 19)

Trestné chování v kyberprostoru – Téma by mělo zahrnovat přehled o nelegálních aktivitách v kyberprostoru, o metodách pachatelů kybernality, jak definovat kybernetickou kriminalitu, vyšetřování kybernality (forenzní analýza), přehled legislativy ČR a EU a zásady trestního práva (29 s. 6-7).

Kyberterorismus - *„Trestná činnost páchaná za primárního využití či cílení prostředků IT s cílem vyvolat strach či neadekvátní reakci.“* (29 s. 59)

Digitální stopa – Je definována jako evidence všech informací o činnosti uživatele v rámci digitálního prostředí (aplikace, Internet, atd.) (140).

Motivace útočníků – K pochopení je důležitý popis efektů nelegálního chování v kyberprostoru, tj. jaký efekt nelegální chování v kyberprostoru útočníkům přináší (29).

Dark web (či deep web) - Je termín pro všechny webové stránky, které nejsou dostupné z klasických vyhledávačů, ale pouze za pomoci speciálního software (37). Tyto stránky mívají ilegální obsah a uživatel si zde může zakoupit ilegální zboží či služby, ale také škodlivý kód za účelem páchání kybernality.

Legislativa v oblasti kybernetické bezpečnosti a v oblasti ochrany dat – tj. zákon č. 101/2000 Sb., o ochraně osobních údajů a změně souvisejících zákonů (zákon o ochraně osobních údajů), zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti), aj. (3,4,33)

Související legislativa ČR a EU – tj. směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS), nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27.dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů), zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů, aj. (2,22,46).

Duševní vlastnictví – Je definováno zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) (141).

Profesní etika a etické kodexy – Vnímání profesní etiky a znalost některých etických kodexů – např. globální komunity odborníků na bezpečnost ICT s názvem ASIS International (142).

Kybernetická válka a národní strategie kybernetické bezpečnosti – viz. kap. 6.2. – „Vývoj národní kybernetické bezpečnosti a legislativy“.

Mezinárodní politika kybernetické bezpečnosti - viz. kap. 6.2. – „Vývoj národní kybernetické bezpečnosti a legislativy“.

Etický hacking – Použití technik hackingu s cílem identifikovat potencionální hrozby a zlepšit ochranu zabezpečení. Bývá požadován po dodavatelích bezpečnostních testů v rámci zachování důvěrných informací. Je založen zejména na principech – mít povolení k testování, respektovat soukromí organizace, řádně uzavřít testování a zamezit tak nepovolenému přístupu a informovat odpovědné osoby o nalezených zranitelnostech (143).

Příloha B – Požadavky pracovního trhu

B.1: Specialista Kybernetické bezpečnosti – plynárenské systémy (144)

Specifikace:

- práce s interní dokumentací a ZKB;
- aktualizace bezpečnostní dokumentace plynárenských systému – provozní technologie SCADA, politiky, směrnice a navazující interní předpisy;
- provádění analýz a sledování trendů v oblasti bezpečnosti SCADA;
- zpracování a pravidelná aktualizace katalogu rizik SCADA;
- aktivní účast na „Bezpečnostním výboru společnosti“;
- tvorba reportů a zpráv o stavu bezpečnosti SCADA;
- zajištění souladu „Bezpečnostní politiky“ s dodavateli systémů SCADA;
- pravidelná aktualizace „Plánu obnovy“ po havárii;
- spolupráce s ostatními útvary společnosti v oblasti komplexní bezpečnosti;
- identifikace, evidence a spolupráce při řešení bezpečnostních incidentů;
- zajištění souladu mezi ZKB a projektů SCADA;
- zajišťování nezbytných aktivit na systémech SCADA dle ZKB a příslušné VKB.

Požadavky:

- VŠ vzdělání technického směru;
- komunikativní znalost anglického jazyka;
- všeobecný rozhled v oblasti firemní bezpečnosti počítačově řízených systémů;
- znalost příslušných norem a ZKB a jejich implementace v praxi;
- Windows OS;
- znalost systému SCADA;
- průmyslové komunikační protokoly.

