Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Metody pro vytváření standardů IoT pro využití ve Smart Cities

Disertační práce

Autor: Ing. Bc. Hana Důbravová

Studijní program: Systémové inženýrství a informatika

Studijní obor: Informační a znalostní management

Školitel: prof. Ing. Vladimír Bureš, Ph.D., MBA

Katedra/pracoviště školitele: Katedra informačních technologií

Hradec Králové duben 2024

Prohlášení:

Prohlašuji, že jsem disertační práci zpracovala samostatně a s použitím uvedené literatury.

V Moravanech dne 12. 4. 2024 Ing. Bc. Hana Důbravová

Poděkování:

Ráda bych poděkovala svému školiteli prof. Ing. Vladimíru Bureši, Ph.D., MBA za odbornou podporu a metodické vedení v rámci celého doktorského studia a především při zpracovávání této disertační práce. Dále bych ráda poděkovala své dceři Simoně Švecové, a dalším kolegům, kteří mě podporovali v průběhu celého doktorského studia a při psaní této práce.

Anotace

Koncepce Smart Cities a její postupná implementace do měst a obcí v České republice a v zahraniční je založena na využívání procesů a metod z oblastí informačního a znalostního managementu.

V rámci integrace různých částí koncepce Smart Cities či Smart Home konceptů dochází ke zvyšování potencionálních rizik v rámci kybernetických hrozeb. Tato rizika je nezbytné snižovat prostřednictvím nových nebo aktualizovaných bezpečnostních standardů či právních předpisů. Oblasti, ve kterých jsou využívány Smart technologie, zahrnují především vysoké množství různých IoT senzorů, čidel, aplikací.

Pro vytváření bezpečnostních standardů v oblasti informačních technologií jsou dostupné převážně neefektivní metody s využíváním kancelářských aplikací Microsoft Office. Obdobný neformalizovaný proces je využíván při přípravě a aktualizaci nových právních předpisů. Prvotní oblast přípravy se tak jeví jako neefektivní, zdlouhavá a časově náročná a mnohdy s velkým vytížením vysoce kvalifikovaných pracovníků. S pomocí implementace odpovídajících metod a procesů, které řeší vědní disciplíny znalostního a informační managementu včetně ekonomických věd, může být proces prvotní přípravy nových či aktualizovaných bezpečnostních standardů a nových právních předpisů efektivní, automatizovaný a formalizovaný.

Disertační práce analyzuje, zkoumá a navrhuje optimální metody a procesy využívané v oblastech informačního a znalostního managementu v kombinaci s vhodnými metodami pro zpracovávání textu s cílem zefektivnění procesu prvotní přípravy nových bezpečnostních standardů pro IoT za účelem využití v dílčích tematicky zaměřených částech koncepce Smart Cities a současně proces přípravy a nových právních předpisů na základě zjištění skutečného stavu s následnou validací v rámci expertních skupin.

Hlavním přínosem práce je návrh inovativních metod a jejich kombinace pro vytváření nových bezpečnostních standardů v tematicky zaměřených částech koncepce Smart Cities v České republice a dále při přípravě nových právních předpisů s možností využití při aktualizaci stávajících interních předpisů organizace.

Annotation

The Smart Cities concept and its gradual implementation in cities and municipalities in the Czech Republic and abroad uses processes and methods from information and knowledge management.

Integrating various parts of the Smart Cities or Smart Home concepts increases the potential risks of cyber threats. These risks must be mitigated through new or updated security standards or legislation. The areas where innovative technologies are used mainly include many IoT sensors and applications.

Inefficient methods of using Microsoft Office applications are primarily available for creating security standards in IT. A similar formalised process is used to develop and update new legislation. Thus, the initial preparation area appears inefficient, lengthy, and time-consuming, often with a heavy workload on highly skilled staff. With the implementation of appropriate methods and processes that address the disciplines of knowledge and information management, including economic sciences, the initial preparation of new or updated security standards and new legislation can be efficient, automated, and formalised.

This dissertation analyses, investigates, and proposes optimal methods and processes used in the fields of information and knowledge management in combination with appropriate methods for word processing in order to streamline the process of initial preparation of new security standards for IoT for use in the sub-topics of the Smart Cities concept, and at the same time, the process of preparation and new legislation based on the findings of the actual situation with subsequent validation within expert groups.

The main contribution of the thesis is the proposal of innovative methods and their combination for the creation of new security standards in thematically focused parts of the Smart Cities concept in the Czech Republic, as well as in the preparation of new legislation with the possibility of use in updating existing internal regulations of the organization.

OBSAH

Seznam zkratek

Seznam obrázků

Seznam tabulek

Seznam Business Process Model and Notation

ÚVOD

Přijaté koncepty pro Smart Cities (chytrá města) nebyly v posledních letech zcela komplexní, byly roztříštěné v zahraničí i v České republice. V rámci nekomplexního řešení vzniklo mnoho různých nesourodých dokumentů (metodických doporučení, metodik, strategií aj.). Tyto různorodé strategické dokumenty pro Smart Cities obsahují v obecné a metodické rovině postupy a procesy pro implementaci dílčích prvků a technologií.

Diskuze o budoucnosti Smart Cities bývají hlavními tématy odborných konferencí (Hollands, 2008). Na základě realizovaného průzkumu a na základě stále rostoucí tendence požadavků pro implementaci dílčích částí do měst a obcí byly identifikovány kritické faktory (řízení a organizace, informační technologie, politický kontext, lidé a komunity, ekonomika, vybudovaná infrastruktura a přírodní prostředí aj.), které by měly být řešeny (Chourabi et al., 2012). Identifikace uvedených faktorů a existujících koncepčních přístupů by měla být řešena především v rámci aspektů zaměřených na efektivní integraci a využívání prostředků informačních technologií, procesy a metody při zavádění a řízení dílčích částí koncepce Smart Cities v organizacích (Nam & Pardo, 2011).

V rámci implementace dílčích částí koncepce Smart Cities klíčovou roli sehrávají oblasti informačního (IM) a znalostního managementu (ZM) v návaznosti na oblasti ekonomických věd. Prostřednictvím těchto vědních disciplín jsou integrovány různé metody z oblastí IM a ZM tak, aby postupný proces integrace těchto částí do organizací byl efektivní a formalizovaný. Vědní disciplíny z oblastí managementu zahrnují zejména sběr, analýzu a sdílení informací či zpracovávání dat mezi různými subjekty (obcemi, kraji, městy, bezpečnostními složkami aj.), čímž dochází k efektivnímu využívání těchto informací a současně jsou získávány znalosti nové, na jejichž základu dochází k implementaci inovací.

Inovace jsou i v současnosti velmi rozšířeným pojmem, který je skloňován v mnoha různých odvětvích či zapracováván do různých projektů. Pojem „inovace“ bezprostředně souvisí s prostředky informačních technologií (hardware a software) a byl charakterizován mnoha různými autory. Inovace jsou tedy výstupem komplexního (celopodnikového) systému managementu inovačních aktivit, přičemž důležitým aspektem jsou informace a znalosti (Grublová & Franek, 2014).

V souladu s nedávnými diskusemi zaměřenými na přehodnocení samotného zdůvodnění a relevance o konceptech Smart Cities vznikají nové směry výzkumu

interdisciplinárních aspektů a role znalostního managementu (Odusanya, 2019). Formováním teorie inovací ve veřejném sektoru v návaznosti na Smart Cities byl řešen i návrh nového rámce pro inovace pro podporu řízení informačních technologií (Misuraca & Viscusi, 2015).

Nedílnou součástí procesu zavádění inovací je i kreativita, která by však neměla být zaměňována za inovaci. Pod pojmem kreativita si lze představit vlastní nápad (myšlenku, ideu) jedince, která je přeměněna na hodnotu pro zákazníky, jež jsou ochotni za tu hodnotu zaplatit, a následně poté se z hodnoty stává inovace.

Kreativita je tedy jako pojem charakterizována jako generování nových myšlenek, hlubších porozumění nebo řešení, která jsou nová a užitečná pro danou situaci nebo problém (Goller & Bessant, 2017).

Města a obce investují nemalé finanční prostředky do inteligentních technologií založených na datech za účelem zvyšování poskytovaných služeb pro své občany, čímž dochází ke generování velkého množství dat, jež jsou sdílena prostřednictvím datových portálů. Hledání inovativních způsobů využití těchto dat napomáhá zlepšování řízení měst a obcí, kdy jsou hledána efektivní řešení pro optimalizaci interních procesů, funkcí, služeb, strategií a zásad (Radziszewska, 2023). Problém nastává v oblasti zavádění nových interních předpisů či bezpečnostních standardů, které souvisejí s moderními technologiemi, a to zejména v oblasti informačních technologií. Pro tyto moderní technologie, kdy je využíváno zejména prvků IoT ve spojení s informačními systémy (IS), umělou inteligencí a cloudovými službami, je omezující neexistence odpovídajících bezpečnostních standardů, které by mohly organizace využít ve svých strukturách. Problém však neznamenají pouze odborně zaměřené bezpečnostních standardy pro IoT v rámci jejich využití v dílčích částech koncepce Smart Cities, problém lze nalézt už v samotném prvotním procesu přípravy nových bezpečnostních standardů a také v rámci prvotního procesu přípravy nových právních předpisů. Problematika prvotní přípravy nových bezpečnostních standardů byla doposud řešena minimálně, avšak obdobným způsobem je poměrně významněji řešen proces pro prvotní přípravu nových právních předpisů. S ohledem na tuto skutečnost je práce zpracována v návaznosti na proces pro prvotní přípravu nových právních předpisů, přičemž tento proces lze aplikovat i na proces přípravy nových bezpečnostních standardů.

Proces prvotní přípravy nových právních předpisů však doposud není v České republice formalizován a samotná příprava zahrnuje vysokou náročnost na časové

vytížení personálních kapacit v organizacích, což má za následek zvýšení mzdových nákladů a ve výsledku celkovou neefektivitu procesu. V případě formalizování procesu pro prvotní přípravu nových právních předpisů a bezpečnostních standardů by mohly navrhované metody včetně jejich kombinace být do budoucna formalizovány a implementovány např. do organizačního řádu či jiných interních směrnic v organizacích.

Aktuálnost řešení této problematiky v souvislosti s IM a ZM v rámci koncepce Smart Cities dokládá i pandemie COVID-19, která zdůraznila potřebnost využívání IT v rámci zajišťování ochrany obyvatel a veřejného pořádku (Abdalla et al., 2023).

V současné době je tedy neméně důležitým prvkem i vzájemná koordinace měst, obcí a krajů při přípravě strategických dokumentů např. v rámci sdílení vytvořených bezpečnostních standardů pro IoT v oblasti krizového řízení při ochraně obyvatel a veřejného pořádku. Využívání moderních informačních technologií, jako jsou IoT a další Smart řešení, se stalo po období pandemie COVID-19 nejaktuálnějším tématem koncepce Smart Cities. Tyto technologie umožňují operativní získávání dat a informací o situaci ve městech pro rychlé zpracovávání a následné využití pro koordinaci bezpečnostních složek v rámci efektivního řešení krizových situací. Nedílnou součást podílející se na ochraně a bezpečnosti obyvatel, veřejného pořádku ve městech a obcích při vzájemné koordinaci s městy, obcemi a kraji tvoří bezpečnostní složky, které jsou součástí integrovaného záchranného systému České republiky (Špaček, 2009).

Integrovaný záchranný systém České republiky (IZS ČR) je tvořen třemi základními složkami – Policií České republiky (PČR), Hasičským záchranným sborem České republiky (HZS ČR), poskytovateli Zdravotnické záchranné služby České republiky (ZZS ČR) a jednotkami požární ochrany zařazenými do plošného pokrytí kraje jednotkami požární ochrany. Základní složky IZS ČR doplňují ostatní složky IZS ČR a poskytují pomoc při záchranných a likvidačních pracích na vyžádání. Ostatní složky IZS ČR jsou tvořeny vyčleněnými silami a prostředky ozbrojených sil, ostatními ozbrojenými bezpečnostními sbory, ostatními záchrannými sbory, orgány ochrany veřejného zdraví a dalšími službami (Špaček, 2009). Bezpečnost může být dále ve městě či obci rozšířena zřízením obecní policie. Problematikou bezpečnostních složek státu v souvislosti s koncepcí Smart Cities se zabývali i mnozí autoři.

