Karta (nových) kompetencí pro sektor ICT (Kybernetická bezpečnost)

1. PŘEHLED SEKTOROVÝCH TRENDŮ

Východiskem pro identifikaci nových kompetencí je **monitoring aktuálních a budoucích trendů**, které sektor mění a redefinují kvalifikační požadavky na pracovníky v příslušném sektoru. Jsou zde zaznamenány trendy a změny, které odvětví aktuálně proměňují (nové) anebo ty, jež mají takový potenciál do budoucna (budoucí).

Identifikované **trendy** (resp. technologie, produkty či služby) jsou jednotně uváděny jako „**Pojem K 4.0**“, který odkazuje k Průmyslu 4.0 i zkrácenému názvu projektu „Kompetence 4.0“. Přehled je výsledkem obsahové analýzy dostupných národních a mezinárodních informačních zdrojů, identifikovaných analytiky projektu, a dále zdrojů doporučených panelem expertů (pracovní skupinou). Výsledný přehled, předkládaný k veřejnému připomínkování, byl panelem expertů verifikován. Složení pracovní skupiny je uvedeno na konci dokumentu.

Tabulka č. 1: Přehled sektorových trendů

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
Automatizace				
Digitální dvojče		nová	https://www.vseoprumyslu.cz/digitalizace/digitalni-prototypovani/digitalni-dvojce-vudci-technologie-inteligentniho-prumyslu.html	Digitální dvojče je digitální model reálného, například výrobního, měřicího apod. automatizovaného zařízení, na němž lze simulovat jeho fungování, komunikaci mezi jeho složkami atd. Může se také učit z různých zdrojů a adaptovat na měnící se podmínky. Taková virtuální replika reálných zařízení pomáhá odhalit různé chyby a nesrovnalosti ještě předtím, než se dané zařízení uvede do provozu. Využívá se hlavně ve výrobních závodech, kde dokáže zkrátit dobu zprovoznění nových linek či závodů a umožňuje zvyšovat jejich efektivitu.

Projekt Mapování budoucích kompetencí jako součást systémových opatření pro vymezení požadavků trhu práce je financován z Evropského sociálního fondu v rámci Operačního programu Zaměstnanost a státního rozpočtu ČR.

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
				V současnosti je pojem digitální dvojče chápán především jako virtuální reprezentace fyzických objektů, jednak výrobních a přepravních zařízení, ale také procesů, systémů, pracovníků nebo celého prostředí. Digitální dvojče tak již není pouze virtuální model reálného protějšku, ale dynamický nositel dat a stavových informací získaných prostřednictvím množství senzorů a snímačů propojených internetem věcí.
Distribuované řídící systémy (DCS)		nová	https://plcynergy.com/what-is-a-dcs/	Distribuované řídicí systémy (DCS) se staly v současné době velice často používané při řízení rozsáhlých a složitých průmyslových procesů a nahrazují dřívější centralizované řídicí systémy. Distribuované architektury řídicích systémů vedou ke zlepšení spolehlivosti a kvality řízení, efektivity řízeného sytému. V současné době se distribuované řídicí systémy nachází v mnoha průmyslových oblastech, jako jsou chemické závody, ropný a plynárenský průmysl, potravinářské jednotky, jaderné elektrárny, vodohospodářské systémy, automobilový průmysl atd. Nacházejí však také uplatnění ve strojní automatizaci.
HMI/SCADA systémy		nová	https://www.vseoprumyslu.cz/automatizace/site-a-komunikace/dosahnete-vice-software-pro-hmi-scada.html	Rozhraní člověk–stroj (HMI) a systémy pro průmyslové řízení a sběr dat SCADA (Supervisory Control and Data Acquisition) mají pro průmyslové organizace zásadní význam. Zejména SCADA umožňuje průmyslovým organizacím řídit průmyslové procesy lokálně nebo na vzdálených místech, sledovat, shromažďovat a zpracovávat data v reálném čase, přímo komunikovat se senzory, ventily, čerpadly, motory a dalšími prvky prostřednictvím softwaru HMI a zaznamenávat události do souboru protokolu.
Kyberfyzický systém		nová	https://www.cio.cz/clanky/fenomen-prumysl-40/	Kyberfyzický systém integruje výpočetní, síťové a fyzické procesy. Počítače a sítě monitorují a řídí fyzické procesy pomocí zpětnovazebných smyček – v závislosti na reakci fyzického systému software interpretuje akci, sleduje výsledky a podle nich upravuje proces. Můžeme si to představit jako počítače a software vložené do zařízení, kde jejich hlavním využitím není samotný výpočet, spíše jde o smyčku akcí a strojové učení.
Prediktivní údržba		nová	https://www2.deloitte.com/cz/cs/pages/deloitte-analytics/solutions/predictive-maintenance.html	Prediktivní údržba pomocí algoritmů pokročilé analytiky a strojového učení hledá vztahy a korelace mezi chováním stroje, jeho okolím, následnou poruchou či odstávkou s cílem určit optimální plán údržby.
Programovatelné logické automaty (PLC, PAC)		nová	https://www.elektroprumysl.cz/automatizace/pr	Programovatelné automaty jsou řídicí systémy přizpůsobené pro řízení průmyslových a technologických procesů, nejběžněji specializované na úlohy převážně logického typu. Svým způsobem je dnes PLC průmyslový mikropočítač

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
			ogramovatelne-automaty-plc	přizpůsobený nasazení v podmínkách průmyslové výroby odolný proti rázům, prachu, výkyvům teplot, vlhkosti, elektrickému i elektromagnetickému rušení. Jedná se tak o klíčový prvek průmyslové automatizace.
Průmyslová a mobilní robotika		nová	https://automa.cz/cz/casopis-clanky/prumyslova-robotika-na-prelomu-stoleti-2000_01_27581_2480/ https://www.vseoprumyslu.cz/robotizace/mobilni-roboty-agv.html	Robotika je interdisciplinární odvětví informatiky a inženýrství. Robotika zahrnuje návrh, konstrukci, provoz a použití robotů. Cílem robotiky je navrhovat stroje, které mohou pomáhat a asistovat lidem. Robotika integruje obory strojírenství, elektrotechnika, informační inženýrství, mechatronika, elektronika, bioinženýrství, počítačové inženýrství, řídicí technika, softwarové inženýrství, matematika atd. Robotika vyvíjí stroje, které dokážou nahradit lidi a replikovat lidskou činnost. Roboty lze použít v mnoha situacích pro mnoho účelů, ale dnes se mnohé používají v nebezpečných prostředích (včetně kontroly radioaktivních materiálů, detekce a deaktivace bomb), výrobních procesech nebo tam, kde lidé nemohou přežít (např. ve vesmíru, pod vodou, ve velkém horku a čištění a zadržování nebezpečných materiálů a záření).
Senzory a měření		nová	https://www.electronicshub.org/different-types-sensors/	Senzory jsou obecně zdroje informací pro nějaký řídící systém, v užším slova smyslu technické zařízení, které měří určitou fyzikální nebo technickou veličinu a převádí ji na signál, který lze dálkově přenášet a dále zpracovat v měřicích a řídících systémech. Nejčastěji jde o elektrický signál (časový průběh napětí nebo proudu); pokud měřená veličina není elektrická, jde o elektrické měření neelektrické veličiny.
Inteligentní sítě				
Digital Asset Management (DAM)		nová	https://brandfolder.com/blog/what-is-digital-asset-management	Správa digitálních aktiv (DAM) je systém softwaru určený k centrálnímu ukládání a správě digitálního obsahu.

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
IT (informační technologie) a OT (operační technologie) konvergence		nová	panel expertů; https://www.ictblog.cz/it-a-ot-postupne-sblizovani-dvou-svetu/	Sbližování IT (informační technologie) a OT (operační technologie). Zavedení digitální inovace určené pro sítě IT do prostředí OT přinese výhody jako je výroba na vyžádání, inventarizace v reálném čase, vzdálené monitorování a orchestrace procesů. To zase vede ke zvýšené efektivitě, produktivitě a ziskovosti. Kritická data a vysoce citlivé zdroje OT je však třeba pečlivě chránit, protože se čím dál častěji stávají cílem hackerů. Původně byly OT a IT sítě izolovány od sebe z dobrého důvodu: Například OT systémy a procesy nemohou odolat latenci. Vysoce citlivé zařízení, které monitoruje termostat na kotli naplněném tisíci litry žíravých chemikálií nebo spravuje složité a vysoce automatizované výrobní patro, závisí na informacích a reakci v reálném čase. Zpoždění nebo prostoje, které se obvykle vyskytují v IT síti, jsou v tomto případě naprosto nemyslitelné. Zařízení OT jsou také v průměru starší a citlivější. Některé mohou zůstat na svém místě a provozovat stejnou aplikaci a operační systém bez jediné aktualizace nebo opravy po celá desetiletí. Což znamená, že mnoho z těchto zařízení je vysoce zranitelných vůči starším bezpečnostním chybám. Hlavní obranou bylo (až doposud) rozhodnutí o jejich vynechání z veřejné IT sítě.
Smart grids		nová	https://energie21.cz/smart-grids-v-cesku-1-soucasnost-a-hlavni-cile/	Smart Grids (SG) jsou chytré elektrické sítě, které se samy monitorují a které dokážou kombinovat klasické centrální zdroje s alternativními zdroji elektrické energie. Zahrnují inteligentní řídicí systém monitorující aktuální provoz sítě, přičemž data jsou pak v reálném čase vyhodnocována a podle aktuální situace se upravuje provoz sítě. Zároveň se monitoruje technický stav sítě, která je schopna tzv. self healingu, kdy se síť za pomoci implementovaných inteligentních prvků dokáže sama bez zásahu člověka uvést do rovnováhy. SG komunikují se zákazníkem v reálném čase a optimalizují jeho spotřebu s ohledem na aktuální cenu elektřiny a k zátěži životního prostředí, což umožňuje lépe začlenit obnovitelné zdroje elektřiny.
Internet věcí				
Edge computing		nová	https://www.globema.cz/edge_computing/	Přesun výpočetní techniky a zpracování z centralizovaných serverů ke zdroji – na zařízení shromažďující tato data.