B.2: Specialista/-ka pro informační bezpečnost Junior (145)

Specifikace:

- aktivní spolupráce s odbornými a obchodními útvary na tvorbě, zavádění a hodnocení nástrojů a procesů v oblasti informační bezpečnosti;
- zajištění reakce na případy podezření úniku citlivých dat;
- příprava podkladů pro stanoviska a doporučení týkající se řízení informační bezpečnosti pro vedení banky;
- kontrola a vyhodnocování správnosti procesů a postupů používaných v informační bezpečnosti;
- sledování vývoje a trendů v informační bezpečnosti.

Požadavky:

- ochotu se vzdělávat, primárně v oblasti informační bezpečnosti
- dobrá znalost anglického jazyka slovem i písmem
- výborné organizační, komunikační a prezentační schopnosti
- velmi dobré analytické a koncepční schopnosti

B.3: Administrátor IT bezpečnosti (146)

Specifikace:

- sledování úrovně bezpečnosti na OS a na databázové vrstvě v dohledovém nástroji;
- monitoring bezpečnostní úrovně informační bezpečnosti a úroveň zabezpečení na síťové vrstvě prostřednictvím dohledových nástrojů;
- identifikace a správa bezpečnostních incidentů a hrozeb včetně návrhu protiopatření;
- zajištění provedení bezpečnostních testů, včetně zprávy pro zadavatele;
- pravidelný reporting stavu informačního systému KB z hlediska bezpečnosti (provozní report a report pro management);
- řízení bezpečnostních výjimek v informačním systému KB;
- řízení a rozvoj kontrolních systémů bezpečnosti v IS KB;
- udržování znalostí o současných technologiích v oblasti bezpečnosti;
- implementace bezpečnostních standardů v prostředí KB a kontrola jejich dodržování.

Požadavky:

- technické znalosti v oblasti IT bezpečnosti a souvisejícího monitoringu;
- znalost nástrojů IT bezpečnosti – SIEM, firewall, proxy, kontrola zranitelnosti, hackerských nástrojů, zabezpečení koncových bodů;
- znalost operačních systémů včetně technologií, jako jsou, VPN, Domain Name System (DNS), atd.;
- zkušenosti s informační bezpečností v oblasti finančních služeb.

B.4: Specialista pro kybernetickou bezpečnost (147)

Specifikace:

- výkon svěřených aktivit v oblastech informační bezpečnosti podle ISO27000 a ZKB;
- provádění analýz rizik zpracování dat a provozu informačních systémů;
- shromažďování údajů, zajišťování a vedení povinných evidencí a agend;
- spolupráce při formulacích, údržbě a reálném uplatňování pracovních postupů a standardů týkajících se ochrany informací v rámci celého životního cyklu IT řešení;
- účast na ověřování shody dosahované úrovně informační bezpečnosti s požadovanou úrovní;
- související konzultační, podpůrná a edukační činnost.

Požadavky:

- základní orientace v oblasti informační a technické bezpečnosti;
- základní orientace v metodách řízení dodávek a provozu IT;
- znalost problematiky zpracování a ochrany dat;
- osobní integrita – předpoklady pro udělení prověrky NBÚ (Národní bezpečnostní úřad, stupeň „vyhrazeno“, případně „důvěrné“).

B.5: Specialista/ka řízení bezpečnosti informací (146)

Specifikace:

- účast na procesech hodnocení a řízení rizik informační bezpečnosti;
- správa registru informační aktiv;
- metodická podpora vlastníků informačních aktiv, poskytovaní konzultací a školení v oblasti řízení rizik informační bezpečnosti;
- reportování vyhodnocení rizik informační bezpečnosti;
- příprava plánu řízení rizik informační bezpečnosti;
- zavádění vybraných bezpečnostních opatření v bance;

Požadavky:

- VŠ vzdělání se zaměřením na IT, finanční služby nebo řízení.