Elizabeth E. John (2019) zpracovala esej, ve které se zaměřila na srovnání činnosti policie s moderními technologiemi. Ve svých úvahách se zaměřila na činnosti policie jako na soukromoprávní subjekt, kdy uvádí, že díky moderním technologiím

v chytrých městech bude policie začleněna do městské infrastruktury takovým způsobem, že nebude mít výsostné postavení. V souvislosti s novými senzory v rámci inteligentního řízení dopravy, kamerovými systémy a dalšími senzory se zamýšlí i nad problematikou omezování svobody a pohybu obyvatel. Obyvatelé tak jsou pod neustálým dohledem chytrých technologií a policie, čímž je zvýšena bezpečnost, avšak současně může docházet k omezování soukromí.

Přední místo zaujímá z hlediska bezpečnosti osob biometrická identifikace, která se zaměřuje na rozpoznávání obličeje, prstů a dalších informačních systémů (IS) umožňujících identifikaci osob (Khoumeri et al., 2018). Další možností, jak zvýšit bezpečnost obyvatel, je využití Light-Emitting Diode osvětlení a IoT senzorů, které mohou být spolu s kamerovými systémy (CCTV) implementovány v komplexní řešení tak, aby příslušníky bezpečnostních složek v reálném čase přes operační středisko upozorňovaly na možné anomálie a nahodilé situace (Vogiatzaki et al., 2020).

Tyto nové aplikace sice zlepšují kvalitu života v Smart Cities, avšak s ohledem na využívání prvků informačních technologií dochází k vysokému přenosu citlivých dat, která jsou shromažďována prostřednictvím IS sloužících pro chytré parkování, prohlížení míst prostřednictvím on-line streamů z kamer umístěných ve městech a jiných aplikací, čímž může docházet ke vzniku různých rizik v souvislosti s využíváním informačních technologií. Na základě těchto aspektů je nutné řešit ochranu těchto dat právě prostřednictvím odpovídajících bezpečnostních standardů tak, aby tato citlivá data byla vhodně zabezpečena v rámci provozovaných IS pro Smart Cities. Na svém významu nabývá i tzv. Crowdsourcing, který je využíván pro sběr dat v informačních systémech pro Smart Cities (Cilliers & Flowerday, 2014).

Na základě výše uvedeného je disertační práce profilována na oblast analýzy a návrhů vhodných metod pro přípravu nových právních předpisů s možností aplikace na proces přípravy nových bezpečnostních standardů pro IoT v rámci jejich využití v tematicky zaměřených částech koncepce Smart Cities v České republice. Řešení problematiky je situováno do oblasti kvalitativního výzkumu a současně je abstrahováno od konkrétních postupů a metod, přičemž jsou využity kombinace metod a jejich dílčích částí a prvků tak, jak kvalitativní výzkum připouští.

Disertační práce a návrh nových metod pro přípravu nových bezpečnostních standardů pro IoT v rámci jejich využití v tematicky zaměřených částech koncepce Smart Cities jsou tedy v návaznosti na odborné zaměření autorky zpracovány v kontextu ochrany obyvatel a veřejného pořádku ve městech, obcích a krajích

a z pohledu bezpečnostních složek, čímž práce současně přináší i další přínos do této problematiky, která je velmi aktuální v návaznosti na pandemii COVID-19.

Disertační práce je rozdělena do šesti kapitol včetně úvodu a závěru. V úvodní části jsou vymezena základní paradigmata, zaměření a zdůvodnění samotné práce. V první kapitole je popsán metodologický postup pro řešení práce včetně stanovení výzkumných otázek, v druhé kapitole jsou rozpracovány cíle a přínosy práce. Ve třetí kapitole je analyzován současný stav, přičemž je nejprve zpracována analýza strategických konceptů Smart Cities ČR, dále je zpracována rešeršní strategie zkoumaného problému na národní a mezinárodní úrovni a v poslední části této kapitoly jsou rozpracovány bezpečnostních standardy pro IoT s návazností na možnosti využití v koncepci Smart Cities. Ve třetí kapitole je popsán význam znalostního a informačního managementu a ekonomických věd v návaznosti na předchozí kapitoly a řešený problém. Ve čtvrté kapitole jsou představena základní východiska, rámcové pohledy a navrženy vhodné metody pro přípravu nových bezpečnostních standardů pro IoT. V závěru této kapitoly je provedena validace výstupů v rámci expertních skupin a rozpracováno zhodnocení řešeného problému a vlastních přínosů s důrazem na publikační činnost v rámci doktorského studia a též uvedeny další aspekty, s jejichž pomocí bude možné v budoucnu tuto problematiku v praxi rozvíjet.

Motivací a jedním z hlavních cílů práce je návrh vhodných metod či jejich kombinace pro zlepšení prvotního procesu přípravy nových bezpečnostních standardů pro IoT s využitím v tematických částech koncepce Smart Cities s možností uplatnění i v rámci zlepšení prvotního procesu přípravy nových právních předpisů pro formalizaci tohoto postupu ve formě interních směrnic.

Disertační práce obsahuje i cizí výrazy a anglické pojmy, které jsou mnohdy obtížně přeložitelné do českého jazyka. Tyto výrazy a pojmy jsou charakterizovány přímo v textu nebo jsou vysvětleny v seznamu zkratek a pojmů tak, aby čtenářům usnadnily čtení samotného textu.

1 METODOLOGICKÝ POSTUP

Disertační práce je zpracována metodou kvalitativního výzkumu. Kvalitativní výzkum se stal součástí běžného života odborníků, akademiků či dalších osob, které přicházejí v rámci pracovního procesu do styku s požadavky na různé analýzy textu, místní šetření či jiné výzkumné činnosti.

Kvalitativní výzkum interpretuje pohledy subjektů tak, že výzkumník přijímá jejich perspektivu a využívá podrobný popis každodenních situací. Tímto způsobem dochází k porozumění akcím a významům v jejich sociálně-pracovním kontextu s důrazem na přesnost otevřených a nestrukturovaných výzkumných plánů. Dochází tak k redukci počtu proměnných vztahů mezi nimi na základě kombinace metod indukce, dedukce a analýzy. V rámci kvalitativního výzkumu tedy převažují zájem o reálné celky, interakce mezi aktéry a individuálními osudy a současně je kvalitativní výzkum zaměřen na pochopení a interpretaci hlubších významů a kontextů lidského chování, zkušeností a sociálních interakcí. Proces kvalitativního výzkumu je tedy založen na induktivní logice, kdy na začátku výzkumného procesu probíhají pozorování, analýza a další zkoumání jevů s následným vyhodnocováním aktuálního stavu za pomoci dalšího odpovídajícího sběru dat v reálném prostředí za využití metod kvalitativního výzkumu.

Zkoumaná problematika zaměřená na prvotní proces přípravy nových bezpečnostních standardů a nových právních předpisů tak úzce souvisí právě s kvalitativním výzkumem zejména v rámci základního principu indukce a využívaných metod pro kvalitativní výzkum (obsahová analýza, hodnotová analýza, brainstorming, Delphi metoda aj.). Problematiku zaměřenou na zlepšení prvotní části procesu přípravy nových bezpečnostních standardů pro IoT s využitím v tematicky zaměřených částech koncepce Smart Cities bylo nutné zkoumat tak, aby problém byl pochopen do hloubky se všemi souvislostmi. Cílem bylo získání dalších poznatků na základě reálného stavu tak, aby byl umožněn nový pohled na řešený problém a metody bylo možné využít v praxi včetně dalšího budoucího rozvoje.

Metodologický postup řešení disertační práce byl tedy navržen pro řešení v oblasti kvalitativního výzkumu. Při zpracovávání této práce byla s ohledem na zpracovávaný problém využívána kombinace metod a dílčích prvků z více analytických metod bez aplikace konkrétních přesných metod podle jejich přesné metodologie tak, jak je to povoleno v kvalitativním výzkumu.

Metodologický postup byl rozdělen do dílčích částí:

Stanovení účelu a cílů výzkumu – v rámci řešené problematiky byl definován hlavní účel a byly definovány cíle výzkumu. Hlavním cílem disertační práce je analýza a návrh metod z oblastí pro zpracování nových bezpečnostních standardů pro využití v tematicky zaměřených dílčích částech koncepce Smart Cities.

Určení konceptuálního rámce – v této části byl stanoven celkový konceptuální rámec pro řešenou problematiku, na jehož základě byly analyzovány dílčí procesy a další faktory ovlivňující přípravu nových právních předpisů a bezpečnostních standardů.

Analýza současného stavu – v této části byl analyzován stav řešeného problému na národní a mezinárodní úrovni (články, studia, projekty aj.), dále byly analyzovány strategické koncepty Smart Cities v ČR, bezpečnostní standardy pro IoT a taktéž byl zjišťován skutečný stav řešeného problému u stanovených organizací – Krajský úřad Pardubického kraje, Národní úřad pro informační a kybernetickou bezpečnost, Ministerstvo vnitra České republiky, Císař, Čéška, Smutný s. r. o. (soukromá advokátní kancelář).

Stanovení výzkumných otázek – na základě analýzy současného stavu a určení konceptuálního rámce byly vhodně sestaveny výzkumné otázky, které byly současně stanoveny v návaznosti na zkoumanou problematiku a vztahy mezi souvisejícími proměnnými.

V kvalitativním výzkumu jsou výzkumné otázky stanovovány v rámci indukce. Indukce je proces usuzování, při kterém výzkumník vyvozuje obecný závěr, který získal díky dílčím poznatkům. Indukce vychází z poznatku, že představitelé (instance) dané jevové kategorie se vyznačují jistou vlastností. Z toho lze vyvodit, že tuto vlastnost budou mít také její další instance. Jinými slovy, z pravidelnosti zkoumaných událostí je odvozeno obecné pravidlo o určité pravidelnosti, jež je platné pro další události na jiném místě nebo v jiném čase (Hendl, 2016).

Indukce je tedy metoda, která slouží pro zkoumání jednotlivých událostí (faktů), na základě kterých dochází k vyvozování všeobecně platných závěrů. Metoda indukce je základem pro výstavbu induktivní stavěné teorie s cílem popsat význam získaných informací. Proces indukce zahrnuje dílčí části: definice předmětů zkoumání, stanovení výzkumných cílů, určení množiny zkoumaných jevů a implikaci závěru založeného na principu opatrnosti (Zháněl et al., 2014).

Anglický filozof a ekonom John Stuart Mill (1806–1873) navrhl systém induktivních pravidel získávání a ověřování teorií, která jsou známá jako Millova pravidla (Hendl, 2005):

- Metoda souhlasu – pokud dva případy fenoménu mají jenom jednu vlastnost společnou, pak tato vlastnost je jejich příčinou nebo důsledkem.
- Metoda rozdílu – jestliže existuje případ, v němž se objeví daný fenomén, a případ, v němž se neobjeví, a oba případy se liší v jedné charakteristice, pak tato charakteristika je příčinou nebo nutnou částí příčiny uvažovaného fenoménu.
- Metoda společné shody a rozdílů. Tato metoda spojuje obě předchozí metody.
- Metoda zbytků – pokud se oddělí od fenoménu to, co je známé jako důsledek určitých předchozích událostí, pak zbytek je důsledkem zbývajících příčin.
- Metoda společné variace – fenomény, které se souběžně mění, jsou propojeny nějakou příčinou.

Výzkumné otázky byly stanoveny na základě přístupu zakotvené teorie, kdy formulace výzkumných otázek vychází z určitého problému, který je řešen. Výzkumné otázky jsou pak formulovány v širším kontextu s ohledem na řešený problém (Hendl, 2005). Každá výzkumná otázka je doprovázena svým zdůvodněním na základě zakotvené teorie, jež je základním přístupem v kvalitativním výzkumu.

Výzkumné otázky (VO) byly formulovány:

VO1: Mohou zvolené metody z oblasti informačního a znalostního managementu a metody pro zkoumání textu inovovat neformalizovaný proces přípravy nových právních předpisů a nových bezpečnostních standardů?

VO2: Může využití kvalitativní obsahové analýzy s vhodným softwarem zkrátit potřebnou dobu pro přípravu nových právních předpisů a bezpečnostních standardů?

VO3: Jsou navržené metody IT Governance (informační management), SECI (znalostní management) a využití kvalitativní obsahové analýzy v souladu s principem 3E?

VO4: Bude zefektivnění prvotního procesu přípravy nových právních předpisů a bezpečnostních standardů přínosné pro další uplatnění v praxi při formalizování procesu přípravy nových právních předpisů?