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
M2M komunikace		nová	https://www.cad.cz/strojirenstvi/38-strojirenstvi/6972-rozdil-mezi-m2m-a-iot.html	Pro komunikaci IoT, označované také zkratkou M2M (Machine-to-machine communication), je charakteristické využívání rádiového spektra. Zařízení M2M je rozmanitá množina datových stanic, které vzájemně předávají informaci přenášenou relativně malou přenosovou rychlostí mezi zařízeními či stroji, např. do centrální databáze, nebo jde o komunikaci mezi zařízením a člověkem. Využití M2M je od individuálního řízení domácnosti, přes senzory, kamerové dohledové systémy, zabezpečovací systémy až po systémy podílející se na účtování dodávek v energetických sítích a jejich distribuovaného řízení (decentralizace výroby energií, inteligentní sítě). Zařízení M2M reagují na určité změny v reálném čase; příkladem jsou měřiče energií a systémy automatizace rozvodných sítí (Smart Grid), spotřeby, teploty, obchodu či moderní lékařské aplikace MBAN diagnostikující zdraví pacientů (e-Health).
Platformy IoT		nová	https://cs.education-wiki.com/9690551-iot-platform	Internet of Things je víceúrovňová platforma, která provádí přímou správu, automatizaci a zajišťování připojených zařízení v okruhu internetu věcí. Je provozován pomocí cloudových, bezpečnostních a expertních systémů připojených k hardwarovým zařízením.
Kybernetická bezpečnost				
Analýza chování uživatelských entit – UEBA		nová	panel expertů; https://www.autocont.cz/portfolio/kyberneticka-bezpecnost/ochrana-dat-pred-unikem-a-kradezi	UEBA je zkratkou pro User and Entity Behavioral Analyse. Jedná se nástroj identifikující model typického a atypického chování lidí a zařízení. Samotné anomální chování je pak poměrově hodnoceno v reálném čase výpočtem bezpečnostního skóre. Na základě jeho celkové výše je možné definovat okamžitou reakci na tento druh události. Celá technologie využívá dnešních moderních metod umělé inteligence a strojového učení a je velmi účinná při odhalování hrozeb původem z interního prostředí organizace. Dále je tato technologie vhodná pro nasazení do prostředí IoT, kde není velký prostor na zajištění bezpečnostních kontrol na samotném koncovém zařízení.
Analýza rizik		nová	Kybernetická bezpečnost (2. díl). Ing. Vymazal, Sdělovací technika 5/2016	Metodika/proces sloužící k rozpoznání, předpovídání a vyhodnocení jednotlivých hrozeb a jejich dopadů na daný informační systém. Analýza rizik navazuje na vlastní bezpečnostní proces a představuje zpětnou vazbu pro daný informační systém a oblasti tímto informačním systémem dotčené.

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
BotNet		nová	https://www.digitalnipevnost.cz/viki/botnet	Botnet je síť nakažených zařízení (boti, zombie), které může útočník vzdáleně ovládat. Malware, kterým jsou zařízení nakažená, je spuštěný na pozadí a uživatel o něm neví. Nakažená zařízení se stávají „spícími agenty“ a v libovolné chvíli je může útočník aktivovat a přikázat jim, aby provedly nějakou akci. Boti jsou napojení na centrální uzel botnetu a očekávají instrukce. Nejčastěji útočníci boty využívají k rozesílání spamu, provádění DDoS útoku nebo šíření dalšího malwaru. Útočníci, kteří botnety provozují, je za účelem finančního zisku pronajímají. Zločinci si například najmou botnet k tomu, aby DDoS útokem vyřadili z provozu weby konkurenčních podniků.
Business Impact Analysis – BIA		nová	panel expertů; https://czwiki.cz/Lexikon/Business_Impact_Analysis	Analýza dopadů (BIA) je základem celého procesu řízení kontinuity činností organizace (Business Continuity Management, BCM). Sestává z technik a metod, pomocí kterých se hodnotí jaké dopady by na organizaci a další zainteresované strany mělo narušení dodávek klíčových produktů nebo služeb organizace a jejich podpůrných kritických činností. Součástí BIA je stanovení minimálních úrovní zdrojů potřebných pro obnovení kritických činností ve stanovených časech a na stanovených úrovních.
ClickFraud		nová	https://www.mediaguru.cz/slovnik-a-mediatypy/slovnik/klicova-slova/podvodne-prokliky-click-fraud/	Podvodné prokliky (Click Fraud) se vztahují k PPC marketingu (součást Search Marketingu). Jedná se o umělé generování klikání na reklamy. PPC systémy jsou systémy, kde se za prokliky platí, tedy umělým navyšováním klikání se zvyšují i náklady zadavatelů.
Digitální gramotnost		nová	https://portaldigi.cz/digislovnik/digitalni-gramotnost/	Digitální gramotnost je soubor kompetencí nutných k identifikaci, pochopení, interpretaci, vytváření, komunikování a účelnému a bezpečnému užití digitálních technologií. Tyto kompetence využívá občan za účelem udržení či zlepšení své kvality života a kvality života svého okolí, tj. např. za účelem pracovní i osobní seberealizace, rozvoje svého potenciálu a udržení či zvýšení participace na společnosti. Referenční model DigComp člení kompetence digitální gramotnosti do těchto oblastí: zpracování informací, komunikace a spolupráce, vytváření digitálního obsahu, bezpečnost a řešení problémů.
Disaster Recovery Plan – DRP		nová	Kybernetická bezpečnost (2. díl). Ing. Vymazal, Sdělovací technika 5/2016	Metodiky a postupy sloužící k obnově funkčnosti informačního systému po živelných pohromách a jiných zásadních událostech.
DLP - Data Leakage (loose) Prevention		nová	panel expertů	Data Loss Prevention technologie se využívá pro identifikaci a ochranu citlivých dat a informací před jejich ztrátou nebo odcizením.

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
Implementační scénář		nová	panel expertů; článek Kybernetická bezpečnost (1. díl), Ing. Michal Vymazal, in Technika a vzdělání	Soubor metodických pokynů a doporučení týkajících se zapojení daného zařízení, infomačního systému, organizačních opatření, technických opatření, best practice apod. To vše pod hlavičkou konkrétní národní bezpečnostní autority, která scénář schválila, zveřejnila na svých stránkách. Každý implementační scénář by měl obsahovat: princip, provedení, funkčnost, efekt a smysl daného celku. Nedílnou součástí je samozřejmě topologické schéma celého řešení.
Kritická informační infrastruktura		nová	panel expertů, https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/povinne-osoby/#od3	Kritickou informační infrastrukturou (KII) se dle § 2 písm. g) a písm. i) zákona č. 240/2000 Sb., krizového zákona, rozumí prvek nebo systém prvků kritické infrastruktury, v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti dle § 2 písm. b) zákona č. 181/2014 Sb. o kybernetické bezpečnosti. V praxi se jedná o takové informační nebo komunikační systémy, příp. ICS/SCADA systémy, které naplní kritéria pro určení prvků KII
Podnikový CERT/CIRT (Computer Emergency Response Team/ Computer Incident Response Team)		nová	NI P4.0	Podnikové týmy pro informační bezpečnost
Ransomware		nová	https://www.zive.cz/ransomware/sc-434/default.aspx	Jako ransomware se označuje typ malwaru, který uživateli brání přistupovat k infikovanému počítači. Pro opětovné získání přístupu je nutné útočníkovi zaplatit. Ransomware někdy šifruje soubory na disku, obrana již nakaženého počítače je proto obtížná
Sandbox		nová	NI P4.0	Sandbox je označení pro bezpečnostní mechanismus v rámci počítačové bezpečnosti, který slouží pro oddělování běžících procesů. Sandbox poskytuje procesům, které v něm běží, omezený přístup ke zdrojům hostitelského počítače - přístup k disku je typicky omezen na vybrané adresáře, přístup k síti na vybrané servery a porty apod. Sandbox je často využíván pro spouštění neotestovaného kódu nebo nedůvěryhodných programů z neověřených třetích stran, od neověřených dodavatelů, či od nedůvěryhodných uživatelů. Sandbox, doslova přeložený jako pískoviště, je vlastně místo, kde se písek nedostane (nemá dostat) mimo vyhrazenou plochu.
SIEM - management bezpečnostních infomací a událostí		nová	panel expertů; https://www.digitalnipevnost.cz/viki/siem	Systém pro správu bezpečnostních informací a událostí (Security Information and Event Management). Jedná se o analytický software, který sbírá a koreluje události z bezpečnostních a síťových zařízení, případně z aplikací. Dokáže identifikovat podezřelé události, jako jsou stažení souborů nebo příliš vysoký přenos informací. SIEM na rozdíl od jiných bezpečnostních softwarů hrozbu neodstraňuje, ale zaznamenává data, která pomohou správcům sítě v podniknutí dalších obranných kroků. SIEM generuje bezpečnostní reporty, které zjednoduší například bezpečnostní audity. SIEM plní funkce dvou samostatných systémů: SIM – Sbírá,