B6: Konzultant v oddělení kybernetické bezpečnosti (148)

Specifikace:

- práce na analýzách IT bezpečnosti, zkoumat zranitelná místa a hrozby;
- návrh a zavádění procesních i technických bezpečnostních opatření;
- tvorba studií na témata kybernetické bezpečnosti;
- práce na projektech pro největší české i nadnárodní společnosti;
- podpora oddělení auditu a ostatní kolegy svými expertními znalostmi.

Požadavky:

- být absolventem magisterského studia (případně student posledního ročníku) se zaměřením na IT (obory bezpečnosti výhodou);
- mít hluboký zájem o kybernetickou bezpečnost, nové trendy;
- být schopen pracovat samostatně a na několika projektech současně v rychle se měnícím prostředí;
- silné komunikační dovednosti;
- mít dobrou orientaci v IT;
- dobře komunikovat v AJ.

B.7: IT specialista – oblast bezpečnosti a ochrany dat (149)

Specifikace:

- identifikace/definice požadavků z oblasti bezpečnosti, ochrany dat;
- sledování legislativy/regulativy v uvedené oblasti (zákony, vyhlášky, nařízení, směrnice, normy, doporučení, standardy, atd.);
- provádění analýz rizik, tvorba dokumentací, směrnic, nařízení a reportů z uvedených oblastí;
- rozvíjení interního kontrolního systému, systému oprávnění, oblast business continuity;
- implementace opatření.

Požadavky:

- ISO normy z oblasti bezpečnosti;
- znalost cizího jazyka (němčina nebo angličtina);
- předpokladem je zájem o problematiku IT bezpečnosti;
- analytické myšlení.

B.8: Specialista pro síťovou bezpečnost (147)

Specifikace:

- provozní administrace IDS a dalších bezpečnostních prvků sítě;
- vyhodnocování bezpečnostních incidentů a návrh detekčních mechanismů;
- účast na projektových aktivitách – včetně návrhů, vývoje, konfiguračních změn, testování, údržby systémové dokumentace a přebírání výstupů z projektů do provozu;
- příprava, plánování a spolupráce při provádění bezpečnostních testů;
- související konzultační, podpůrná a edukační činnost.

Požadavky:

- systémová administrace a administrace síťových prvků;
- znalosti a orientace v prostředcích technické a síťové bezpečnosti;
- praktické zkušenosti s firewally a IDS;
- praktické zkušenosti s analýzou síťového provozu;
- znalost aplikačních protokolů.

B.9: IT Security Expert (150)

Specifikace:

- definování požadavků na IT bezpečnost s cílem minimalizace rizik;
- spolupráce na výběru dodavatelů a technologií z pohledu zajištění bezpečnosti;
- tvorba pravidel pro šifrování a analýzu rizik;

Požadavky:

- praktické zkušenosti v oblasti informační bezpečnosti a znalost souvisejících norem a nařízení;
- znalost firewallu a antivirové ochrany;
- zájem o novinky a trendy v IT bezpečnosti.

B.10: IT Security Specialist (146)

Specifikace:

- sledování úrovně bezpečnosti na OS a na databázové vrstvě v dohledovém nástroji;
- identifikace a správa bezpečnostních incidentů a hrozeb včetně návrhu protiopatření;
- zajištění bezpečnostních testů, včetně výsledné zprávy;
- pravidelný reporting stavu informačního systému KB z hlediska bezpečnosti;
- řízení bezpečnostních výjimek a rozvoje kontrolních systémů;
- udržování znalostí o současných technologiích v oblasti bezpečnosti;
- implementace nových bezpečnostních standardů a kontrola jejich dodržování.