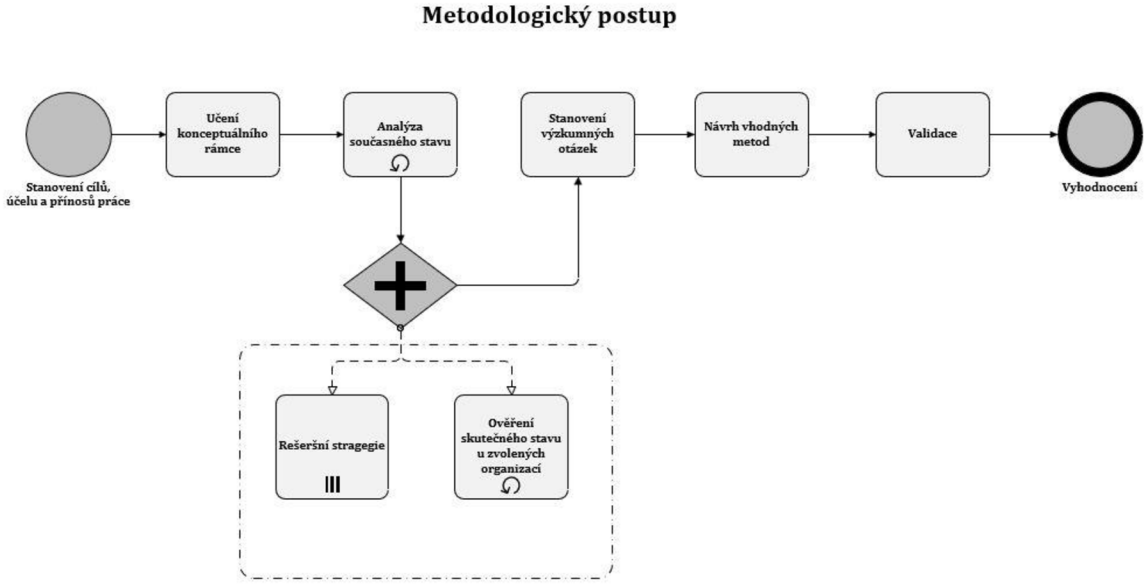
Návrh vhodných metod – v rámci této etapy byly navrženy metody, jejichž návrh byl proveden na základě analýzy a ověření současného stavu u vhodných organizací.

Validace v rámci expertní skupiny – v rámci této etapy byla provedena validace návrhu vhodných metod a jejich kombinace u vhodných organizací, jež jsou uvedeny

výše. Validace byla provedena na základě stanoveného postupu a kritérií aplikovaných v kvalitativním výzkumu.

Vyhodnocení – v rámci této etapy bylo provedeno vyhodnocení řešeného problému, přínosů a dále byly rozpracovány možné aspekty pro budoucí vývoj či využití v praxi.

Komplexní metodologický postup byl pro názornost zpracován prostřednictvím modelu BPMN a je zobrazen na obrázku 1.



Model BPMN 1 Metodologický postup

Zdroj: Vlastní zpracování

V rámci celé této práce je dále pro zjednodušení celého textu a z hlediska opakovatelnosti stanovených cílů práce a řešeného problému uváděna řešená oblast zkráceně ve smyslu návrhu nových metod pro přípravu nových bezpečnostních standardů a nových právních předpisů namísto zlepšení prvotního procesu přípravy nových bezpečnostních standardů pro IoT v rámci jejich využití v tematicky zaměřených částech koncepce Smart Cities. Dále je řešený problém v celé práci rozpracován zejména v návaznosti na prvotní proces přípravy nových právních předpisů, protože prvotní proces přípravy nových bezpečnostních standardů byl doposud řešen minimálně. Prvotní proces přípravy nových právních předpisů lze aplikovat i na prvotní proces přípravy nových bezpečnostních standardů, poněvadž procesy přípravy obou forem jsou totožné, a tedy i navržené vhodné metody či jejich kombinace lze aplikovat pro obě formy prvotního procesu přípravy.

V celé práci byly využity metody:

- Metody empirické – pozorování, srovnání, analýza, rozhovor, písemné dotazování.
- Metody logické – analýza, syntéza, indukce, dedukce, abstrakce, konkretizace, generalizace, analogie.

Disertační práce je současně zpracována i takovým způsobem, aby zjištěné a ověřené cíle splňovaly podmínky definice výzkumu podle Frascati manuálu. Výzkum a experimentální vývoj byly definovány jako systematická práce vykonávaná za účelem zvýšení úrovně vědomostí a znalostí lidstva, kultury a společnosti s cílem návrhů nových způsobů aplikace dostupných znalostí (OECD, 2015).

Pro splnění podmínky výzkumné činnosti je nutné splnění pěti základních kritérií: prvku novosti, prvku kreativity, prvku nejistoty, prvku systematičnosti a prvku reprodukovatelnosti a převoditelnosti. Základním prvkem výzkumu musí být nový koncept nebo nápad, jenž zlepšuje současnou znalost.

Prvek nejistoty lze nalézt v rámci dalšího rozvoje výzkumu z hlediska praktické spolupráce s organizacemi podílejícími se na přípravě nových právních předpisů a bezpečnostních standardů, kdy není zcela zřejmé, jakým směrem bude další rozvoj probíhat a jakých výstupů bude dosaženo. Organizací podílejících se na přípravě nových právních předpisů a bezpečnostních standardů je více a každá organizace může výstupy z této disertační práce rozvíjet na základě vlastního uvážení bez jakýchkoliv omezení.

Prvek nejistoty je splněn především v tom, že není zřejmé, zdali dalším rozvojem bude výstup v podobě nového speciálního softwaru, případně zda výstup z této disertační práce v podobě návrhu metody bude rozšířen o prvky umělé inteligence či zdali budou začleněny další prvky z dalších oblastí.

Prvek novosti lze v rámci řešeného tématu disertační práce spatřovat především v návrhu a ověření optimalizace metod a procesů pro prvotní přípravu nových právních norem a bezpečnostních standardů v oblastech informačního a znalostního managementu. Současný proces pro přípravu nových právních předpisů a bezpečnostních standardů je založen pouze na ruční lidské činnosti (práci) s využitím standardního kancelářského softwaru MS Office, čímž je celkové zpracování z časového a finančního hlediska velmi náročné a zdlouhavé. Prvek novosti tedy zavádí prokazatelně nový koncept či návrh, který zlepšuje současný stav.

Prvek kreativity je splněn, pokud se jedná o rutinní činnosti, které jsou běžně využívány, avšak pokud nové metody zlepšují rutinní činnost, je podmínka prvku kreativity splněna. V rámci řešeného problému je prvek kreativity splněn, poněvadž rutinní činností při přípravě nových právních předpisů a bezpečnostních standardů je využívání standardního kancelářského softwaru MS Office, kdy je prvotní příprava řešena bez automatizovaných procesů či odpovídajících inovativních metod, které by zefektivňovaly z hlediska informačního a znalostního managementu celkový proces prvotní přípravy.

Prvek systematičnosti neboli systematické plánování je obsažen v rámci plánovaných činností, které povedou k návrhu a ověření stanovených výzkumných otázek v rámci této disertační práce. Účel systematičnosti a zlepšení v podobě návrhů a ověření inovace sníží administrativní zátěž při přípravě nových právních předpisů a nových bezpečnostních standardů a současně systematicky rozšíří v podobě inovací stávající postup včetně možnosti snížení nákladů na rozpočet organizace.

Prvek reprodukovatelnosti a převoditelnosti je zahrnut v rámci dalších činností, které do budoucna mohou být rozšířeny ze stran různých organizací, jež se podílejí na přípravě nových právních předpisů a nových bezpečnostních standardů. Navržené a ověřené metody v rámci této disertační práce budou volně dostupné, převoditelné a reprodukovatelné bez omezení pro možnost dalšího využití dle potřeb konkrétních organizací.

2 CÍLE DISERTAČNÍ PRÁCE

V aktuálním dynamickém prostředí městského a obecního rozvoje představuje koncept Smart Cities důležitý prvek proměny urbanistických částí. Postupná integrace pokročilých technologií a inovativních řešení přináší především zlepšení nabízených služeb ze strany měst, obcí a krajů, ale i významné zlepšení kvality života obyvatel. Nosným prvkem pro integraci těchto inovací je využívání IoT. Tyto senzory umožňují rozsáhlý sběr a analýzu dat v reálném čase, čímž dochází k efektivnímu rozvoji a řízení městských zdrojů např. v případě dopravní obslužnosti, odpadového hospodářství, bezpečnosti veřejného prostranství. Nicméně s rostoucí závislostí na těchto technologiích dochází ke zvyšování bezpečnostních opatření, která je nutné implementovat v rámci ochrany informační infrastruktury před kybernetickými útoky.

Postupná implementace konceptu Smart Cities vyžaduje nejen technologické inovace, ale i důkladnou legislativní a normativní podporu prostřednictvím právních předpisů a bezpečnostních standardů. Proces přípravy nových právních předpisů a bezpečnostních standardů se stává náročným procesem, poněvadž bezpečnostní standardy by měly být přizpůsobeny v rámci dílčích odvětví (sektorů), aby byly přímo aplikovatelné a nebyly pouze obecnými doporučeními, jež by bylo nutné opětovně modifikovat ze strany organizací.

S ohledem na stále se zrychlující vývoj v oblasti informačních technologií je tento proces často náročný a vyžaduje specializované znalosti, nástroje, procesy a metody a vysoké časové nároky na vypracování, což vede ke zvýšenému časovému zatížení personálních kapacit a specializovaných odborníků. Pro správné pochopení a implementaci technologických aspektů v legislativním rámci je důležité, aby příprava bezpečnostních standardů a nových právních předpisů probíhala efektivně s pomocí vhodných procesů a metod a s využitím profesionálního softwarového nástroje, aby se celkový proces prvotní přípravy zjednodušil a snížil celkové zatížení personálních kapacit z hlediska časové a finanční náročnosti.

Hlavním cílem disertační práce je analýza a návrh metod z oblastí pro zpracování nových bezpečnostních standardů pro využití v tematicky zaměřených dílčích částech koncepce Smart Cities. Naplnění hlavního cíle vyžaduje splnění dílčích cílů, které formují obsah a strukturu práce a současně nastiňují možné otázky pro další rozšiřující výzkum pro praktické využití zejména v sektoru státní správy v rámci společné spolupráce.

Dílčí cíle:

- Analýza existujících strategických dokumentů pro Smart Cities v ČR.
- Analýza současného stavu využívaných metod pro zpracovávání bezpečnostních standardů a právních předpisů v ČR i zahraniční, zjištění skutečného stavu ve zvolených organizacích.
- Analýza existujících bezpečnostních standardů a jejich využití v tematicky zaměřených částech koncepce Smart Cities v kontextu využívání moderních technologií.
- Stanovení výzkumných otázek na základě provedené analýzy současného stavu řešeného problému.
- Návrh vhodných metod pro přípravu nových bezpečnostních standardů a nových právních předpisů. Určení relevantních vztahů a propojení s ostatními souvisejícími aspekty a procesy.
- Validace navržených metod v rámci expertní skupiny, zhodnocení vlastních přínosů včetně využitelnosti v praxi.

Hlavním přínosem navržených metod a jejich kombinace je zejména možnost využití pro vytváření nových bezpečnostních standardů v tematicky zaměřených částech koncepce Smart Cities s možností využití při přípravě nových právních předpisů a interních předpisů v organizacích. Hlavní přínos současně doplňují vedlejší přínosy, kdy celý proces prvotní přípravy může být do budoucna dále rozvíjen odpovídajícími organizacemi za účelem formalizování celého postupu procesu přípravy a integrace např. do organizačních řádů.

Cílem této práce však není návrh nových bezpečnostních standardů pro IoT v rámci jejich využití v návaznosti na koncepci Smart Cities. Z hlediska náročnosti, celkového rozsahu a hlavně dodržení disertability není cílem práce ani návrh nových bezpečnostních standardů pro IoT v rámci jejich využití v jiných oblastech. Vytvoření bezpečnostních standardů by bylo velmi obtížné a náročné z hlediska různorodosti využívání IoT senzorů v různých odvětvích a organizacích, ve kterých jsou současně implementovány různé frameworky z oblasti informační bezpečnosti, a mohou být zpracovávány i utajované informace dle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Dílčí zařazení řešeného problému do aplikovaného výzkumu, průmyslového výzkumu nebo experimentálního vývoje není v disertační práci podrobně rozvedeno, protože rozdělení do konkrétního typu výzkumu se využívá u VaVal projektů, a pro tuto disertační práci je tedy určení přesného typu výzkumu nerelevantní. Relevantní je

pouze dodržení podmínky pro vědecko-výzkumnou činnost, tedy disertabilitu, aby byly splněny parametry stanovené pro zpracování disertační práce.