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
				analyzuje a archivuje systémové logy a hlásí problémy, které v nich nalezne; SEM – Události monitoruje v reálném čase a upozorňuje na aktuální bezpečnostní ohrožení. Protože je SIEM primárně analytický nástroj, je vhodné ho v bezpečnostní struktuře propojit s firewallem a dalšími zařízeními v síti.
Zero trust		nová	panel expertů; https://www.computerworld.cz/clanky/sedm-principu-zero-trust/	Nulová důvěra jako základ kybernetické bezpečnosti. V modelu zero trust nemá žádné zařízení ani aktivum inherentní důvěru. Každý požadavek na zdroj by měl vyvolat posouzení bezpečnostního stavu. To zahrnuje nepřetržité monitorování stavu podnikových aktiv, která mají přístup do prostředí, ať už jsou ve vlastnictví organizace nebo jiného subjektu, pokud mají přístup k interním zdrojům.
Virtuální a rozšířená realita				
Rozšířená realita		nová	https://www.netmagnet.cz/blog/rozsirena-realita-a-jeji-vyuziti-v-online-marketingu/	Rozšířená realita nebo také „augumentová realita" je označení pro vizuální dosazení digitálního objektu do reality za pomocí 3D skenů okolního prostředí. Tento objekt zasazený do reálného světa lze poté pozorovat pomocí obrazovky daného zařízení.
Virtualizace		nová	panel nástrojů, https://azure.microsoft.com/cs-cz/overview/what-is-virtualization/	Virtualizace vytváří simulované neboli virtuální výpočetní prostředí namísto fyzického prostředí. Virtualizace často zahrnuje počítačem vytvořené verze hardwaru, operačních systémů, úložných zařízení atd. To umožňuje organizacím rozdělit jeden fyzický počítač nebo server na několik virtuálních počítačů. Každý virtuální počítač pak může pracovat nezávisle a spouštět různé operační systémy nebo aplikace, zatímco sdílí prostředky jediného hostitelského počítače. Virtualizace vytvářením více prostředků z jednoho počítače nebo serveru zlepšuje škálovatelnost a úlohy. Díky tomu ve výsledku snižuje celkový počet využívaných serverů, spotřebu energie, náklady na infrastrukturu a požadovanou údržbu. Virtualizace spadá do čtyř hlavních kategorií. První je virtualizace plochy, která umožňuje jednomu centralizovanému serveru poskytovat a spravovat přizpůsobené plochy. Druhá je virtualizace sítě, navržená pro rozdělení šířky pásma sítě mezi nezávislé kanály, které se později přiřadí konkrétním serverům nebo zařízením. Třetí kategorie je virtualizace softwaru, která odděluje aplikace od hardwaru a operačního systému. Čtvrtá kategorie je virtualizace úložiště, která kombinuje několik prostředků síťového úložiště v jediném úložném zařízení, ke kterému má přístup více uživatelů.
Virtuální realita		nová	https://vreducation.cz/virtualni-realita-historie-a-soucasnost/	Virtuální realita (VR) je technologie umožňující uživateli ocitnout se v simulovaném prostředí, ideálně doprovázené jeho interakcí s ním. Technologie virtuální reality

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
				vytvářejí iluzi skutečného světa (např. při výcviku boje, pilotování, lékařství), nebo fiktivního světa počítačových her.
Sítě				
5G sítě		nová	panel expertů; https://www.ctu.cz/5g	Nová generace mobilních sítí. Navazuje na předchozí generace sítí 3G (přinesla rozšíření internetu do mobilu a vedla k rozmachu smartphonů) a 4G (nabídla mnohem rychlejší přenos dat a umožnila například sledovat streamovaná videa na cestách). 5G odráží nové potřeby komunikace jak na straně koncových uživatelů, tak i v oblasti průmyslu a výhledově i v dalších sektorech. K optimalizaci provozu a snížení rušení jsou používány tzv. aktivní antény umožňující zlepšit využití kmitočtů použitím směrování vyzařovaných svazků rádiových vln. Aktivní antény umožňují základnové stanici dynamicky směřovat vysílaný signál (rádiové svazky) zejména do míst, kde se nacházejí terminály. Technologie elektrického nasměrování svazku bez nutnosti mechanického nastavení antény je využívána již řadu desetiletí u různých rádiových systémů, nicméně až s potřebou další optimalizace využití kmitočtů (a souvisejícím technickým pokrokem) došlo k zavedení dynamického řízení vyzařování antén i do běžných komerčních systémů.
6G sítě		budoucí	panel expertů; https://6gmobile.fel.cvut.cz/	6G sítě najdou uplatnění hlavně v internetu věcí. Rychlost by mohla dosáhnout až 1 Tb/s. Vzroste i počet komunikačních kanálů, kterými by se signál měl šířit, přičemž vždycky bude třeba vybrat ten nejkvalitnější. Výzkumníci z ČVUT úspěšně ověřili, že s výběrem vhodného komunikačního kanálu může pomoci umělá inteligence.
Správa a analýza dat				
Big Data		nová	NI P4.0; https://www.oracle.com/cz/big-data/what-is-big-data/	Big data jsou rozmanitější data, která přicházejí ve větším rozsahu a s větší rychlostí. Tyto aspekty také známe jako tři R. Jednoduše řečeno, big data jsou větší a komplexnější datové sady především z nových zdrojů. Tyto datové sady jsou tak objemné, že tradiční software pro zpracování dat s nimi jednoduše nedokáže pracovat. Tyto obrovské objemy dat lze ale nyní využít k řešení (nejen) obchodních problémů, které bylo v minulosti téměř nemožné řešit.
Business Intelligence - BI		nová	https://managementmania.com/cs/business-intelligence	Business Intelligence (používá se též zkratka BI) je označení pro analytické a vykazovací podnikové aplikace. Umožňují ucelenou a efektivní práci s firemními daty, slouží jak pro zpracování dat z minulosti, tak také pro předpovědi či simulace

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
				budoucího vývoje. Jejich hlavním cílem je poskytnout kvalitní data pro rychlejší a efektivnější rozhodování.
Datové jezero		nová	https://docs.microsoft.com/cs-cz/azure/architecture/data-guide/scenarios/data-lake	Data Lake je úložiště, které obsahuje velké množství dat v nativním, nezpracovaném formátu. Data Lake Store jsou optimalizovaná pro škálování na terabajty a petabajty dat. Data obvykle pocházejí z několika heterogenních zdrojů a můžou být strukturovaná, částečně strukturovaná nebo nestrukturovaná. Ve nápadu s Data Lake je ukládání všeho v původním, netransformované stavu. Tento přístup se liší od tradičního datového skladu, který transformuje a zpracovává data v době přijímání.
Prediktivní analytika		nová	https://www.growdata.cz/trendy-v-bi-2020/	Prediktivní analytika vychází ze získaných informací a ze stávajících datových souborů za účelem předpovězení budoucích pravděpodobností. Jelikož jsou budoucí data odhadovaná, je nutné vždy zahrnout možnost chyby z její definice, i když tyto chyby se neustále snižují, protože softwary, které dnes spravují velké objemy dat, jsou neustále chytřejší a efektivnější. Prediktivní analytika ukazuje, co se může v budoucnu stát s přijatelnou úrovní spolehlivosti, včetně několika alternativních scénářů a posouzení rizik. Hlavní podstatou je lépe porozumět zákazníkům, produktům, partnerům a identifikovat včas potenciální rizika a příležitosti pro společnost.
Preskriptivní analytika		nová	https://www.growdata.cz/trendy-v-bi-2020/	Preskriptivní analytika jde oproti prediktivní analytice ještě o krok dále do budoucnosti. Prověřuje data nebo obsah, aby bylo možno určit, jaká rozhodnutí by měla být učiněna a jaké kroky podniknuty k dosažení zamýšleného cíle. Je charakterizována technikami v podobě grafové analýzy, simulace, komplexního zpracování událostí, neuronových sítí, heuristiky a strojového učení. Preskriptivní analytika se snaží zjistit, jaký bude dopad budoucího rozhodnutí, aby bylo možné toto rozhodnutí upravit ještě dříve, než budou skutečně učiněno. Tato analytika pomáhá optimalizovat plánování, výrobu, inventarizaci a návrh dodavatelského řetězce tak, aby co nejlépe vyhovoval vašim zákazníkům.
Řízení kvality dat (DQM)		nová	panel expertů; https://www.growdata.cz/trendy-v-bi-2020/	DQM je považováno za klíčový faktor pro zajištění účinné analýzy. Kvalita často spočívá v získávání dat, v datové struktuře, implementaci pokročilých datových procesů, v efektivní distribuci dat, či v dohledu nad správností dat a jejich aktualizací. Pro správné uchopení a upevnění základů, je potřeba podniknout kroky v podobě 5 pilířů: Lidé, Profilování dat, Definování kvality dat, Reporting dat, Oprava dat
Software, hostování, cloud				