Požadavky:

- znalost některého nástrojů IT bezpečnosti (např. SIEM, firewall, kontrola zranitelnosti, hackerských nástrojů, zabezpečení koncových bodů);
- znalost OS, databází a dalších technologií;

B.11: IT Security Specialist (151)

Specifikace:

- analýza a vyhodnocování auditních záznamů;
- řízení přístupu do systémů a aplikací;

- participace na rozvoji bezpečnostních standardů architektury, integrace systémů v souladu s IT strategií a s obecnými technologickými trendy v oblasti bezpečnosti;
- zpracování bezpečnostní politiky IS a příslušných předpisů za danou oblast a jejich pravidelná aktualizace;
- provádění kontrol přidělování a změn přístupových práv a rolí do systémů a aplikací;
- školení zaměstnanců na počítačovou bezpečnost;
- spolupráce při vypracování a aktualizaci analýzy rizik informačních systémů;
- vypracování, aktualizace a testování plánu obnovy.

Požadavky:

- znalost OS;
- znalost síťových protokolů, topologie sítí;
- znalost bezpečnostních standardů ISO/IEC 27002, ISO/IEC 27001;
- praktické zkušenosti s EZS, atd.

B.12: Etický hacker / pentester (148)

Specifikace:

- provádění bezpečnostního hodnocení a etický hacking, (bezpečnostní hodnocení architektury, bezpečnostní hodnocení konfigurace, revize zdrojového kódu, penetrační testy zaměřující se na síťovou aplikační vrstvu, včetně mobilních a IoT technologií);
- návrh implementace bezpečnostních řešení napříč různými doménami včetně cloud computingu, DLP, identity managementu, mobilní bezpečnosti a řízení zranitelností;
- sdílení provedených expertíz jako součást širších IT rizik, kybernetických a regulatorních projektů v oblasti IT.

Požadavky:

- absolvent magisterského studia v oboru se zaměřením na informační technologie;
- mít relevantní pracovní zkušenosti (alespoň 2 roky na obdobné pozici);
- být schopen pracovat samostatně a na několika projektech v rychle se měnícím prostředí;

Příloha C – Přehledy studijních plánů

C.1 České vysoké učení technické v Praze – Fakulta informačních technologií (152)

Studijní obor: Bezpečnost a informační technologie (bakalářský)			
Semestr	**Název předmětu**	**Rozsah výuky[68]**	**ECTS kredit**
1.	Programování a algoritmizace 1	2+2+2	6
	Právo a informatika	2+0+0	3
	Číslicové a analogové obvody	2+2+0	5
	Programování v shellu 1	2+2+0	5
	Matematická logika	2+1+0	5
	Základy matematické analýzy	3+2+0	6
2.	Programování a algoritmizace 2	2+3+0	7
	Databázové systémy	2+2+1	6
	Struktura a architektura počítačů	2+3+0	6
	Lineární algebra	4+2+0	7
3.	Algoritmy a grafy 1	2+2+0	6
	Automaty a gramatiky	2+2+0	6
	Základy diskrétní matematiky	2+2+0	5
	Administrace OS Windows	2+1+0	4
	Architektury počítačových systémů	2+2+0	5
4.	Bezpečnost	2+2+0	6
	Operační systémy	2+2+0	5

[68] U oborů, kde jsou některé z předmětů vyučovány v laboratořích je rozsah výuky uváděn ve formátu p+c+l (p=přednáška, c=cvičení, l=laboratoř). V oborech, kde součástí žádného z předmětů není výuka v laboratořích je používán formát p+c (p=přednáška, c=cvičení).

	Počítačové sítě	2+2+0	5
	Administrace OS Unix	2+2+0	5
	Bezpečný kód	2+2+0	5
5.	Softwarové inženýrství I	2+1+0	5
	Pravděpodobnost a statistika	2+2+0	5
	Hardwarová bezpečnost	2+2+0	5
	Systémová a síťová bezpečnost	2+2+0	5
	Ekonomické a manažerské principy	2+2+0	4
6.	Dokumentace, prezentace, rétorika	2+2+0	4

C.2 České vysoké učení technické v Praze – Fakulta informačních technologií (152)

Studijní obor: Počítačová bezpečnost (navazující magisterský)