3 ŘÍZENÍ ZNALOSTÍ A INFORMACÍ V ORGANIZACÍCH PŘI PŘÍPRAVĚ BEZPEČNOSTNÍCH STANDARDŮ

V této kapitole je rozpracován význam a role informačního managementu při řízení znalostí a informací v organizacích v návaznosti na studijní program, řešenou problematiku prvotního procesu přípravy nových bezpečnostních standardů a nových právních předpisů.

Informační management byl charakterizován mnoha definicemi, např. jako *„soubor činností a procesů sloužící ke sběru, správě a uchovávání informací z jednoho nebo více zdrojů za účelem následné distribuce těchto znalostí koncovému uživateli nebo skupině uživatelů“* (Matula, 2017).

Dále byl definován jako transdisciplinární soubor poznatků, metod a doporučení systémových přístupů a informatiky, které pomáhají účelově realizovat informační procesy manažerského myšlení a jednání k dosažení podnikatelských cílů organizace (Vymětal et al., 2005).

Návaznost k dalším vědám je možné nalézt i v ekonomických vědách v kontextu podnikatelské výkonnosti v rámci vlivu na konkurenceschopnost podniku při zavádění inovací. Další vztah představuje procesní hledisko, kdy jsou v organizacích implementovány různé postupy, jež zajišťují efektivní výměnu procesů v rámci v rámci životního cyklu.

Významný rozvoj přinesla 2. polovina 20. století, kdy byl zaveden pojem „framework“ (doporučení), který je chápán jako systém pravidel, nápadů a přesvědčení, jež jsou využívány pro plánování nebo pro rozhodování při řešení konkrétních problémů. Framework může obsahovat podpůrné programy, knihovny, návrhové vzory či doporučené postupy, přičemž hlavním cílem je převedení typických problémů v dané oblasti tak, aby problém byl vyřešen odpovídajícím a efektivním způsobem (Matula, 2017). V 90. letech 20. století byl informační management konceptualizován z perspektivy procesního řízení v tom smyslu, že by měl obsahovat všechny etapy informačního procesu v organizacích. Vnímání současného IM charakterizují činnosti, kdy je nutné dělat věci správně a hospodárně (Effectiveness and Efficiency).

Role informačního managementu spočívá především v činnostech, jako jsou organizování, vyhledávání, získávání, zajištění a udržení informací v organizacích,

přičemž úzce souvisí i s řízením interních procesů v organizacích při správě dat (Dolák, 2018).

Základním koncepčním dokumentem je informační strategie, která navazuje na globální strategii organizace. Globální strategie vymezuje celkový koncept úspěšného fungování organizace a současně navazuje na další strategické a interní dokumenty organizace (Matula, 2017). Informační strategie by měla být vhodně doplněna o prvky informační politiky, na jejichž základě dochází k řízení určité oblasti, formulaci cílů, výběru vhodných metod a prostředků pro dosažení stanovených cílů. Strategie tedy představuje plánovanou činnost, která směřuje k dosažení stanovených cílů a systematicky vychází z informační politiky organizace (Lukáš et al., 2008).

Pro nastavení vhodné informační strategie bývá obvykle důležité, aby organizace měla vhodně nastavenou organizační strukturu. Organizace má mnoho definic a podob, kdy smyslem jejího fungování je realizace činností pro dosažení stanovených cílů. Pro správné fungování činností je v managementu zaveden pojem organizování, jehož smyslem je uspořádání prvků (sekcí, odborů, oddělení) v systému takovým způsobem, aby jejich aktivity byly efektivně koordinovány a kontrolovány tak, aby s maximální mírou bylo dosahováno stanovených cílů (Vymětal et al., 2005). Organizační struktura organizace je založena na rozdělení kompetencí, pravomocí, odpovědnosti a odborně ji lze definovat jako formální systém pravidel, úkolů a mocenských vztahů, který řídí spolupráci a užití zdrojů pro dosažení cílů podniků (Střížová, 2007). Jednotná klasifikace organizačních struktur však doposud neexistuje a v organizacích je dána schválenou organizační strukturou ze strany manažerského vedení dané organizace. Pro efektivní řízení a dosahování stanovených cílů v souvislosti s informačními technologiemi v organizacích je důležité mít vhodně implementovány odpovídající metody.

V rámci IM je však zavedeno mnoho metod, které jsou využívány v různých organizacích. Výběr vhodné metody tak závisí na konkrétních požadavcích a stanovených cílech, pro které má být metoda určena. V kontextu současné doby čtvrté průmyslové revoluce označované jako Průmysl 4.0 (anglicky *Industry 4*.0) se svět kolem nás neustále mění a rozvíjí rychlostí, která byla ještě před několika desetiletími nepředstavitelná. V tomto rychle se rozvíjejícím světě nabývá stále na větším významu znalostní management (anglicky *Knowledge Management*), který se jeví jako klíčový prvek pro udržení konkurenceschopnosti a inovativnosti organizací. Význam a role

znalostního managementu jsou veřejně diskutovány v akademické sféře, mezi experty a dalšími odborníky z praxe.

Znalostní management lze charakterizovat jako disciplínu, která se zabývá systematickým a organizovaným přístupem k zachycení, rozvoji, sdílení a využívání znalostí a zkušeností v rámci organizace s cílem zlepšení výkonnosti, inovativnosti a schopnosti adaptace na změny. Tento přístup zahrnuje nejen technické aspekty, jako je správa databází a informačních systémů, ale také sociální a kulturní faktory, které ovlivňují sdílení a využívání znalostí (Pitra & Mohelská, 2015).

Znalostní management zahrnuje aktivní a systémový přístup ke znalostem, kdy je při implementaci tohoto vědního oboru vyžadována nejen tvorba znalostí v dané formě a struktuře, ale důležitým aspektem je i reálný a včasný přenos nových znalostí do realizační fáze (praxe). Bývá obvykle spojován s ekonomickými vědami, protože v rámci ekonomických věd jsou aplikovány v organizacích různé metody pro zavádění inovací a inovace nelze zavádět bez potřebných a nových znalostí. Pro zavádění ZM bývá využíván systémový přístup, někdy nazývaný jako systémové myšlení, který přispívá ke sjednocování znalostí z různých vědních disciplín (Častorál, 2008). Důležitým aspektem je znalost, která je transformována do využitelné podoby v rámci učící se organizace, kdy postupným učením nastává adaptace na nové znalosti, změny a inovace v organizacích.

Klíčové aspekty znalostního managementu zahrnují identifikaci, zachycení, hodnocení, sdílení, využívání a uchovávání znalostí. Tyto aspekty pomáhají organizacím nejen udržet si konkurenční výhodu, ale také se přizpůsobit novým tržním trendům a technologickým inovacím. Význam znalostního managementu pramení z jeho schopnosti transformovat individuální znalosti na institucionální znalosti, které jsou přístupné a využitelné pro celou organizaci.

V zahraniční literatuře je znalostní management definován různými autory, přičemž každá definice reflektuje odlišné perspektivy a aspekty disciplíny. Například Davenport a Prušák (1998) popisují znalostní management jako proces zachycování, distribuce a efektivního využívání znalostí. Nonaka a Takeuchi (1995) zdůrazňují důležitost transformace tichých znalostí znalostí (tj.osobních, obtížně sdělitelných znalostí) na explicitní znalosti.

Řízení znalostí a informačních technologií je řešeno v různých organizacích tak, aby zavádění inovací a využívání informačních technologií bylo vhodně koordinováno a interní procesy byly vhodným způsobem vytvářeny a aktualizovány.

Využívání metod z oblastí znalostního a informačního managementu lze nalézt i u bezpečnostních složek státu a vládních organizací. Vztah mezi výkonem a vzděláním u policie byl řešen v rámci studie ve Virginii u 12 městských policejních oddělení za účelem zjištění úrovně komunikačních dovedností, dovedností v oblasti vztahů s veřejností, schopnosti rozhodovat (Smith & Aamodt, 1997). Další studie byla zaměřena na měření vynaložených nákladů souvisejících s výkonem služby v kontextu vynaložených výdajů na míru kriminality ve městech a konkrétně tedy byla měřena obousměrná vazba vztahů mezi policií a kriminalitou (Swimmer, 1974).

Navrhované metody z oblastí znalostního a informačního managementu jsou využívány i v rámci jiných interních procesů při řízení policie a výkonu služby, například v rámci studie, která byla zpracována ve Velké Británii, kdy u policie bylo zkoumáno porozumění managementu znalostí a sdílení znalostí ve veřejném sektoru prostřednictvím případových studií na základě šetření politik a strategií managementu znalostí a procesů sdílení znalostí ve čtyřech policejních složkách (Seba & Rowley, 2010). Dále byla implementace principů a postupů založených na znalostním informačním managementu zkoumána v kontextu využívání informačních technologií u policie a celkovém procesu organizace práce (Manning, 1992).

Policejní profese se vyznačuje i širokou škálou požadovaných typů znalostí a časovým tlakem, pod kterým musejí policisté často jednat a využívat různé typy znalostí (Emil Berg et al., 2008). Na základě toho je důležité aktivní vedení policejních manažerů při podpoře sdílení nových znalostí. Při zavádění a sdílení nových znalostí mezi policisty jsou tyto znalosti využívány i při vymáhání práva (*Knowledge Management in Law Enforcement: Knowledge Views for Patrolling Police Officers - Stefan Holgersson, Petter Gottschalk, Geoff Dean, 2008*, b.r.).

V rámci další studie bylo testováno sdílení informací mezi orgány činnými v trestním řízení v rámci dokazování, přičemž byly testovány dva přístupy pro sdílení informací, a to přístup pro kvalitu dat a přístup pro ochranu soukromí (Plecas et al., 2011). Nejdůležitější inovace však zahrnují počítače a související software, jehož prostřednictvím jsou získávány, zpracovávány a kódovány získané informace k výkonu policejních činností. Zvýšený důraz je kladen na přístup k informacím o policejních problémech a výkonu policejních sil a na zákonné změny tak, aby rozvoj sdílených výsledků a cílů byl v případě potřeby sdílený a srozumitelný.

Na základě výše uvedených informací ze zahraničních periodik lze konstatovat, že informační a znalostní management a jeho metody jsou využívány u policie

a současně i v kontextu práva. V České republice mohou být metody z oblasti informačního a znalostního managementu implementovány např. v rámci krajských ředitelství Policie ČR a dále na celostátních útvarech PČR či v jiných bezpečnostních složkách. Navrhované metody mohou být současně přínosem i pro oblast bezpečnostních složek v České republice při zavádění procesu řízení znalostí a správě informačních technologií.

Další oblastí, ve které jsou metody z oblasti znalostního a informačního managementu využívány, jsou vládní organizace (Government). Rozvoj znalostního managementu byl v posledních desetiletích implementován i do vládních organizací (Buheji et al., 2014), na základě čehož byl definován v Indii vládní rámec pro vytvoření a udržení iniciativy řízení znalostí ve vládních organizacích (Misra et al., 2003). Vládní organizace však v rámci implementace metod z oblastí znalostního a informačního managementu zaostávají, i přestože si to vedoucí představitelé státních organizací uvědomují (Liebowitz, 2004). Klíčovými prvky pro oblast strategického řízení znalostí v rámci vládních organizací či samospráv (místní, krajské) jsou interní znalostní strategie a procesy strategického řízení (Laihonen & Mäntylä, 2018). Současně vzrůstá i počet požadavků na řízení interních procesů spojených s informačními technologiemi v organizacích (Butler et al., 2008).

Na základě ověření skutečného stavu u vládních organizací bylo zjištěno, že metody z oblasti znalostního a informačního managementu nejsou v organizacích zavedeny v rámci optimalizace jiných interních procesů a současně nejsou tyto metody využívány ani v souvislosti s řešeným problémem.

Interní procesy ve vládních organizacích jsou řízeny především neefektivním způsobem, což má za následek vyšší pracovní zatížení pracovníků, vyšší náklady, delší čekací lhůty pro vyřízení požadavků aj. Tento problém lze tedy nalézt v rámci různých interních procesů u vládních organizací či bezpečnostních složek. Proces řízení znalostí a informačních technologií ve vládních organizacích by měl být vhodně integrován, nejlépe v rámci celé hierarchické struktury dané organizace.