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
Service Oriented Architecture (SOA)		nová	NI P4.0; https://managementmania.com/cs/service-oriented-architecture	Service Oriented Architecture (SOA) je koncept či přístup k tvorbě informačních systémů. V pojetí SOA je informační systém rozvíjen a řízen s důrazem služby, tedy pohled konzumentů (zákazníků, uživatelů, jiných systémů).
Site Reliability Engineering		nová	https://docs.microsoft.com/cs-cz/learn/modules/intro-to-site-reliability-engineering/2-what-is-sre-and-why-does-it-matter	Technická disciplína, která pomáhá organizaci udržitelně dosahovat *odpovídající* úrovně spolehlivosti jejích systémů, služeb a produktů.
Software as a Service		nová	NI P4.0; https://it-slovnik.cz/pojem/saas	Software as a Service (v překladu „software jako služba“) je služba, která se týká poskytování softwaru, který je využíván přes webové rozhraní. Služba umožňuje organizacím přístup k funkcím softwaru za dohodnutou cenu, která se pro danou aplikaci obvykle platí jednou za měsíc nebo za rok. Jelikož se při této službě software hostuje na dálku, uživatelé nemusí investovat do dalšího hardwaru. Software as a Service odstraňuje u firem nutnost instalovat, nastavovat nebo aktualizovat daný software.
Storage as a Service		nová	NI P4.0; https://it-slovnik.cz/pojem/saas	Storage as a Service, neboli úložiště jako služba, je služba, kterou si klient či celá firma pronajímá úložný prostor od třetí strany. Data jsou přenášena od klienta k poskytovateli služeb přes internet a klient by pak měl mít ke svým datům přístup za pomoci softwaru poskytnutého provozovatelem úložiště. Tento software se používá k provádění běžných úkolů souvisejících se skladováním dat, jde zejména o zálohování údajů a různé datové přenosy. Služba je využívána nejčastěji u malých a středních firem, protože ty mají obvykle nízké náklady a nemohou si dovolit vlastní servery, IT personál aj.
Umělá inteligence				

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
Brain-Computer Interface		nová	https://inteligentnisvet.cz/clanky/co-je-to-bci-a-proc-bude-rok-2022-pro-tuto-technologii-naprosto-zlomovy	Brain-computer interface (BCI), neuralink, je neurální rozhraní propojující mozek s počítačem, je pojítkem pro spolupráci mezi biologickým mozkem a umělým zařízením, pro jejich oboustrannou komunikaci. Na BCI je možné pohlížet jako na nástroj, ve kterém akce jedince neprocházejí obvyklými výstupy z mozku. BCI umožňuje díky nasnímaným signálům z mozku provádět vnější aktivitu. Můžeme se setkat s pojmem rozhraní mysl-stroj (MMI), někdy i jako přímé nervové rozhraní nebo rozhraní mozek-stroj (BMI). Jde o přímou komunikační cestu mezi mozkem a externím zařízením. BCI systémy jsou často zaměřeny na pomoc, rozšíření nebo opravu lidské kognitivní či smyslově-motorické funkce. Praktické využití lze nalézt v mnoha aplikacích, např. rychlé odpovědi na jednoduché otázky, převod myšlenek na text, ovládání prostředí na monitoru a v neposlední řadě provoz neuro-protéz, které se zaměřují na náhradu či obnovu poškozeného sluchu, zraku a pohybu.
Chatbot		nová	https://powervirtualagents.microsoft.com/cs-cz/what-is-a-chatbot/	Chatbot (chatovací robot) je softwarová aplikace, která se používá k přirozenému zapojení do lidské konverzace. Chatovací roboti se běžně používají v mnoha různých odvětvích pro mnoho různých účelů. Chatovací roboti používají umělou inteligenci a zpracování přirozeného jazyka, aby pomohli uživatelům komunikovat s webovými službami nebo aplikacemi prostřednictvím textu, grafiky nebo řeči. Chatovací roboti mohou rozumět přirozenému lidskému jazyku, simulovat lidskou konverzaci a provádět jednoduché, automatizované úkoly. Chatovací roboti se používají v různých kanálech, jako jsou aplikace pro zasílání zpráv, mobilní aplikace, weby, telefonní linky a hlasové aplikace. Chatovací roboty lze vyvíjet tak, aby zvládali jen několik jednoduchých příkazů, nebo aby sloužili jako komplexní digitální asistenti a interaktivní agenti. Chatovací robot může být součástí větší aplikace nebo může být zcela samostatný.
MLOps: Industrialized AI		nová	Deloitte - Tech Trends 2021:	Nasazování a udržování modelů strojového učení v produkčním provozu.

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
Strojové učení		nová	https://azure.microsoft.com/cs-cz/overview/what-is-machine-learning-platform/	Strojové učení je proces použití matematických modelů dat, pomocí kterých se počítač učí bez přímých instrukcí. Považuje se za součást umělé inteligence. Strojové učení využívá algoritmy k identifikaci vzorů v datech a tyto vzory se pak používají k vytvoření datového modelu, který dokáže formulovat předpovědi. S větším množstvím dat a více zkušenostmi jsou výsledky strojového učení přesnější – stejně jako se lidé zlepšují díky větší praxi. Díky přizpůsobitelnosti je strojové učení skvělou volbou v situacích, kdy se data neustále mění, kdy se charakter požadavku nebo úlohy stále posouvá nebo kdy by naprogramování řešení nebylo efektivně možné.
Vývoj software				
Agilní řízení projektů		nová	https://berufenet.arbeitsagentur.de/berufenet/faces/index?path=null/berufsfelder/suchergebnisseBerufsfelder/kurzbeschreibung/digitalisierung&dkz=129987&fil=eJwzNCAKGBKnjAQAAGl%2FFrM%3D	Flexibilní implementace komplexních požadavků na velké datové / obchodní analytické projekty
DevOps		nová	https://azure.microsoft.com/cs-cz/overview/what-is-devops/	Označení DevOps vzniklo spojením slov vývoj (development, Dev) a provoz (operations, Ops), představuje spojení lidí, procesů a technologií, jehož cílem je zajistit průběžné doručování kvalitních produktů a služeb zákazníkům. DevOps umožňuje dříve izolovaným rolím (vývoj, provoz IT, kontrola kvality a zabezpečení) vzájemnou spolupráci a koordinaci s cílem poskytovat lepší a spolehlivější produkty. Přechodem na kulturu DevOps spolu s využitím nástrojů a postupům týmy získávají schopnost lépe reagovat na potřeby zákazníků, zvýšit důvěru v aplikace, které vytvářejí, a rychleji dosahovat obchodních cílů. DevOps ovlivňuje životní cyklus aplikací prostřednictvím fází plánování, vývoje, doručování a provozu. Jednotlivé fáze se spoléhají na ostatní a nejsou určené pro konkrétní role. V rámci skutečné kultury DevOps je každá role v té či oné míře zapojená ve všech fázích.

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
Kubernetes		nová	https://azure.microsoft.com/cs-cz/topic/what-is-kubernetes/#devops-and-kubernetes	K vytváření moderních aplikací se čím dál častěji používají kontejnery, což jsou balíčky mikroslužeb společně s jejich závislostmi a konfiguracemi. Kubernetes je opensourcový software pro nasazování a správu těchto kontejnerů ve velkém.
Průběžná integrace a průběžné nasazování (CI/CD)		nová	https://azure.microsoft.com/cs-cz/overview/what-is-devops/#practices	Kontinuální integrace je postup vývoje softwaru, při kterém vývojáři často začleňují změny kódu do hlavní větve kódu. Kontinuální integrace využívá automatizované testy, které se spustí vždy při potvrzení nového kódu. to znamená, že kód v hlavní větvi je vždy stabilní. Průběžné doručování je časté automatizované nasazování nových verzí aplikace do provozního prostředí. Automatizací kroků nutných k nasazení týmy omezují výskyt případných problémů, ke kterým by mohlo během nasazení dojít, a umožňují častější aktualizace. Po nasazení obou postupů je výsledným procesem CI/CD, který zahrnuje kompletní automatizaci všech kroků mezi potvrzením kódu a nasazením do produkce. Implementace CI/CD umožňuje týmům soustředit se na sestavování kódu, snižuje nutnou režii a omezuje případné lidské chyby při ručních rutinních krocích. Díky CI/CD je také proces nasazování nového kódu mnohem rychlejší a méně rizikový. Nasazování, ke kterému dochází častěji a s menšími přírůstky, pomáhá týmům zajistit větší flexibilitu a produktivitu získat větší jistotu při spouštění kódu.
Compliance				