Semestr	**Název předmětu**	**Rozsah výuky**	**ECTS kredit**
1.	Problémy a algoritmy	2+2	5
	Matematika pro informatiku	3+2	7
	Moderní technologie Internetu	2+1	5
	Reverzní inženýrství	1+2	5
2.	Paralelní a distribuované programování	2+2	5
	Statistika pro informatiku	4+2	7
	Hardwarová bezpečnost	2+2	5
	Systémová bezpečnost	2+2	5
	Matematika pro kryptologii	2+1	5
3.	Pokročilá kryptologie	2+2	5
	Síťová bezpečnost	2+1	5
	Povinně volitelně magisterské ekonomicko manažerské předměty, verze 2016: Infor-	2+0	3

	mační bezpečnost		
4.	Povinně volitelné magisterské humanitní předměty, verze 2016: Kybernalita	2+0	3

C.3 České vysoké učení technické v Praze – Fakulta elektrotechnická (153)

Studijní obor: Kybernetická bezpečnost (magisterský)

Semestr	**Název předmětu**	**Rozsah výuky**	**ECTS kredit**
1.	Pokročilá algoritmizace	2+2+0	6
	Pokročilé síťové technologie	2+0+2	6
	Bezpečnost systémů	2+2+0	6
	Statistická analýza dat	2+2+0	6
2.	Teorie algoritmů	3+2+0	6
	Kombinatorická optimalizace	3+2+0	6
	Matematická kryptografie	4+2+0	6
3.	Komunikační bezpečnost	3+2+0	6
	Zajištění kvality software	2+2+0	6
4.	Volitelné odborné předměty[69]	v závislosti na zvoleném předmětu	5

[69] Nejsou zahrnuty v analýze.

C.4 Masarykova univerzita – Fakulta informatiky (154)

Studijní obor: Bezpečnost informačních technologií (zaměření: Kybernetická bezpečnost) (navazující magisterský)[70]			
Semestr	**Název předmětu**	**Rozsah výuky**	**ECTS kredit**
1.	Graph Theory (Teorie grafů – povinně volitelný)	2+1+0	5
	Statistics for Computer Science (Statistika pro výpočetní vědy)	2+2+0	6
	Advanced Computer Networking (Pokročilé síťové technologie – povinně volitelný)	2+0+0	4
	Komunikace člověka s počítačem (povinně volitelný)	1+1+0	4
	Communication and Soft Skills (Komunikace a měkké dovednosti)	3+2+0	7
	Teorie a metoda práva ICT	0+2+0	3
2.	Specifika online komunikace	0+2+0	4
	Real Time Systems (Real-time systémy – povinně volitelný)[71]	2+0+0	4
	System Verification and Assurance (Systémové ověření a ujištění – povinně volitelný)	2+2+2	8
	Probability in Computer Science (Pravděpodobnost ve výpočetních vědách)	2+2+0	6
	Advanced Topics of Cyber Security (Pokročilá témata kybernetické bezpečnosti)	2+1+1	5

[70] Obor nemá v doporučeném studijním plánu zahrnut povinný předmět „Řízení informační bezpečnosti“ v rozsahu 2+0+0 za 4 ECTS kredity. V uvedeném přehledu chybí, nicméně do analýzy v kap. 12. – „Analýza studijních oborů“ byl zahrnut, neboť se předpokládá, že absolvent tento povinný požadavek musí splnit.

[71] Systémy, které provádějí výpočetní operace v reálném čase.

	Úvod do práva ICT I	2+1+0	4
	Kyberkriminalita a kybernetická bezpečnost	0+2+0	3
3.	Advanced Topics in Information Technology Security (Pokročilá témata v bezpečnosti informačních technologií)	1+1+2	6
	Secure coding principles and practices (Principy a praktiky bezpečného kódování – povinně volitelný)	2+2+2	8
	Applied Cryptography (Aplikovaná kryptografie)	1+1+1	5
	Laboratory of security and applied cryptography (Laboratoř bezpečnosti a aplikované kryptografie – povinně volitelný)	0+2+1	3
	Úvod do práva ICT II	2+1+0	4
4.	Postgraduate seminar on IT security and cryptography (Postgraduální seminář o IT bezpečnosti a kryptografii)	0+2+1	4