Disertační práce se zaměřuje na užší řešení problematiky u vládních organizací v souvislosti s procesem prvotní přípravy nových bezpečnostních standardů a nových právních předpisů ve formě návrhu a ověření vhodných metod. Současně však může řešit i problém v širším měřítku u vládních organizací či bezpečnostních složek v souvislosti se zaváděním inovací do interních procesů dané organizace. Navržené metody mohou být využity i pro optimalizaci jiných interních procesů (podrobněji

kapitola 5.5 validace výsledků v rámci expertních skupin). Oblast znalostního a informačního managementu a odpovídající metody jsou tedy primární oblastí, na jejímž základě bylo nutné řešit definovaný problém (výzkumné otázky) včetně všech souvislostí (optimalizace jiných interních procesů organizace), které byly zjištěny při ověřování skutečného stavu.

Řešený problém a stanovené cíle včetně výzkumných otázek však není možné řešit bez metod náležejících do oblastí informačního a znalostního managementu včetně odpovídajícího vzdělání v této oblasti. Kvalifikovaní odborníci bez vhodného vzdělání z uvedených oblastí nemohou vhodně navrhnout a implementovat metody z uvedených vědních disciplín. Navrhované metody a současně využití v praxi mohou řešit kvalifikovaní odborníci, kteří mají odpovídající vzdělání v oblastech znalostního a informačního managementu. Tento problém by nebylo možné řešit v souvislosti s jiným vzděláním či v jiném studovaném oboru, poněvadž oblast znalostního a informačního managementu je spojena s dalšími vědami, které souvisejí i s manažerským řízením v organizacích. Manažerské řízení v organizacích současně zahrnuje proces řízení znalostí a řízení informačních technologií na základě vhodných metod tak, aby procesy v organizacích byly řízeny efektivně, inovativně a s minimálními náklady na provoz organizace. Ve vládních organizacích obecně či v souvislosti s řešeným problémem je však oblast znalostního a informačního managementu řešena minimálně či vůbec. Tato práce tak vhodně a efektivně inovuje interní procesy v podobě nových metod z oblastí informačního a znalostního managementu u uvedených organizací s možností využití i v jiných organizacích.

4 ANALÝZA SOUČASNÉHO STAVU

V této kapitole je analyzován současný stav řešeného problému v návaznosti na stanovený cíl a dílčí cíle uvedené v kapitole 2 a dále v návaznosti na stanovený metodologický postup rozpracovaný v kapitole 1.

Nejprve byly analyzovány platné strategické dokumenty zaměřené na Smart Cities v ČR, dále byly analyzovány využívané metody pro zpracovávání stávajících a nových bezpečnostních standardů a právních předpisů. Současně byly analyzovány existující bezpečnostní standardy pro IoT v návaznosti na využívané informační technologie v koncepci Smart Cities.

4.1 Strategické koncepty Smart Cities v ČR

Období celosvětové pandemie COVID-19 v letech 2020 a 2021 bylo spojeno s rozvojem Smart technologií pro zajišťování bezpečnosti občanů v obcích, městech a krajích. Do podvědomí vstoupily především problematika internetu věcí (IoT) a velký rozvoj v oblasti kybernetické bezpečnosti po celém světě.

Rozvoj koncepce Smart Cities spolu s rozšiřováním kybernetické bezpečnosti je také jedním z cílů Inovační strategie České republiky 2019–2030, kterou zpracovala Rada pro výzkum, vývoj a inovace v roce 2019 (Jirotková et al., 2019).

Inovační strategie zahrnuje devět základních pilířů, které se navzájem doplňují v oblasti digitalizace, bezpečnosti, kybernetické bezpečnosti, veřejné správy a Smart technologií. Ve svých dílčích částech systematicky poukazuje na postupy spojené s ochranou obyvatel, v nichž figuruje vzájemná koordinace krajských samospráv a bezpečnostních složek s důrazem na kybernetickou bezpečnost a Smart technologie (Jirotková et al., 2019).

Vláda České republiky nechala v roce 2020 zpracovat rozsáhlou studii, která analyzovala stávající stav implementace koncepce Smart Cities u krajů, měst a obcí. Výstupem provedené studie byl návrh doporučení pro implementaci v souvislosti s novými trendy (Grega et al., 2018). Výsledné doporučení bylo zahrnuto i do Národní RIS3 strategie ČR (NRIS3), která je současně hlavním strategickým dokumentem pro zajišťování efektivního zacílení evropských, národních a regionálních aktivit vedoucích k posílení a rozvoji inovací v rámci krajů (Kolektiv autorů, 2019).

Národní RIS3 strategie ČR je strategickým dokumentem zajišťujícím efektivní zacílení evropských, národních, regionálních a soukromých prostředků na aktivity vedoucí k posílení výzkumných inovačních kapacit, a to do prioritně vytyčených perspektivních oblastí na národní i krajské úrovni.

V roce 2021 byla vládou ČR schválena nová koncepce Smart Cities – odolnost prostřednictvím Smart řešení pro obce, města a regiony (Nencková & Bízková, 2021). Tato nová koncepce byla rozšířena o problematiku zaměřenou na spolupráci krajů a složek IZS ČR při ochraně obyvatelstva ve Smart Cities. Tato část je součástí 3. pilíře a je tvořena čtvrtou částí s názvem Komponenta A4 Rychlá reakce – integrovaný přístup k odolnosti. Obsahem této části je vyšší důraz na implementaci a rozšiřování cílů ochrany bezpečnosti obyvatel, součinnost krajů a složek IZS ČR a bezpečnostních složek s využíváním IT, IoT a dalších Smart řešení. V komponentě A4 Rychlé reakce – integrovaný přístup k odolnosti bylo stanoveno pět základních cílů, které jsou vyobrazeny v tabulce 1.

Tabulka 1 Rychlá reakce – Integrovaný přístup k odolnosti, 4. část 1. pilíře

Rychlá reakce – Integrovaný přístup k odolnosti	
Cíle	• Rozvíjení integrované bezpečnosti na vertikální a horizontální úrovni. • Příprava měst a obcí v podobě reakcí na extrémní meteorologické jevy. • Systematická, efektivní integrace pro sdílení a vytěžování dat mezi obcemi, městy, kraji při testování inovativních bezpečnostních technologií a přístupů. • Koordinace městských, obecních a krajských úřadů s odpovědnými úřady pro snižování rizik při narušení prvků kritické infrastruktury. • Technické vybavení měst, obcí a krajů pro zvládání katastrof antropogenního a přírodního původu včetně dalších nahodilých událostí velkých dopadů.

Zdroj: Nencková, Bízková, 2021, vlastní přepracování

Tyto základní cíle komponenty A4 Rychlá reakce byly rozpracovány do 5 dílčích částí a jednotlivých typových opatření určených pro implementaci.

1. Rozvíjení integrované bezpečnosti na vertikální a horizontální úrovni

- Zpracování manuálu (metodiky) pro zahrnutí kritéria bezpečnosti do všech činností měst, obcí a krajů.
- Zavedení systému bezpečnostního situačního managementu.
- Koncepční testování inovativních bezpečnostních technologií.
- Nasazování pokročilých analytických nástrojů pro vytěžování dat.
- Komplexní rozvoj metropolitních dispečinků jako center situačního a krizového řízení.
- Zabezpečování objektů a kritické infrastruktury.
- Nastavení dostatečné koordinace na úrovni kraje vedoucí k ochraně obyvatel a území měst a obcí v kraji včetně vydávání veřejně dostupných dokumentů.

2. Příprava měst a obcí v podobě reakcí na extrémní meteorologické jevy

- Zavedení opatření v oblasti realizace zelené infrastruktury měst, obcí a krajů vedoucích ke snížení rizik plynoucích z nahodilých meteorologických jevů, vln sucha, eroze půdy atd.

3. Systematická, efektivní integrace pro sdílení vytěžovaných dat mezi obcemi, městy, kraji při testování inovativních bezpečnostních technologií a přístupů

- Zavedení opatření v oblasti realizace zelené infrastruktury měst, obcí a krajů vedoucích ke snižování rizik plynoucích z nahodilých meteorologických jevů, vln sucha, eroze půdy atd.

4. **Koordinace městských, obecních a krajských úřadů s odpovědnými úřady pro snižování rizik při narušení prvků kritické infrastruktury**

- Zajištění kompatibility inovativních technologických řešení v rámci krizového řízení fungujících na všech úrovních veřejné správy.
- Selektivní ochrana profesí, které jsou nutné pro řešení krizových situací, typicky lékaři, zdravotní personál, hasiči atd.
- Průběžná aktualizace krizových plánů měst, obcí a krajů s ohledem na možnosti nových řešení a technologií.

5. Technické vybavení měst, obcí a krajů pro zvládání katastrof antropogenního a přírodního původu včetně dalších nahodilých událostí velkých dopadů

- Zavedení systému environmentální bezpečnosti na úrovni měst, obcí a krajů s využitím dostupných digitálních technologií.
- Vytvoření a správa funkčního systému varování a vyrozumění obyvatel využívajícího nové technologické možnosti na úrovni krajů, měst a obcí.

Novými trendy by měly být zejména digitální a kybernetické technologie. Krajům bylo doporučeno, aby se více zapojily do rozšiřování a využívání Smart technologií nebo IoT, aby současně poskytovaly jednotnou koordinaci v městech a obcích na svém území při postupné implementaci konceptu Smart Cities v podobě Smart regionu.

Současně byla rozšířena i Národní RIS3 strategie ČR pro programové období 2021–2030 (Kolektiv autorů, 2021b). Její součástí jsou krajské přílohy, které definují krajské priority a návrhy intervencí k jejich naplňování, specifikují krajská aplikační odvětví (krajské domény specializace) za účasti podnikatelské sféry, výzkumné sféry, ale také subjektů z neziskové sféry včetně klastrových organizací a představitelů veřejné správy (Kolektiv autorů, 2019). S rozšířením Národní RIS3 strategie ČR pro programové období 2021–2030 proběhla aktualizace krajských RIS3 strategií o část

s názvem „Digitální agenda“. V této části je zahrnuta část podpory a využívání nových technologií ve veřejné sféře (kraje, složky IZS ČR). Pro přehlednost a názornost je pro Národní RIS3 strategii ČR vypracováno schéma jejích jednotlivých cílů, které jsou vyobrazeny v tabulce 2.

Tabulka 2 Schéma cílů NRIS3 strategie

Schéma cílů Národní RIS3 Strategie				
Strategické cíle	**A.**	**B.**	**C.**	**D.**
	Zvýšení inovační výkonnosti firem	**Zvýšení kvality veřejného výzkumu**	**Zvýšení dostupnosti kvalifikovaných lidí pro výzkum, vývoj a inovace**	**Zvýšení využití nových technologií a digitalizace**
Specifické cíle	**A.1** Posílení inovační výkonnosti stávajících firem a reakce na průmyslovou transformaci, technologické a společenské změny.	**B.1** Zvýšení kvality a společenské relevance veřejného výzkumu.	**C.1** Zlepšení schopnosti vzdělávacího systému připravovat osoby pro výzkum, vývoj a inovace.	**D.1** Podpora digitalizace a využití nových technologií v podnikání.
	A.2 Vznik a růst nových firem a využití nových příležitostí.	**B.2** Zvýšení kvality prostředí pro realizaci veřejného výzkumu.	**C.2** Rozvoj dovedností pro chytrou specializaci, průmyslovou transformaci a podnikání.	**D.2** Podpora digitalizace a využití nových technologií ve veřejné sféře.
	A.3 Zlepšení fungování inovačních ekosystémů na národní a regionální úrovni.		**C. 3** Zvýšení potenciálu a motivace pracovníků ve výzkumných organizacích.	

Zdroj: Metodická doporučení krajům pro aktualizace krajských RIS3 strategií v programovém období 2021+, 2019, vlastní přepracování

Ministerstvo vnitra České republiky (MVČR) je gestorem bezpečnostního výzkumu a integrovalo do NRIS3 strategie ČR související témata a samostatnou strategii s názvem „Meziresortní koncepce podpory bezpečnostního výzkumu ČR 2017–2023 s výhledem do roku 2030 (Oddělení bezpečnostního výzkumu MVČR, 2017). Platná a funkční definice formulovaná Poradním sborem pro evropský bezpečnostní výzkum, anglicky *European Security Research Advisory Board*, umísťuje bezpečnostní výzkum na průsečík environmentálního, ekonomického a společenského

kontextu udržitelného rozvoje. Bezpečnostním výzkumem se rozumí výzkumné, vývojové a inovační činnosti, jejichž cílem je identifikace, prevence, příprava a ochrana proti nezákonným jednáním nebo jednáním úmyslně poškozujícím (evropské) společenství, lidské bytosti, organizace nebo struktury, hmotné i nehmotné statky a infrastruktury včetně zajištění operační kontinuity po takovém jednání a zmírnění jeho důsledků (Oddělení bezpečnostního výzkumu MVČR, 2017).