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
Governance, Risk Management and Compliance (GRCM)		nová	panel expertů	Kybernetická bezpečnost pracuje s tzv. operačním, resp. nefinančním rizikem. Vyžaduje komplexní pojetí, přičemž každý článek organizace hraje v jejím zajištění svou specifickou roli. Rozhodující přitom zdaleka není jen technologie, na kterou se často klade největší, často bohužel jediný důraz. Přitom největším rizikem obvykle bývá lidský faktor. Mimo nastavení potřebných technických a organizačních opatření a zajištění souladu s legislativou je nutné zavést kontinuální přístup ke kybernetické bezpečnosti, který budou chápat a dodržovat všichni zaměstnanci. K tomu slouží kultura bezpečnosti, resp. firemní kultura, k jejímuž prosazování (nejen) slouží GRCM a CMS. Oba tyto systémy pracují s mitigací významných operačních rizik. GRCM integruje různá data, která spolu souvisí, dohromady. Kdykoli je možné přesně určit, které aktivum má vliv na jaké riziko. Pokud nastane bezpečnostní událost, je odpovědný manažer velmi rychle schopen určit, kde bude mít případný incident dopad, jak se zvýší riziko, a stejně jsem schopen sledovat aktivně vývoj rizika při realizaci nápravných či preventivních opatřeních. Realizace opatření určených pro kybernetickou bezpečnost není z pohledu implementace nijak zásadně odlišná od realizace požadavků standardu řady ISO 27000 a dalších mezinárodních standardů, jako jsou americké NIST.
Kybernetická compliance – důraz na prevenci		nová	panel expertů	Kybernetická compliance (Cybersecurity Compliance) je součástí širšího Complinace Management Systému (CMS) každé organizace (veřejnoprávní i soukromé). Ten je zase součástí celkového řídícího a kontrolního systému organizace. CMS slouží k dosahování shody (tedy compliance) se závaznými pravidly nejrůznějšího druhu a právní závaznosti, včetně pravidel etických. Vlastní kybernetická compliance se pak soustřeďuje zejména na dodržování různých kontrol (obvykle uzákoněných regulačním úřadem, zákonem nebo průmyslovou skupinou) k ochraně důvěrnosti, integrity a dostupnosti dat. Požadavky na compliance se liší podle odvětví a sektoru, ale obvykle zahrnují použití řady specifických organizačních a procesních opatření, systémů a technologií k ochraně dat. Rizika je nutno zohlednit nejen v interních předpisech a postupech pro obchodní a další činnost, ale též ve vnitřní kontrole a v compliance programech (součást CMS).
Decentralizované technologie				

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
BDLT protokol		nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	BDLT je protokolem, který vytváří digitální knihu nezměnitelných záznamů všech činností provedených v rámci daného systému. Díky tomu je taková databáze (registr) mnohem odolnější vůči útokům a nevyžaduje jednoho správce, který by dohlížel nad bezpečností vzniku, uchování a přenosu informace a digitálních hodnot. Zajišťují ji kryptografické algoritmy, které navíc nedovolují záznamy libovolně měnit nebo vícekrát použit, jak to dnes můžeme provést s textem, fotografií, filmem - teměř s každým digitálním obsahem.
Blockchainová adresa a klíče pro šifrování obsahu		nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Slouží k identifikaci uživatelů. Po přistoupení k síti, resp. po založení peněženky, každý účastník automaticky získává: (i) veřejný klíč viditelný všem účastníkům, prostřednictvím kterého mu ostatní mohou posílat zprávy nebo hodnoty (zašifrované a díky tomu neviditelné pro ostatní účastníky);(ii) soukromý klíč, pomocí kterého podepisuje jím poslanou zprávu nebo hodnotu a dešifruje záznamy zasílané ostatními na jehoadresu; (iii) blockchainovou adresu, což je jakási digitální identita uživatele; je pseudonymní, tj. jednoznačně jej identifikuje, ale neodkrývá jeho právní identitu.
Blockchainový vyhledávač		nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Aplikace, která umožňuje vyhledání informací zapsaných do blockchainové databáze.
Decentralizované aplikace	dApps	nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Oproti tradičním aplikacím běží decentralizované aplikace na p2p sítích, nikoliv na jednom počítači. Podmínkou využívání dApps na mobilu, počítači či jakémkoliv zařízení je peněženka (účet), kde jsou uchovány soukromé a veřejné klíče uživatele, díky kterým komunikuje s distribuovaným registrem.
Hashování		nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Matematická funkce, kdy podle daných pravidel lze vytvořit z jakékoliv vstupní informace otisk (hash, číselnou řadu), tj. výrazně zmenšený zápis dat, který původní informaci jednoznačně identifikuje. Sebemenší změna vstupní informace kompletně změní hash.
Chytré smlouvy		nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Jednoduché počítačové programy uložené v BDLT, přičemž výsledek jejich provedení je vždy zapsán do distribuovaného registru.
P2P síť		nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Distribuovaná síť počítačů, které udržují systém v chodu. Počítače (uzly) mohou mít různé role (např. potvrzování transakci); od toho bude také odvislé to, zda budou mít stažený celý registr daného systému (fullnode, plný uzel) či nikoliv.

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
Platební a investiční digitální aktiva		nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Slouží jako měnová jednotka, jako prostředek směny a uchovatel hodnoty. Na rozdíl od tradičních (tzv. fiat) měn mají kryptoměny pevně daná pravidla fungování a emise. Kromě toho jsou využívány jako odměna pro nody, tedy pro uživatele, kteří udržují daný blockchain v chodu.
Registr (kniha stavu)		nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Seznam všech záznamů o interakcích, např. finančních transakcích, nabytých právech k věcem. Velmi často data většího objemu (videa, obrázky, texty) nejsou uložena v BDLT, ale v tvz. off-chain úložištích.
Soukromé systémy s omezeným přístupem	Permissioned private	nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Soukromé systémy s omezeným přístupem (ang. permissioned private) veškerá práva se omezují na předem vybrané subjekty. Zároveň není třeba udržovat velké množství kopií, ani propagovat (vysílat) informace o transakcích po celém světě. Soukromé blockchainy mohou být proto efektivnější. Pro určité okruhy uživatelů může být výhodou vyšší soukromí, kdy jsou na jednu stranu všichni uživatelé identifikováni, a na druhou stranu poskytují informace pouze ostatním partnerům a nikoli veřejnosti. Nevýhodou je, že je daleko menší okruh subjektů, které mohou odhalit chybu v systému a kódu. Ještě větší nevýhodou je, že mají tyto projekty zpravidla nízký počet síťových uzlů, které navíc daleko snáze mohou jednat ve shodě (kolaborovat) proti zájmu celé sítě. Nižší úroveň decentralizace pak způsobuje to, že daný systém pozbývá necenzurovatelnost a nezměnitelnost jednou zapsaných dat. Provozovatel soukromého blockchainu může přepsat historii blockchainu (například za účelem opravy chyby) nebo cenzurovat některé transakce.
Technologie distribuovaného registru		nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Technologie distribuovaného registru umožňuje samostatný výkon předem definovaných úkonů a zároveň bezpečné uložení jejich výsledků bez toho, aby je musela ověřit třetí strana nebo prostředník. Všechny záznamy jsou uloženy (distribuovány) v sítí počítačů - kopie souboru s databází je sdílená a synchronizována mezi účastníky, nikoliv na jednom místě
Transakční síť		nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky (https://www.mpo.cz/assets/cz/podnikani/digitalni-	Prostřednictvím transakční sítě mohou stroje samy vykonávat smlouvy, provádět směnu hodnot a záznamy o jejich komunikaci se budou ukládat do decentralizované databáze.

Pojem K 4.0	Alternativní název	nový/ budoucí	Zdroj informace	Vysvětlení pojmu K 4.0
			spolecnost/2020/1/Potencial_decentralizovanych_technologii_pro_rozvoj_ceske_ekonomiky.pdf)	
Veřejné systémy s omezeným přístupem	Public permissioned)	nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Veřejné systémy s omezeným přístupem (ang. public permissioned) umožňují všem přístup k informacím v systému a iniciování nových záznamů (transakcí); schválit je ale mohou pouze vybraní účastníci, kteří také jako jediní mohou zahájit změnu mechanismu řízení systému.
Veřejné systémy s otevřeným přístupem	Public permisionless	nová	Studie: Potenciál decentralizovaných technologií pro rozvoj české ekonomiky	Veřejné systémy s otevřeným přístupem (ang. public permisionless), kde jsou veškeré transakce a obsahy účtu auditovatelné kýmkoliv a kdokoliv si může stáhnout celý blockchain do svého počítače a podílet se na udržování sítě. Veřejné blockchainy mají otevřený zdrojový kód, existující na více nezávislých počítačích, a jsou proto bezpečnější, plně transparentní a nemají jednoho správce. Správcem je samotný kód programu. Uživatelé jsou si tedy rovni. Výhodou vyšší decentralizace je pak bezpečnost. Nevýhodou je obvykle slabší governance a tím pádem menší akceschopnost ve chvíli, kdy je třeba provést změny v protokolu.

2. NOVÉ ODBORNÉ KOMPETENCE

Nové sektorové trendy (viz Tabulka č. 1) byly v dalším kroku rozpracovány a konkretizovány do podoby **odborných kompetencí**. Zde je popsáno, jak se příslušná změna zkoumaného sektoru promítá do požadavků na kompetence stávajících nebo zcela nových profesí.