C.5 Univerzita Tomáše Bati ve Zlíně – Fakulta aplikované informatiky (155)

Studijní obor: Bezpečnostní technologie, systémy a management (bakalářský)

Semestr	**Název předmětu**	**Rozsah výuky**	**ECTS kredit**
1.	Matematický seminář	2+4+0	6
	Základy počítačové techniky	0+0+2	2
	Základy informatiky	2+0+2	5
	Systemizace bezpečnostního průmyslu	3+1+0	4
	Fyzika v bezpečnostních technologiích	2+1+0	4
	Právní řád I	3+1+0	4
	Inženýrská grafika	1+0+2	3
2.	Matematická analýza	2+3+0	6

	Mechanika a termika	3+2+0	5
	Elektrické obvody	2+1+2	5
	Právní řád II	3+1+0	4
	Mechanické zábranné systémy	2+0+1	4
	Programování	0+1+3	4
3.	Diferenciální rovnice	2+2+0	4
	Instrumentace a měření	2+0+2	5
	Operační systémy a jejich bezpečnost	2+0+2	4
	Základy informatiky	2+0+2	5
	Psychologie a marketingové komunikace	2+1+0	3
	Elektřina a magnetizmus	2+2+2	5
4.	Technologie komerční bezpečnosti I	3+1+0	4
	Elektrotechnika a průmyslová elektronika	2+1+2	6
	Technické prostředky bezpečnostního průmyslu	2+0+2	5
	Databázové systémy	1+0+2	5
	Počítačové sítě	2+0+0	4
	Kriminalistické technologie a systémy	2+0+2	5
5.	Mikroelektronika	2+0+2	4
	Technologie komerční bezpečnosti II	3+1+0	4
	Mikropočítače a PLC	2+0+3	4
	Technologie detektivních činností	2+1+0	4
	Elektronické bezpečnostní systémy	3+1+2	6
	Kryptologie	2+0+2	5
6.	Projektování bezpečnostních systémů	2+2+0	5
	Bezpečnost informací	2+0+2	4
	Speciální bezpečnostní technologie	2+1+0	4

C.6 Univerzita Tomáše Bati ve Zlíně – Fakulta aplikované informatiky (155)

Studijní obor: Bezpečnostní technologie, systémy a management (navazující magisterský)

Semestr	Název předmětu	Rozsah výuky	ECTS kredit
1.	Podnikatelské právo v průmyslu komerční bezpečnosti	2+1+0	4
	Provoz počítačových sítí	2+0+2	4
	IZS státu, krizový a informační management	2+1+1	5
	Telekomunikační systémy	2+0+2	4
	Robotika	2+0+2	6
	Nadstandardní prvky objektové bezpečnosti	2+0+2	4
	Počítačové viry a bezpečnost	1+0+2	3
	Odborná praxe		5
2.	Geografické informační systémy	1+0+2	4
	Informační systémy	2+0+2	5
	Bezpečnostní technologie ochrany informačních systémů	2+0+2	3
	Technologie budov	2+0+2	4
	Elektronické zabezpečovací a přístupové systémy	2+0+2	4
	Kriminologie	2+1+0	4
	Ergonomie a psychologie bezpečnosti	1+0+1	2
3.	Kybernetická bezpečnost	2+0+2	4
	Kamerové systémy	2+0+2	4
	Projektování integrovaných systémů	2+0+2	6
	Modelování krizových situací	2+1+2	6
	Elektromagnetická kompatibilita	2+0+1	3
	Forenzní vědy	2+2+0	5

4.	Management bezpečnostního inženýrství	2+1+0	4
	Základy podnikání	0+2+0	3
	Základy první pomoci	0+7+0	1

C.7 Vysoká škola báňská – Technická univerzita Ostrava – Fakulta elektrotechniky a informatiky (156)

Studijní obor: Informační a komunikační bezpečnost (navazující magisterský)