Hlavními prioritami bezpečnostního výzkumu jsou:

- stabilita, spolehlivost a udržitelnost společenských a ekonomických environmentálních systémů,
- snižování rizik a zvyšování odolnosti,
- rozvoj bezpečnostního systému,
- řešení bezpečnostních incidentů.

Hlavními cíli bezpečnostního výzkumu jsou:

- **Efektivní zásah** – v rámci tohoto cíle jsou rozvíjeny oblasti zaměřené na včasnou výstrahu a situační přehled, efektivní intervenci a vyšetřování incidentů.
- **Adaptabilní bezpečnostní systém** je zaměřen na krizové řízení, bezpečnostní politiku, vnitřní schopnosti bezpečnostního systému a management bezpečnosti informací.
- **Resilientní komunity** – tento cíl je zaměřen na bezpečnost veřejného prostoru, bezpečnost infrastruktur a environmentální bezpečnost.

  Definice cíle uvádí: *„Rozvíjí se předpoklady pro zachování kontinuity služeb a přístupu k nim a respektu k základním společenským hodnotám a potřebám zranitelných skupin obyvatelstva v průběhu krizové situace nebo pod tlakem protispolečenských jevů. Infrastruktury a jejich kritické prvky i části veřejného prostoru jsou navrhovány a stavěny tak, aby odolávaly přírodním katastrofám, haváriím i projevům protispolečenského chování a umožňovaly flexibilní, kontrolované využití v době krizové situace a rychlou obnovu. Proaktivní bezpečnostní kontrola jako prvek zvyšování odolnosti je přizpůsobena dynamice pohybu osob a zboží i standardům lidských práv a zachování důstojnosti jedince. Komunity zasažené závažným bezpečnostním incidentem jsou schopny se s nimi rychle a úspěšně vypořádat včetně minimalizace okamžitých i dlouhodobých a chronických následků.“* (Oddělení bezpečnostního výzkumu MVČR, 2017).

Národní strategie kybernetické bezpečnosti České republiky pro období 2021–2025 ve třetí kapitole vyobrazuje dílčí strategické cíle a vize, jejichž součástí je i část s názvem „Odolná společnost 4.0“.

Vize Národní strategie kybernetické bezpečnosti ČR pro období 2021–2025 jsou vyobrazeny v tabulce 3.

Tabulka 3 Vize Národní strategie kybernetické bezpečnosti

Vize Národní strategie kybernetické bezpečnosti		
Sebevědomě v kyberprostoru	**Silná a spolehlivá spojenectví**	**Odolná společnost 4.0**
Strategické cíle		
• Celonárodní přístup s důrazem na sdílení informací, koordinaci a spolupráci. • Rozvoj schopností a kapacit státu v kybernetické bezpečnosti. • Posílení zabezpečení a odolnosti infrastruktury. • Rozvoj schopností, predikce, detekce a agilní reakce na kybernetický útok. • Účinná strategická komunikace. • Prevence a potírání kybernetické kriminality.	• Efektivní mezinárodní spolupráce. • Tvorba spojenců. • Prosazování zájmů ČR v zahraničí. • Vytváření dialogu v mezinárodním prostředí. • Podpora otevřeného a bezpečného chování v kyberprostoru. • Export know-how.	• Zajištění bezpečnosti digitalizace státní správy (eGovernmentu). • Kvalitní systém vzdělávání. • Osvětová činnost. • Spolupráce státu a soukromé sféry a občanů. • Vytváření expertní základny.

Zdroj: Kolektiv autorů NÚKIB, 2020, vlastní přepracování

Součástí Národní strategie kybernetické bezpečnosti ČR pro období 2021–2025 je i Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025. Akční plán v části C Odolná společnost 4.0 v bodu 88 uvádí: *„Je nutné se podílet na bezpečném rozvoji Smart Cities v ČR v souladu s „Koncepcí SMART Cities – odolnost prostřednictvím SMART řešení pro obce, města a regiony,“* a to například metodickým vedením, konzultacemi ve spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB) a Ministerstvem pro místní rozvoj (MMR) v průběhu celého období 2021–2025 (Kolektiv autorů, 2021a).

Rozvoj implementace koncepce Smart Cities je tedy zahrnut i do strategických dokumentů řešících rozvoj kybernetické bezpečnosti v ČR.

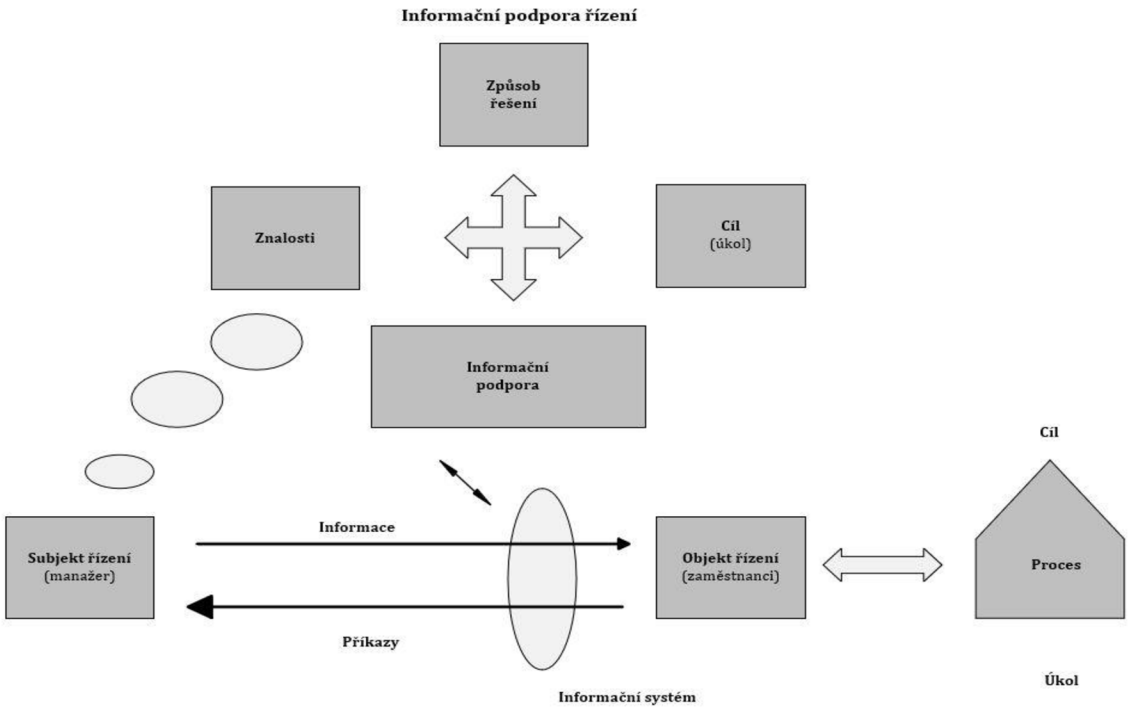
Dílčí části koncepce Smart Cities jsou rovněž součástí strategických a rozvojových dokumentů krajů, měst a obcí. Výběr a rozsah implementace dílčích částí koncepce Smart Cities zahrnutých do strategických dokumentů krajů, měst a obcí pro

implementaci v krajích, městech a obcích jsou řešeny a zahrnovány do strategických dokumentů na základě samostatné působnosti krajů, měst a obcí (autonomní přístup). Ke strategickým dokumentům lze zařadit např. Strategie rozvoje, Strategie ICT, Strategie pro vzdělávání, Strategie pro Smart Cities aj.

V rámci implementace koncepce Smart Cities ve městech a obcích jsou prvky informačního a znalostního managementu klíčové. Díky informačnímu procesu, který zahrnuje sběr, správu a analýzu dat, lze účinně plánovat a řídit současný i budoucí vývoj této koncepce.

Proces řízení je souhrnem dílčích řídících procesů realizovaných jednotlivými řídícími pracovníky organizace. Kvalita řízení je dána kvalitou jednotlivých řídících procesů, kvalitou celkového procesu, který podporuje a integruje dílčí řídící procesy v jeden celek (Lukáš et al., 2008).

Z hlediska správné a efektivní implementace koncepce Smart Cities je důležitá informační podpora řízení, která představuje proces činností podporujících řízení po informační stránce. Proces informační podpory řízení je zobrazen na obrázku 1 na další straně.



Obrázek 1 Proces informační podpory řízení

Zdroj: Lukáš et al., 2008, vlastní přepracování

4.2 Metody pro přípravu nových bezpečnostních standardů a nových právních předpisů

Pro zkoumání aktuálního stavu metodik a jiných metod pro přípravu a zpracování legislativních norem, bezpečnostních standardů a doporučení s využitím informačních technologií byla provedena rešerše, která je založena na metodickém postupu rešeršní strategie (anglicky *Search Strategy*). Odborné články byly hledány ve vědeckých databázích Scopus, Web of Science (WoS). Zpracovaná rešeršní strategie byla pro přehlednost rozdělena do dílčích podkapitol.

4.2.1 Česká republika

Tato dílčí část rešeršní strategie rozpracovává řešenou problematiku v rámci České republiky.

Prvně bylo zmíněno využívání kybernetických metod v právu v knize od V. Knappa. Kniha vymezuje předmět zkoumání a možnosti aplikace kybernetických strojů v právu a jejich obtíže, dále rozpracovává obecné předpoklady pro využívání kybernetických metod v právu, v soudní statistické dokumentaci (Knapp, 1963).

V České republice byla problematika automatizovaného zpracovávání textů dále řešena v rámci obhájené disertační práce z roku 2007, tedy téměř po 45 letech. V této disertační práci byla zpracována analýza právních textů, které však nebyly předem syntetizovány s využitím prostředků informačních technologií, ale byly zkoumány v rámci odborného přirozeného jazyka. Cíle této práce byly zaměřeny na výskyt možných problémů, které se mohou vyskytovat při zpracovávání právních textů s využitím počítačové techniky, a dále na zkoumání hierarchických vztahů v návaznosti na možnost zpracovávání právních textů v podobě automatizovaného zpracování. Dále práce rozpracovávala problematiku lingvistické, strukturální, logické analýzy a zkoumala zpracování jevů právních textů včetně následné syntézy. V závěru byl rozpracován volně dostupný software (v čase zpracovávání práce v roce 2007), který byl využit jako expertní systém pro zpracování právních textů, kdy byla vytvořena znalostní báze ze strany autora (Ptašnik, 2007).

Na řešení problematiky spojené s přípravou nových právních předpisů navazuje kniha od M. Kokeše vydaná v roce 2020, která rozpracovává „temné zákoutí legislativního procesu“ spojené zejména s přípravou vládních návrhů zákonů v České republice. Kniha je svým zaměřením zpracována jako přehledová publikace, jež shrnuje problematiku přípravy legislativního procesu z hlediska zákonodárného procesu. Obsahuje přes 650 literárních zdrojů a z hlediska zpracování poskytuje

čtenářům vhled do řešené problematiky na národní a mezinárodní úrovni a poukazuje na současné problémy spojené s přípravou nových právních předpisů (Kokeš, 2020).

Z hlediska řešeného problému v této disertační práci lze tedy konstatovat, že tato disertační práce navazuje na problém, který byl v minulosti s velkými odstupy rovněž zpracován.

Tato disertační práce svým zaměřením systematicky navazuje a analyzuje metody z oblastí informačního a znalostního managementu pro efektivní zpracování nových právních předpisů a bezpečnostních standardů s možností dalšího využití v praxi.

Návrh metod pro přípravu nových právních předpisů a bezpečnostních standardů je tedy primárně určen pro organizace podílející se na přípravě nových nebo aktualizovaných právních předpisů a bezpečnostních standardů. Další možností uplatnění může nalézt i v mnohých organizacích při přípravě a aktualizaci interních směrnic či jiných pokynů. Návrh vhodných metod může nalézt uplatnění i u organizací na mezinárodní úrovni, což dokládá i publikovaný příspěvek autorky na prestižní zahraniční konferenci (Svecova, 2022).