Přehled nových sektorových trendů slouží jako jedno z východisek pro definování nových kompetencí. Dalším zdrojem identifikace nových kompetencí je průběžné doplňování struktury a obsahu „kompetenční pyramidy" sektoru ze strany panelu expertů. Přitom dochází ke komparaci návrhů struktury kompetenční pyramidy s aktuálním obsahem Národní soustavy povolání (NSP) a Národní soustavy kvalifikací (NSK), resp. s Centrální databází kompetencí (CDK) a dále s obsahem kurikul (prioritně rámcových vzdělávacích programů – RVP). Jako nové odborné kompetence jsou v tomto procesu akceptovány i dovednosti, které v těchto zdrojích nejsou adekvátně (komplexně) obsaženy. Cílem tohoto postupu je předložit podněty k aktualizaci soustav a/nebo vzdělávacích programů. Z uvedeného vyplývá, že zdrojem pro stanovení nových odborných kompetencí není pouze vstupní analýza nových sektorových trendů, ale i výsledky průběžné činnosti panelu expertů na popisu kompetenční pyramidy, jejich komparace s obsahem vzdělávacích programů a obsahem CDK (soustav NSP a NSK). Výsledný přehled, předkládaný k veřejnému připomínkování, byl panelem expertů verifikován. Složení pracovní skupiny je uvedeno na konci dokumentu.

Vysvětlivky:

Pracovní pozice, alternativní název: *konkretizace povolání (pracovní pozice nebo skupina obdobných pracovních pozic), které v pracovních činnostech novou odbornou kompetenci uplatňuje.*

KÚ = kvalifikační úroveň: *upřesňuje kvalifikační náročnost pracovní pozice. KÚ 3 – typicky učňovská úroveň; KÚ 4-5 – typicky maturitní úroveň; KÚ 6-7 – typicky vysokoškolská/VOŠ úroveň (VOŠ = pouze KÚ 6).*

Stejná odborná kompetence se může u různých pracovních pozic a různých kvalifikačních úrovní opakovat.

Tabulka č. 2: Přehled nových odborných kompetencí

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Bezpečnostní monitoring (SIEM)	Specialista bezpečnostního monitoringu	Specialista SIEM	6-7	Detekce bezpečnostních incidentů
Bezpečnostní monitoring (SIEM)	Specialista bezpečnostního monitoringu	Specialista SIEM	6-7	Řízení procesu zajištění bezpečnosti informací a událostí

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Bezpečnostní monitoring (SIEM)	Specialista bezpečnostního monitoringu	Specialista SIEM	6-7	Tvorba regulárních výrazů
Bezpečnostní technologie	Bezpečnostní technik IT		4	Detekce a prevence síťových útoků
Bezpečnostní technologie	Operátor kybernetického bezpečnostního operačního centra		4	Detekce a prevence síťových útoků
Bezpečnostní technologie	Operátor kybernetického bezpečnostního operačního centra		4	Dodržování zásad etiky a bezpečnostní kultury
Bezpečnostní technologie	Operátor kybernetického bezpečnostního operačního centra		4	Orientace v zásadách bezpečnosti a bezpečnostních složkách
Bezpečnostní technologie	Správce klasifikovaných dat		4	Detekce a prevence síťových útoků
Bezpečnostní technologie	Správce klasifikovaných dat		4	Dodržování zásad etiky a bezpečnostní kultury
Bezpečnostní technologie	Správce klasifikovaných dat		4	Orientace v bezpečnostních hrozbách
Bezpečnostní technologie	Správce klasifikovaných dat		4	Orientace v zásadách bezpečnosti a bezpečnostních složkách
Bezpečnostní technologie	Správce komponent datové a serverové infrastruktury		4	Detekce a prevence síťových útoků
Bezpečnostní technologie	Správce komponent datové a serverové infrastruktury		4	Dodržování zásad etiky a bezpečnostní kultury
Bezpečnostní technologie	Správce komponent datové a serverové infrastruktury		4	Orientace v bezpečnostních hrozbách
Bezpečnostní technologie	Správce komponent datové a serverové infrastruktury		4	Orientace v zásadách bezpečnosti a bezpečnostních složkách
Bezpečnostní technologie	Správce operačních systémů		4	Detekce a prevence síťových útoků
Bezpečnostní technologie	Správce operačních systémů		4	Dodržování zásad etiky a bezpečnostní kultury
Bezpečnostní technologie	Správce operačních systémů		4	Orientace v bezpečnostních hrozbách

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Bezpečnostní technologie	Správce operačních systémů		4	Orientace v zásadách bezpečnosti a bezpečnostních složkách
Bezpečnostní technologie	Technik datového centra		4	Detekce a prevence síťových útoků
Bezpečnostní technologie	Technik datového centra		4	Dodržování zásad etiky a bezpečnostní kultury
Bezpečnostní technologie	Technik datového centra		4	Orientace v bezpečnostních hrozbách
Bezpečnostní technologie	Technik datového centra		4	Orientace v zásadách bezpečnosti a bezpečnostních složkách
Bezpečnostní technologie	Technik datových analýz a programátor specifických algoritmů		4	Detekce a prevence síťových útoků
Bezpečnostní technologie	Technik datových analýz a programátor specifických algoritmů		4	Dodržování zásad etiky a bezpečnostní kultury
Bezpečnostní technologie	Technik datových analýz a programátor specifických algoritmů		4	Orientace v bezpečnostních hrozbách
Bezpečnostní technologie	Technik datových analýz a programátor specifických algoritmů		4	Orientace v zásadách bezpečnosti a bezpečnostních složkách
Big data	Datový technik		4-6	Třídění dat
Big data	Datový technik		4-6	Zajišťování sběru dat
Big data	Datový vědec		6-7	Prediktivní modelování
Big data	Datový vědec		6-7	Provádění analýzy dat
Big data	Datový vědec		6-7	Systematizace dat z různých formátů
Big data	Datový vědec		6-7	Systematizace dat z různých zdrojů
Big data	Datový vědec		6-7	Třídění dat
Big data	Datový vědec		6-7	Vyhodnocování relevance dat

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Big data	Datový vědec		6-7	Zajišťování sběru dat
Datová analýza	Bezpečnostní analytik		7	Čištění dat
Datová analýza	Bezpečnostní analytik		7	Dolování dat
Datová analýza	Bezpečnostní analytik		7	Orientace v základních metodách analýzy dat
Datová analýza	Bezpečnostní analytik		7	Předzpracování dat
Datová analýza	Bezpečnostní analytik		7	Topologická analýza dat
Datová analýza	Bezpečnostní analytik		7	Využívání různých typů a zdrojů pro dolování dat
Datová analýza	Bezpečnostní analytik		7	Detekování počítačových útoků
Elektronické zabezpečovací systémy	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Analýza odolnosti zabezpečovacího systému
Elektronické zabezpečovací systémy	Architekt kybernetické bezpečnosti		4-7	Analýza sociálních sítí
Elektronické zabezpečovací systémy	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Orientace v legislativě související se zabezpečovacími systémy
Elektronické zabezpečovací systémy	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Šifrování při přenosu dat
Elektronické zabezpečovací systémy	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Tvorba spolehlivostních modelů
Elektronické zabezpečovací systémy	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Zpracování obrazu v zabezpečovacích systémech
Elektronické zabezpečovací systémy	Architekt kybernetické bezpečnosti		4-7	Detekování počítačových útoků
Elektronické zabezpečovací systémy	Bezpečnostní analytik		7	Analýza odolnosti zabezpečovacího systému
Elektronické zabezpečovací systémy	Bezpečnostní analytik		7	Analýza sociálních sítí

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Elektronické zabezpečovací systémy	Bezpečnostní analytik		7	Orientace v legislativě související se zabezpečovacími systémy
Elektronické zabezpečovací systémy	Bezpečnostní analytik		7	Šifrování při přenosu dat
Elektronické zabezpečovací systémy	Bezpečnostní analytik		7	Tvorba spolehlivostních modelů
Elektronické zabezpečovací systémy	Bezpečnostní analytik		7	Zpracování obrazu v zabezpečovacích systémech
Elektronické zabezpečovací systémy	Risk manažer		7	Analýza odolnosti zabezpečovacího systému
Elektronické zabezpečovací systémy	Risk manažer		7	Analýza sociálních sítí
Elektronické zabezpečovací systémy	Risk manažer		7	Orientace v čipových kartách, kontaktních a bezkontaktních systémech
Elektronické zabezpečovací systémy	Risk manažer		7	Orientace v legislativě související se zabezpečovacími systémy
Elektronické zabezpečovací systémy	Risk manažer		7	Orientace v principech a vlastnostech senzorů používaných v zabezpečovacích systémech
Elektronické zabezpečovací systémy	Risk manažer		7	Orientace v systémech napájení zabezpečovacích systémů
Elektronické zabezpečovací systémy	Risk manažer		7	Šifrování při přenosu dat
Elektronické zabezpečovací systémy	Risk manažer		7	Tvorba spolehlivostních modelů
Elektronické zabezpečovací systémy	Risk manažer		7	Zpracování obrazu v zabezpečovacích systémech
Elektronické zabezpečovací systémy	Risk manažer		7	Detekování počítačových útoků
Elektronické zabezpečovací systémy	Síťový specialista		4-7	Analýza odolnosti zabezpečovacího systému