Semestr	**Název předmětu**	**Rozsah výuky**	**ECTS kredit**
1.	Bezpečnost v elektrotechnice	1+0	1
	Multimediální komunikace a zabezpečení obsahu	2+2	4
	Počítačové viry a bezpečnost počítačových systémů	2+2	4
2.	Bezpečnost v komunikacích	2+2	4
	Kryptografie a počítačová bezpečnost	2+2	4
	Počítačová obrana a útok	2+2	4
	Pravděpodobnost a statistika	3+3	6
3.	Kyberkriminalita	2+2	4
4.	Bezpečnost počítačových sítí datových center a cloudových služeb	2+2	4

C.8 Vysoké učení technické v Brně – Fakulta elektrotechniky a komunikačních technologií (157)

Studijní obor: Informační bezpečnost (bakalářský)

Semestr	Název předmětu	Rozsah výuky[72]	ECTS kredit
1.	Fyzika 1	2+1+2	6
	Matematika 1	4+2+0	7
	Počítače a programování 1	2+2+0	5
	Právní nauka	2+0+0	7
	Základy kryptografie	2+3+0	6
2.	Aplikovaná kryptografie	2+2+2	7
	Diskrétní matematika	2+2+0	6
	Matematika	3+2+0	6
	Počítače a programování 2	2+2+0	5
	Úvod do práva ICT 1	2+1+0	4
3.	Komunikační technologie	2+0+3	6
	Management	2+1+0	5
	Mikroekonomie	2+1+0	5
	Pravděpodobnost a statistika	2+2+0	5
	Úvod do práva ICT 2	2+1+0	4
4.	Bezpečnost ICT 1	2+2+2	7
	Datová komunikace	3+1+1	6
	Makroekonomie	2+1+0	5

[72] Bylo dopočítáno z uvedených údajů. Detail oboru: Informační bezpečnost. *Vysoké učení technické v Brně* [online]. Brno: VUT, 2017 [cit. 2017-04-10]. Dostupné z: https://www.vutbr.cz/studium/ects-katalog/detail-oboru?oid=10687

	Síťové operační systémy	2+2+0	5
	Teoretická informatika	2+4+0	7
5.	Bezpečnost ICT 2	2+2+2	7
	Multimediální služby	2+0+2	5
	Softwarové právo	2+0+0	3
6.	Cryptologic Protocol Theory (Teorie kryptografických protokolů)	2+0+1	4
	Kyberkriminalita	2+0+0	3
	Odborná praxe[73]	v rozsahu 160 hodin	0

C.9 Vysoké učení technické v Brně – Fakulta informačních technologií (158)

Studijní obor: Bezpečnost informačních technologií (magisterský)[74]

Semestr	**Název předmětu**	**Rozsah výuky[75]**	**ECTS kredit**
1.	Matematické struktury v informatice	3+1+0	5
	Teoretická informatika	3+1+0	5
	Hardware/Software Codesign (povinně volitelný)	3+1+0	5
2.	Funkcionální a logické programování	2+2+0	5
	Kódování a komprese dat	2+2+0	5
	Paralelní a distribuované algoritmy	3+1+0	5

[73] Není hodnocena ECTS kredity, ale je podmínkou pro absolvování bakalářského studia.

[74] Byly analyzovány osnovy předmětů z akademického roku 2012/2013. Pro akad. rok 2016/2017 nejsou osnovy k dispozici. Skladba povinných a povinně volitelných předmětů se, až na jeden odebraný předmět v akad. roce 2016/2017, nezměnila.

[75] Bylo dopočítáno z dostupných údajů z akademického roku 2012/2013. Pro akad. rok 2016/2017 není rozsah k dispozici. Detail oboru: Bezpečnost informačních technologií. *Vysoké učení technické v Brně* [online]. Brno: VUT, 2017 [cit. 2017-04-10]. Dostupné z: https://www.vutbr.cz/studium/ects-katalog/detail-oboru?oid=11250

	Přenos dat, počítačové sítě a protokoly	3+1+0	5
3.	Biometrické systémy	3+0+1	5
4.	Kryptografie	2+1+0	5
	Návrh, správa a bezpečnost	2+2+0	5