4.2.2 Zahraničí

Tato část rešeršní strategie byla zaměřena na oblast využívání vhodných inovativních softwarových nástrojů pro zvýšení efektivnosti přípravy právních předpisů a bezpečnostních standardů v zahraničí.

Mousmounti (2019) ve své knize popisuje nástroje pro efektivní zákonodárný proces, avšak pouze z hlediska metodicko-právního v podobě RIA, konzultací a zjednodušení. Prosazuje novou myšlenku, že legislativní účinnost je výsledkem složité „mechaniky“ v konceptualizaci, designu a navrhování ze čtyř prvků obsažených v každém právu: účel, obsah, kontext a výsledky. Dochází k závěru, že efektivity lze dosáhnout pomocí koncepčních a metodologických poznatků, které vedou konkrétní volbu zákonodárců při navrhování a prosazování legislativy.

Rodiyah et al. (2022) analyzují využití informačních technologií pro přípravu zákonů a dalších předpisů v Indii.

Palmirani (2022) popisuje využití hybridního přístupu umělé inteligence v souvislosti s evropskou legislativou s cílem analyzování a komparace podobnosti evropských směrnic.

Beaulieu (2020) píše o možnosti využití inovací při navrhování právních předpisů, jejich výhodách a také o překážkách při přijímání. Inovaci spatřuje ve využívání

moderního nástroje CC Dr@ft, ve kterém jsou integrovány prvky automatizace pro práci s dokumenty.

Ashley (2017) ve své knize analyzuje a popisuje interdisciplinární oblasti, které jsou vhodné pro vývoj vhodných softwarových nástrojů založených na využití umělé inteligence v souvislosti s legislativním procesem.

Moore (2019) charakterizuje ve svém článku dopady moderních technologií na právnickou profesi včetně dopadů moderních technologií na zákonodárný proces. Ve své práci popisuje využití automatizovaných procesů za pomoci robotů, dále zmiňuje i implementaci prvků AI.

Ptitsyna (2022) ve svém článku představuje softwarový produkt od společnosti Lawrina, který je využíván pro přípravu smluv a využívá prvky umělé inteligence.

Lloyd (2020) se ve své knize zaměřuje na vývoj informačního práva v UK a EU.

Fekete & Bubori (2019) popisují ve svém článku problematiku vztahů práva a informačních technologií.

Lubua (2017) v se ve své studii zaměřil na využití ICT prostředků pro efektivní využití v eGovernmentu. Studie popisuje využití informačních technologií při legislativním procesu v Tanzanii.

Sartor (2011) ve své knize analyzuje a srovnává problematiku využití informačního a znalostního managementu při legislativním procesu a dále srovnává aspekty právní a legislativní informatiky.

Clark (1992) ve svém článku analyzuje vývoj informačních technologií využívaných v právních službách.

Moses & Chan (2014) popisují a analyzují možnosti využití Big Data v soudních, civilních a policejních procesech za účelem vymáhání práva.

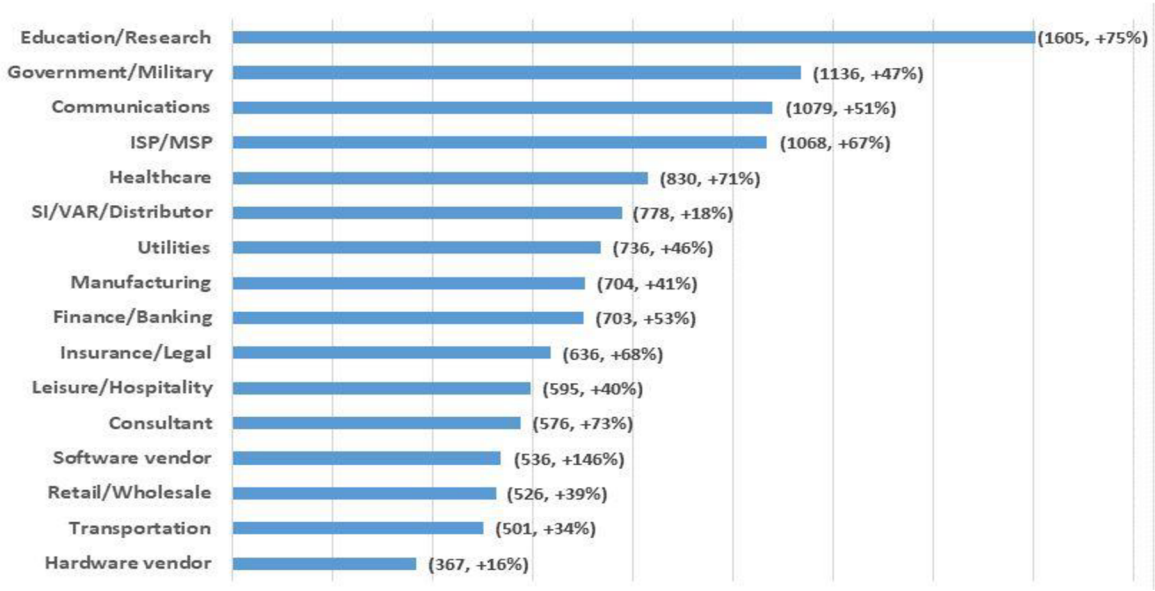
Konkrétní využívání vhodných softwarových nástrojů je v nalezených článcích obsaženo však minimálně. Obdobným způsobem je v zahraničních článcích řešen proces návrhu přípravy nových bezpečnostních standardů a právních předpisů. Na základě zjištěných informací lze konstatovat, že vhodné metody či jejich kombinace, jež by zaváděly inovační prvky do procesu přípravy či následné tvorby, nejsou využívány.

4.2.3 Bezpečnostní standardy pro IoT

V této části rešeršní strategie byla provedena analýza existujících bezpečnostních standardů pro IoT.

Současná doba je dobou velkého rozvoje a zavádění digitalizace do všech odvětví včetně pokročilé implementace nových technologií s využitím umělé inteligence (AI),

IoT či strojového učení. Velmi úzce s touto problematikou souvisí i potřeba ukládání enormních objemů dat v lokálních či cloudových úložištích. V posledních letech vzrostl i počet kybernetických útoků (v období 2020–2021 vzrostl o 50 %), jež byly cíleny především na vzdělávací organizace, vojenský sektor a sektor veřejné správy, komunikační průmysl či zdravotnictví. Statistický přehled kybernetických útoků v souvislosti a s IoT s rozdělením na různá odvětví je zobrazen na obrázku 2 .



Obrázek 2 Kybernetické útoky na IoT v různých odvětvích

Zdroj: Gmcdouga, 2022

Útoky často eskalují právě v krizových okamžicích, kdy lze očekávat, že lidé budou pod pracovním tlakem náchylnější k chybám. Standardním příkladem byly útoky na zdravotnická zařízení v době špičky koronavirové krize, kdy péči o pacienty zhoršil výpadek NIS, s nímž jsou svázány přístroje sloužící k vyšetření nebo podpoře životních funkcí pacientů (Svecova, 2022). Má-li být uplatněn a využíván trend Smart technologií, zejména tedy IoT s využitím sítí 5G, je nutné systémy dostatečně zabezpečit na technické a legislativní (metodické) úrovni.

Nejčastějšími cíli hackerů jsou právě systémy kritické informační infrastruktury (KII), které fungují dle § 2 písm. g) zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (dále jen krizový zákon).

Kritickou informační infrastrukturou se rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, kdy narušení jejich funkcí by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva,

zdraví osob nebo ekonomiku státu. Prvky kritické infrastruktury (zejména stavby, zařízení, prostředky nebo veřejná infrastruktura) jsou určené podle průřezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury a subjektem je provozovatel prvku kritické infrastruktury; jde-li o provozovatele prvku evropské kritické infrastruktury, považuje se tento za subjekt evropské kritické infrastruktury (Zákon o krizovém řízení a o změně některých zákonů (krizový zákon), 2000).

Miniaturní zařízení IoT a další jednoúčelová zařízení s nízkou energetickou spotřebou i kapacitou paměti nejsou vždy schopna obrany proti cíleným a sofistikovaným kybernetickým útokům, čímž se právě tato zařízení stávají v posledních letech cíli ze strany útočníků.

Největším problémem současnosti v souvislosti s využíváním a rozvojem IoT je problém zabezpečení, protože IoT jsou zařízení, na která nelze aplikovat standardní doporučení. Internet věcí je velmi specifická oblast, jejíž bezpečnost je aktuálně nejvíce řešenou problematikou na celosvětové úrovni v mnoha mezinárodních organizacích při vzájemné součinnosti gestorů kybernetické bezpečnosti.

Nejvíce zneužitelné bezpečnostní chyby, tedy kybernetické útoky, jsou zaměřeny na oblast nedostatečné globální správy v podobě *Group Policy Object* (GPO), politik nezabezpečených rozhraní (webových, mobilních, cloudových či API), nemožnost centrální správy aktualizací a především existují problémy v absenci dílčích metodických doporučení, mezinárodních norem a odpovídající právní úpravy. Bezpečnostní rámec pro IoT je tedy nutno řešit komplexně na národní a mezinárodní úrovni z více hledisek, a to z hlediska národních legislativních právních norem, z hlediska evropského práva, z hlediska mezinárodního práva a dále z hlediska celosvětově platných a uznávaných mezinárodních norem a bezpečnostních standardů.

Zákon o zlepšení kybernetické bezpečnosti IoT z roku 2020, podepsaný v prosinci téhož roku, vyžaduje, aby vládní agentury zajistily bezpečnost svých zařízení IoT. Několik států včetně Kalifornie a Oregonu již přijalo zákony o kybernetické bezpečnosti internetu věcí (*2.17 Internet of Things Cybersecurity Improvement Act of 2020*, 2020).

Výše uvedený zákon o kybernetické bezpečnosti internetu věcí systematicky doplňují bezpečnostní standardy a normy zpracovávané a postupně doplňované Národním institutem pro standardy a technologie, anglicky *National Institute of Standards and Technology* (NIST).

Výchozím dokumentem pro řešení bezpečnosti IoT, který zpracoval NIST, je řada publikací s označením NISTIR 8259 (*NISTIR 8259 Series | NIST*, 2020).

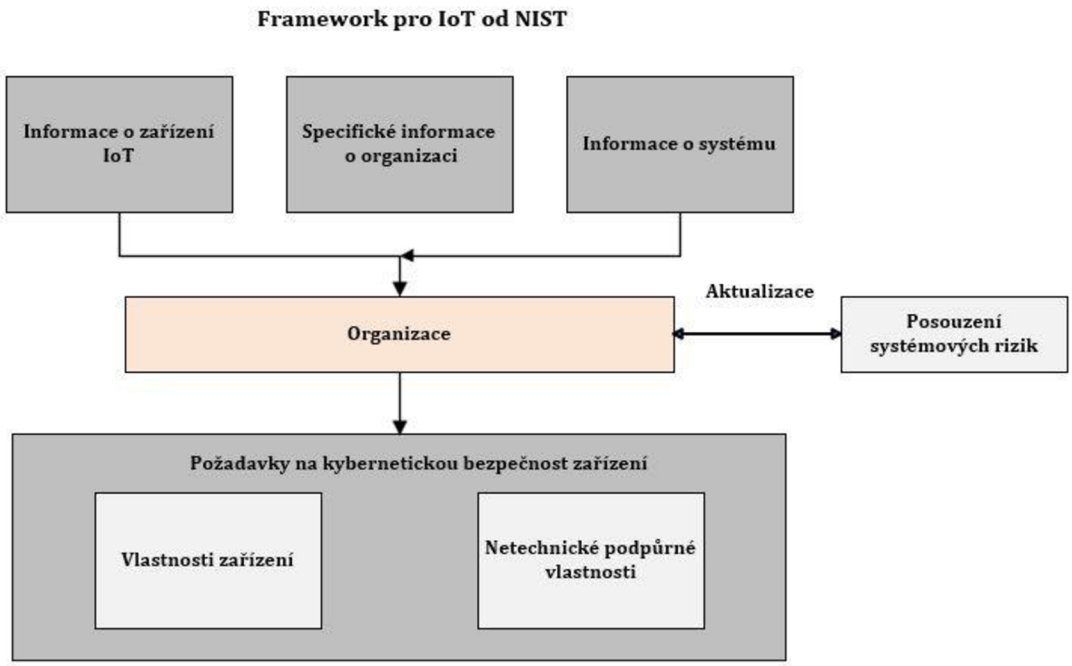
Bezpečnostní standardy a doporučení řady NISTIR 8259 obsahují pokyny výrobcům a jejich podpůrným třetím stranám při navrhování, vývoji, testování, prodeji a podpoře zařízení IoT napříč spektrem zákazníků. Tato řada doporučení je složena ze tří dílčích částí: doporučení pro výrobce zařízení IoT (NISTIR 8259), základní doporučení pro kybernetickou bezpečnost (NISTIR 8259 A) a netechnické doporučení pro IoT v základní úrovni (NISTIR 8259 B). Základní linie NISTIR 8259 A/8259 B představují společnou sadu základních funkcí, které jsou užitečné pro širokou škálu aplikací, případů použití a typů zákazníků. Zjednodušené schéma NISTIR 8259 je zobrazeno na obrázku 3.