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Elektronické zabezpečovací systémy	Síťový specialista		4-7	Orientace v čipových kartách, kontaktních a bezkontaktních systémech
Elektronické zabezpečovací systémy	Síťový specialista		4-7	Orientace v legislativě související se zabezpečovacími systémy
Elektronické zabezpečovací systémy	Síťový specialista		4-7	Orientace v principech a vlastnostech senzorů používaných v zabezpečovacích systémech
Elektronické zabezpečovací systémy	Síťový specialista		4-7	Orientace v systémech napájení zabezpečovacích systémů
Elektronické zabezpečovací systémy	Síťový specialista		7	Šifrování při přenosu dat
Elektronické zabezpečovací systémy	Síťový specialista		7	Tvorba spolehlivostních modelů
Elektronické zabezpečovací systémy	Síťový specialista		7	Zpracování obrazu v zabezpečovacích systémech
Elektronické zabezpečovací systémy	Systémový architekt		7	Analýza odolnosti zabezpečovacího systému
Elektronické zabezpečovací systémy	Systémový architekt		7	Analýza sociálních sítí
Elektronické zabezpečovací systémy	Systémový architekt		7	Orientace v čipových kartách, kontaktních a bezkontaktních systémech
Elektronické zabezpečovací systémy	Systémový architekt		7	Orientace v legislativě související se zabezpečovacími systémy
Elektronické zabezpečovací systémy	Systémový architekt		7	Orientace v principech a vlastnostech senzorů používaných v zabezpečovacích systémech
Elektronické zabezpečovací systémy	Systémový architekt		7	Orientace v systémech napájení zabezpečovacích systémů
Elektronické zabezpečovací systémy	Systémový architekt		7	Šifrování při přenosu dat
Elektronické zabezpečovací systémy	Systémový architekt		7	Tvorba spolehlivostních modelů

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Elektronické zabezpečovací systémy	Systémový architekt		7	Zpracování obrazu v zabezpečovacích systémech
Elektronické zabezpečovací systémy	Systémový architekt		7	Detekování počítačových útoků
Kryptografie	Vývojář kryptografických nástrojů		4-7	Asymetrické šifrování dat
Kryptografie	Vývojář kryptografických nástrojů		4-7	Dešifrování dat šifrovaných asymetricky
Kryptografie	Vývojář kryptografických nástrojů		4-7	Dešifrování dat šifrovaných symetricky
Kryptografie	Vývojář kryptografických nástrojů		4-7	Posuzování rezistence šifrování
Kryptografie	Vývojář kryptografických nástrojů		4-7	Symetrické šifrování dat
Kryptografie	Vývojář kryptografických nástrojů		4-7	Šifrování citlivých dat a know-how organizace
Kryptografie	Vývojář kryptografických nástrojů		4-7	Šifrování dat organizace
Kryptografie	Vývojář kryptografických nástrojů		4-7	Šifrování soukromých dat
Kryptografie	Architekt aplikované kryptografie		4-7	Asymetrické šifrování dat
Kryptografie	Architekt aplikované kryptografie		4-7	Dešifrování dat šifrovaných asymetricky
Kryptografie	Architekt aplikované kryptografie		4-7	Dešifrování dat šifrovaných symetricky
Kryptografie	Architekt aplikované kryptografie		4-7	Posuzování rezistence šifrování
Kryptografie	Architekt aplikované kryptografie		4-7	Symetrické šifrování dat

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Kryptografie	Architekt aplikované kryptografie		4-7	Šifrování citlivých dat a know-how organizace
Kryptografie	Architekt aplikované kryptografie		4-7	Šifrování dat organizace
Kryptografie	Architekt aplikované kryptografie		4-7	Šifrování soukromých dat
Kryptografie	Specialista testování kryptografických nástrojů		4-7	Asymetrické šifrování dat
Kryptografie	Specialista testování kryptografických nástrojů		4-7	Dešifrování dat šifrovaných asymetricky
Kryptografie	Specialista testování kryptografických nástrojů		4-7	Dešifrování dat šifrovaných symetricky
Kryptografie	Specialista testování kryptografických nástrojů		4-7	Posuzování rezistence šifrování
Kryptografie	Specialista testování kryptografických nástrojů		4-7	Symetrické šifrování dat
Kryptografie	Specialista testování kryptografických nástrojů		4-7	Šifrování citlivých dat a know-how organizace
Kryptografie	Specialista testování kryptografických nástrojů		4-7	Šifrování dat organizace
Kryptografie	Specialista testování kryptografických nástrojů		4-7	Šifrování soukromých dat
Kryptografie	Správce kryptografické ochrany		4-7	Asymetrické šifrování dat
Kryptografie	Správce kryptografické ochrany		4-7	Dešifrování dat šifrovaných asymetricky
Kryptografie	Správce kryptografické ochrany		4-7	Dešifrování dat šifrovaných symetricky
Kryptografie	Správce kryptografické ochrany		4-7	Posuzování rezistence šifrování

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Kryptografie	Správce kryptografické ochrany		4-7	Symetrické šifrování dat
Kryptografie	Správce kryptografické ochrany		4-7	Šifrování citlivých dat a know-how organizace
Kryptografie	Správce kryptografické ochrany		4-7	Šifrování dat organizace
Kryptografie	Správce kryptografické ochrany		4-7	Šifrování soukromých dat
Kryptografie	Kryptoanalytik		4-7	Asymetrické šifrování dat
Kryptografie	Kryptoanalytik		4-7	Dešifrování dat šifrovaných asymetricky
Kryptografie	Kryptoanalytik		4-7	Dešifrování dat šifrovaných symetricky
Kryptografie	Kryptoanalytik		4-7	Posuzování rezistence šifrování
Kryptografie	Kryptoanalytik		4-7	Symetrické šifrování dat
Kryptografie	Kryptoanalytik		4-7	Šifrování citlivých dat a know-how organizace
Kryptografie	Kryptoanalytik		4-7	Šifrování dat organizace
Kryptografie	Kryptoanalytik		4-7	Šifrování soukromých dat
Kybernetická bezpečnost	Analytik kybernetické bezpečnosti		6-7	Používání systémů a nástrojů UEBA k odhalení anomálií v chování uživatelů a následná optimalizace
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Analýza digitální identity
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti		4-7	Analýza chování uživatele
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Analýza kódu viru, ladící metody a nástroje
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Hledání a zneužívání chyb v software

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Nastavení zabezpečení fyzického perimetru
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Nastavení zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Orientace v technikách pro snížení šance detekce viru
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Penetrační testovaní softwaru
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Posuzování zabezpečení fyzického perimetru
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Posuzování zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti		4-7	Provádění dynamického zálohování
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti		4-7	Provádění hybridního zálohování
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Srovnání operačních systémů a dobře známých zranitelných míst
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Tvorba antiviru, imunizační technologie
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Zabezpečení fyzického perimetru
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Zajištění obrany proti vyděračskému software
Kybernetická bezpečnost	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Zajištění prevence počítačových útoků
Kybernetická bezpečnost	Auditor kybernetické bezpečnosti		4-7	Nastavení zabezpečení fyzického perimetru

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Kybernetická bezpečnost	Auditor kybernetické bezpečnosti		4-7	Nastavení zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Auditor kybernetické bezpečnosti		4-7	Posuzování zabezpečení fyzického perimetru
Kybernetická bezpečnost	Auditor kybernetické bezpečnosti		4-7	Posuzování zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Auditor kybernetické bezpečnosti		4-7	Zabezpečení fyzického perimetru
Kybernetická bezpečnost	Auditor kybernetické bezpečnosti		4-7	Zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Bezpečnostní analytik		7	Analýza digitální identity
Kybernetická bezpečnost	Bezpečnostní analytik		7	Analýza chování uživatele
Kybernetická bezpečnost	Bezpečnostní analytik		7	Analýza kódu viru, ladící metody a nástroje
Kybernetická bezpečnost	Bezpečnostní analytik		7	Hledání a zneužívání chyb v software
Kybernetická bezpečnost	Bezpečnostní analytik		7	Orientace v technikách pro snížení šance detekce viru
Kybernetická bezpečnost	Bezpečnostní analytik		7	Penetrační testovaní softwaru
Kybernetická bezpečnost	Bezpečnostní analytik		7	Provádění dynamického zálohování
Kybernetická bezpečnost	Bezpečnostní analytik		7	Provádění hybridního zálohování
Kybernetická bezpečnost	Bezpečnostní analytik		7	Srovnání operačních systémů a dobře známých zranitelných míst
Kybernetická bezpečnost	Bezpečnostní analytik		7	Tvorba antiviru, imunizační technologie
Kybernetická bezpečnost	Bezpečnostní analytik		7	Zajištění obrany proti vyděračskému software
Kybernetická bezpečnost	Bezpečnostní analytik		7	Zajištění prevence počítačových útoků
Kybernetická bezpečnost	Bezpečnostní technik IT		4	Dodržování zásad bezpečného chování v kybernetickém prostoru

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Kybernetická bezpečnost	Bezpečnostní technik IT		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Bezpečnostní technik IT		4	Orientace v legislativě upravující kybernetickou bezpečnost
Kybernetická bezpečnost	Bezpečnostní technik IT		4	Orientace v metodikách efektivního zavedení kybernetické bezpečnosti
Kybernetická bezpečnost	Bezpečnostní technik IT		4	Orientace ve specifikách informačních systémů státní správy
Kybernetická bezpečnost	Garant aktiv		4-7	Nastavení zabezpečení fyzického perimetru
Kybernetická bezpečnost	Garant aktiv		4-7	Nastavení zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Garant aktiv		4-7	Posuzování zabezpečení fyzického perimetru
Kybernetická bezpečnost	Garant aktiv		4-7	Posuzování zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Garant aktiv		4-7	Zabezpečení fyzického perimetru
Kybernetická bezpečnost	Garant aktiv		4-7	Zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Manažer kybernetické bezpečnosti		4-7	Nastavení zabezpečení fyzického perimetru
Kybernetická bezpečnost	Manažer kybernetické bezpečnosti		4-7	Nastavení zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Manažer kybernetické bezpečnosti		4-7	Posuzování zabezpečení fyzického perimetru
Kybernetická bezpečnost	Manažer kybernetické bezpečnosti		4-7	Posuzování zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Manažer kybernetické bezpečnosti		4-7	Zabezpečení fyzického perimetru
Kybernetická bezpečnost	Manažer kybernetické bezpečnosti		4-7	Zabezpečení kybernetického perimetru
Kybernetická bezpečnost	Operátor kybernetického bezpečnostního operačního centra		4	Dodržování zásad bezpečného chování v kybernetickém prostoru

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Kybernetická bezpečnost	Operátor kybernetického bezpečnostního operačního centra		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Operátor kybernetického bezpečnostního operačního centra		4	Orientace v legislativě upravující kybernetickou bezpečnost
Kybernetická bezpečnost	Operátor kybernetického bezpečnostního operačního centra		4	Orientace v metodikách efektivního zavedení kybernetické bezpečnosti
Kybernetická bezpečnost	Operátor kybernetického bezpečnostního operačního centra		4	Orientace ve specifikách informačních systémů státní správy
Kybernetická bezpečnost	Programátor		4-7	Orientace v problematice bezpečnosti mobilních zařízení: Android a iOS
Kybernetická bezpečnost	Programátor		4-7	Orientace v zásadách psaní bezpečného kódu
Kybernetická bezpečnost	Pověřenec pro ochranu osobních údajů		4-7	Nakládání s citlivými údaji
Kybernetická bezpečnost	Pověřenec pro ochranu osobních údajů		4-7	Zabezpečení osobních údajů v kybernetickém a fyzickém perimetru
Kybernetická bezpečnost	Pověřenec pro ochranu osobních údajů		4-7	Zabezpečení údajů organizace v kybernetickém a fyzickém perimetru
Kybernetická bezpečnost	Pověřenec pro ochranu osobních údajů		4-7	Zabezpečení zdravotních a lékařských záznamů v kybernetickém a fyzickém perimetru
Kybernetická bezpečnost	Risk manažer		7	Analýza digitální identity
Kybernetická bezpečnost	Risk manažer		7	Analýza chování uživatele
Kybernetická bezpečnost	Risk manažer		7	Analýza kódu viru, ladící metody a nástroje
Kybernetická bezpečnost	Risk manažer		7	Hledání a zneužívání chyb v software
Kybernetická bezpečnost	Risk manažer		7	Orientace v technikách pro snížení šance detekce viru

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Kybernetická bezpečnost	Risk manažer		7	Penetrační testovaní softwaru
Kybernetická bezpečnost	Risk manažer		7	Provádění dynamického zálohování
Kybernetická bezpečnost	Risk manažer		7	Provádění hybridního zálohování
Kybernetická bezpečnost	Risk manažer		7	Srovnání operačních systémů a dobře známých zranitelných míst
Kybernetická bezpečnost	Risk manažer		7	Tvorba antiviru, imunizační technologie
Kybernetická bezpečnost	Risk manažer		7	Zajištění obrany proti vyděračskému software
Kybernetická bezpečnost	Risk manažer		7	Zajištění prevence počítačových útoků
Kybernetická bezpečnost	Správce klasifikovaných dat		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Správce klasifikovaných dat		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Správce klasifikovaných dat		4	Orientace v legislativě upravující kybernetickou bezpečnost
Kybernetická bezpečnost	Správce klasifikovaných dat		4	Orientace v metodikách efektivního zavedení kybernetické bezpečnosti
Kybernetická bezpečnost	Správce klasifikovaných dat		4	Orientace ve specifikách informačních systémů státní správy
Kybernetická bezpečnost	Správce komponent datové a serverové infrastruktury		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Správce komponent datové a serverové infrastruktury		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Správce komponent datové a serverové infrastruktury		4	Orientace v legislativě upravující kybernetickou bezpečnost
Kybernetická bezpečnost	Správce komponent datové a serverové infrastruktury		4	Orientace v metodikách efektivního zavedení kybernetické bezpečnosti
Kybernetická bezpečnost	Správce komponent datové a serverové infrastruktury		4	Orientace ve specifikách informačních systémů státní správy

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Kybernetická bezpečnost	Správce operačních systémů		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Správce operačních systémů		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Správce operačních systémů		4	Orientace v legislativě upravující kybernetickou bezpečnost
Kybernetická bezpečnost	Správce operačních systémů		4	Orientace v metodikách efektivního zavedení kybernetické bezpečnosti
Kybernetická bezpečnost	Správce operačních systémů		4	Orientace ve specifikách informačních systémů státní správy
Kybernetická bezpečnost	Systémový architekt		7	Analýza digitální identity
Kybernetická bezpečnost	Systémový architekt		7	Analýza kódu viru, ladící metody a nástroje
Kybernetická bezpečnost	Systémový architekt		7	Hledání a zneužívání chyb v software
Kybernetická bezpečnost	Systémový architekt		7	Orientace v technikách pro snížení šance detekce viru
Kybernetická bezpečnost	Systémový architekt		7	Penetrační testovaní softwaru
Kybernetická bezpečnost	Systémový architekt		7	Provádění dynamického zálohování
Kybernetická bezpečnost	Systémový architekt		7	Provádění hybridního zálohování
Kybernetická bezpečnost	Systémový architekt		7	Srovnání operačních systémů a dobře známých zranitelných míst
Kybernetická bezpečnost	Systémový architekt		7	Tvorba antiviru, imunizační technologie
Kybernetická bezpečnost	Systémový architekt		7	Zajištění obrany proti vyděračskému software
Kybernetická bezpečnost	Systémový architekt		7	Zajištění prevence počítačových útoků
Kybernetická bezpečnost	Technik datového centra		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Technik datového centra		4	Dodržování zásad bezpečného chování v kybernetickém prostoru

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Kybernetická bezpečnost	Technik datového centra		4	Orientace v legislativě upravující kybernetickou bezpečnost
Kybernetická bezpečnost	Technik datového centra		4	Orientace v metodikách efektivního zavedení kybernetické bezpečnosti
Kybernetická bezpečnost	Technik datového centra		4	Orientace ve specifikách informačních systémů státní správy
Kybernetická bezpečnost	Technik datových analýz a programátor specifických algoritmů		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Technik datových analýz a programátor specifických algoritmů		4	Dodržování zásad bezpečného chování v kybernetickém prostoru
Kybernetická bezpečnost	Technik datových analýz a programátor specifických algoritmů		4	Orientace v legislativě upravující kybernetickou bezpečnost
Kybernetická bezpečnost	Technik datových analýz a programátor specifických algoritmů		4	Orientace v metodikách efektivního zavedení kybernetické bezpečnosti
Kybernetická bezpečnost	Technik datových analýz a programátor specifických algoritmů		4	Orientace ve specifikách informačních systémů státní správy
Prediktivní analýza	Datový vědec		6-7	Aplikování a aktualizace prediktivního modelu
Prediktivní analýza	Datový vědec		6-7	Identifikace dostupných zdrojů dat
Prediktivní analýza	Datový vědec		6-7	Shromažďování dat
Prediktivní analýza	Datový vědec		6-7	Specifikace cíle prediktivní analýzy
Prediktivní analýza	Datový vědec		6-7	Testování prediktivního modelu
Prediktivní analýza	Datový vědec		6-7	Vyhodnocování prediktivního modelu
Prediktivní analýza	Datový vědec		6-7	Zpracování dat

Pojem K 4.0 (Předmět)	Pracovní pozice	Alternativní název	KÚ	Odborná kompetence
Prediktivní analýza	Datový vědec		6-7	Zpracování prediktivního modelu
Sítě	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Měření důležitosti vrcholů v sítích
Sítě	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Orientace v algoritmech pro analýzu a vizualizaci sítí
Sítě	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Orientace v typech sítí a jejich vlastnostech
Sítě	Architekt kybernetické bezpečnosti	Bezpečnostní architekt	4-7	Orientace ve struktuře a vlastnostech rozsáhlých sítí
Sítě	Bezpečnostní analytik		7	Orientace v typech sítí a jejich vlastnostech
Sítě	Síťový specialista		7	Měření důležitosti vrcholů v sítích
Sítě	Síťový specialista		7	Orientace v algoritmech pro analýzu a vizualizaci sítí
Sítě	Síťový specialista		7	Orientace v typech sítí a jejich vlastnostech
Sítě	Síťový specialista		7	Orientace ve struktuře a vlastnostech rozsáhlých sítí
Sítě	Síťový specialista		7	Provádění dynamického zálohování
Sítě	Síťový specialista		7	Provádění hybridního zálohování
Sítě	Systémový architekt		7	Měření důležitosti vrcholů v sítích
Sítě	Systémový architekt		7	Orientace v algoritmech pro analýzu a vizualizaci sítí
Sítě	Systémový architekt		7	Orientace v typech sítí a jejich vlastnostech
Sítě	Systémový architekt		7	Orientace ve struktuře a vlastnostech rozsáhlých sítí
Sítě	Systémový architekt		7	Analýza chování uživatele