Obrázek 3 Standard NISTIR 8259

Zdroj: NISTIR 8259 Series NIST, 2020, vlastní přepracování

Metodický rámec řady NIST SP 800-213 je zaměřen na potřeby federálních agentur, které usilují o nasazení zařízení IoT ve svých systémech. Rámec charakterizuje zařízení IoT pro jejich systémy a je doplněn pokyny pro řešení rizik vzniklých v souvislosti s používáním. SP 800-213 je doplněno o část SP 800-213A, která obsahuje katalog požadavků na kybernetickou bezpečnost zařízení IoT včetně technických a netechnických doporučení („SP 800-213 Series", 2021). Doplňující rámec SP 800-213A může být využit pro zpracovávání interních směrnic a doporučení pro organizace, současně tento rámec navazuje na rámec SP 800-53 Kontroly zabezpečení a soukromí pro informační systémy a organizace (Force, 2020). Uvedené metodické doporučení lze využít ve shodě s řadou NISTIR 8259, kombinací uvedených doporučení

by mělo být dosaženo efektivního zabezpečení IoT pro využití v organizacích. Schéma frameworku pro IoT je zobrazeno na obrázku 4.



Obrázek 4 Framework IoT NIST

Zdroj: SP 800-213 NIST, 2021, vlastní přepracování

National Instituce of Standards and Technology se také podílí na tvorbě metodických doporučení pro zabezpečení pro IoT, která jsou využívána spotřebiteli např. v rámci Smart Home. Současně NIST identifikoval klíčové prvky programu označování internetu věcí z hlediska minimálních požadavků a žádoucích atributů a specifikoval požadované výsledky, čímž umožnil poskytovatelům a zákazníkům volbu nejlepšího řešení pro jejich produkty a služby. Dne 31. srpna 2021 vydal NIST Bílou knihu s návrhem kritérií pro program označování schopností kybernetické bezpečnosti zařízení internetu věcí a požádal o připomínky k návrhu kritérií, které navrhly sadu potenciálních základních bezpečnostních kritérií pro zařízení internetu věcí. Na základě připomínek byly vydány Souhrnná zpráva o kybernetickém označování spotřebitelských produktů IoT a spotřebitelských softwarových produktů (10. května 2022) a Doporučená kritéria pro označování spotřebitelských produktů internetu věcí pro kybernetickou bezpečnost (4. února 2022) („IoT Product Criteria", 2021).

Celosvětová organizace sídlící v USA *s* názvem Cloud Security Alliance se také podílí na tvorbě bezpečnostních standardů pro IoT. V roce 2019 vydala rámec

zavádějící bezpečné kontroly rizik připojených IoT zařízení (*CSA IoT Security Controls Framework*, 2019).

K dalším celosvětovým organizacím sídlícím v USA patří organizace s názvem Certified Threat Intelligence Analyst. Tato organizace se podílí na certifikaci kybernetické bezpečnosti pro IoT a podílí se i v rámci EU na zpracování certifikačního schématu pro IoT podle nařízení EU, které zavádí jednotný rámec pro Evropské certifikace kybernetické bezpečnosti (*IoT Cybersecurity Certification*, 2019).

Průvodce kybernetickou bezpečností IoT byl zpracován v Singapuru (Asie) organizací Infocomm Media Development Authority (collective of authors, 2019). Problematikou bezpečnostních standardů se zabývala i australská organizace IoT Alliance Australia, která v roce 2017 publikovala pokyny pro zabezpečení IoT (Collective of authors, 2017).

Na základě výše uvedených informací lze konstatovat, že problematika a podpora zvyšování bezpečnostních standardů pro IoT je na mezinárodní úrovni a mimo EU aktivně řešena pro běžné spotřebitele a také pro organizace (Business a eGovernment).

Současně je problematika jednotných bezpečnostních standardů a legislativní úpravy řešena na úrovni EU prostřednictvím všech států za účelem sjednocení obecného přístupu o kybernetické bezpečnosti orgánů, institucí a jiných subjektů Unie (*Cyber Resilience Act | Shaping Europe's Digital Future*, 2022). Cílem je nastavení jednotných pravidel kybernetické bezpečnosti u jednotlivých subjektů a posílení odolnosti vůči kybernetickým hrozbám za účelem napravení dosavadního nevyhovujícího stavu, kdy existují na úrovni kybernetické bezpečnosti unijních subjektů velké rozdíly a chybí jednotná úprava pravidel v této oblasti (*Národní úřad pro kybernetickou a informační bezpečnost - Jednotná pravidla kybernetické bezpečnosti subjektů EU jsou opět o něco blíž*, 2022). Kybernetická bezpečnost v souvislosti s legislativním rámcem na úrovni EU je tedy aktivně řešena již několik let.

Členské státy Evropské unie usilovaly o zavedení systému jednotné kybernetické certifikace produktů, procesů a služeb (Svecova, 2022). Tato jejich snaha vyústila v přijetí nařízení EU s názvem Akt kybernetické bezpečnosti (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), 2019).

Nařízení EU zavádí jednotný rámec pro sjednocení kybernetické bezpečnosti v podobě institutu jednotných certifikací produktů, procesů a služeb podle jednotných certifikačních schémat EU platných pro všechny členské státy. Preferována je především oblast pro certifikaci hardwaru. Obsahem nařízení je i vytvoření jednotného certifikačního rámce pro IoT, v tento okamžik dle dostupných informací probíhá příprava certifikačního rámce (*Eurosmart | The Voice of the Digital Security Industry | Eurosmart IoT Certification Scheme*, 2019). V roce 2018 byl zveřejněn dokument, který byl zaměřen na problematiku bezpečnostních standardů, jenž měl za cíl analyzovat nedostatky v oblasti zabezpečení pro IoT. Analýzu zpracovala Agentura EU pro kybernetickou bezpečnost, The European Union Agency for Cybersecurity (ENISA), dokument systematicky mapuje aktuální normy týkající se informační bezpečnosti a soukromí v oblasti IoT (Andrukiewicz et al., 2018).

V průběhu roku 2018 byly současně vydány od ENISA základní bezpečnostní doporučení pro IoT (*Baseline Security Recommendations for IoT*, 2017) a seznam standardních postupů pro bezpečnost IoT v kontextu průmyslu 4.0 (*Good Practices for Security of Internet of Things in the Context of Smart Manufacturing*, 2018).

Finsko definovalo bezpečnostní standardy pro IoT pro spotřebitele normou ETSI TS 103 645 Cyber Security for Consumer Internet of Things (*ETSI TS 103 645 Cyber Security for Consumer Internet of Things*, 2019).

Velká Británie v rámci Britského standardizačního institutu, anglicky *British Standards Institution,* zpracovala tzv. Průvodce pro malé a střední podniky a začínající firmy, který je metodickou pomůckou z hlediska norem při zavádění IoT (Bass et al., 2020).

V UK je zřízena Vládní agentura pro digitalizaci, která zpracovává metodická doporučení v oblasti kybernetické bezpečnosti. V roce 2018 byla publikována pravidla pro bezpečnost spotřebitelského internetu věcí (*Code of Practice for Consumer IoT Security*, 2018) a současně byl publikován kodex pro zabezpečení IoT využívaného ze stran spotřebitelů (*Mapping of IoT Security Recommendations, Guidance and Standards*, 2018).

Další agenturou sídlící v UK, která je současně celosvětovou organizací, je organizace *GSMA*. Tato organizace zpracovala bezpečnostní rámec, jenž poskytuje komplexní soubor osvědčených postupů pro návrh, vývoj a implementaci IoT v organizacích („IoT Security Assessment", 2020).

Bezpečnostní standardy, frameworky a různá doporučení z hlediska zabezpečení pro vývoj a implementaci IoT v organizacích či domácnostech jsou aktivně řešeny ze stran celosvětových organizací a gestorů kybernetické bezpečnosti, jejichž spolupráce je úzce provázána. Lze tedy konstatovat, že problematika zabezpečení IoT je aktivně řešena na národních úrovních, v rámci EU či na úrovni mezinárodní.

Z pohledu legislativního bylo v rámci EU přijato aktualizované znění Směrnice NIS (NIS2) (Směrnice Evropského parlmentu a Rady ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148, 2022). Bezpečnostní doporučení či framework pro IoT však není v aktualizované směrnici NIS2 detailně rozpracováno.

V neposlední řadě je důležité zmínit národní legislativu, která je platná na území České republiky. Primární právní normou v oblasti kybernetické bezpečnosti je zákon o kybernetické bezpečnosti (181/2014 Sb. Zákon o kybernetické bezpečnosti, 2015) a prováděcí vyhláška k zákonu o kybernetické bezpečnosti (Vyhláška č. 82/2018 Sb., obezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), 2018).

V rámci celosvětové působnosti v oblasti IoT pro Smart Cities jsou uznávané pouze standardy IoT-Enabled Smart City Framework (Burns, 2018). Tyto standardy jsou založeny na obecném typu frameworků, které mohou být implementovány v různých odvětvích.

4.2.3.1 Využití bezpečnostních standardů v tematicky zaměřené části koncepce Smart Cities

V rámci této poslední části rešeršní strategie byla rozpracována problematika související s využíváním informačních technologií v návaznosti na tematicky zaměřenou část koncepce Smart Cities související s krizovým řízením (ochranou obyvatel). Tato část rešeršní strategie byla zahrnuta do analýzy současného stavu, protože při návrhu vhodné metody byla zvolena i metoda pro zkoumání textu, jež byla ověřena v rámci vzorku pro prvotní návrh nových bezpečnostních standardů pro IoT využívaných v kamerových systémech. Tato podkapitola tedy podrobně rozpracovává využívání informačních technologií v tematicky zaměřené části koncepce Smart Cities.

Tematicky zvolená oblast s názvem Rychlá reakce je součástí koncepce Smart Cities, která je právně závazná na celém území České republiky (Nencková & Bízková, 2021).

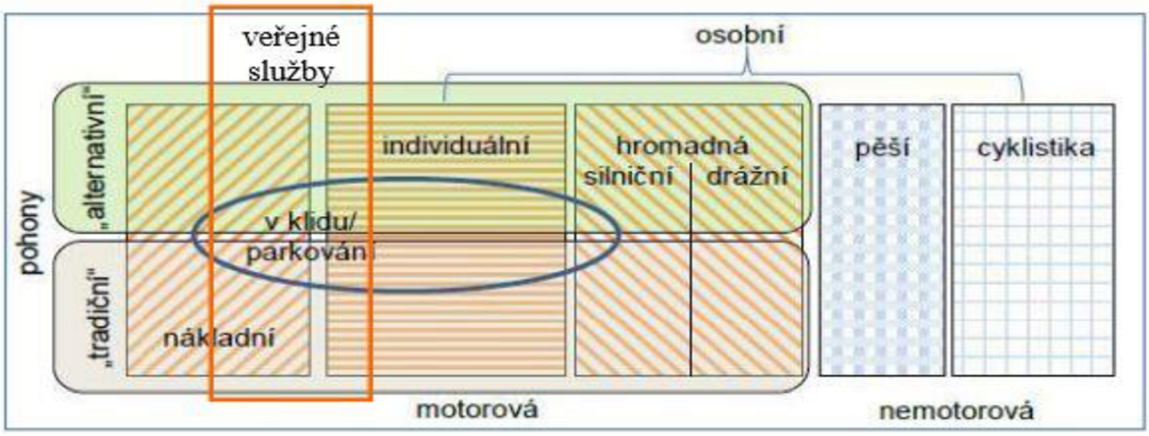
Informační management zahrnuje mnoho procesů, které jsou zásadní pro správnou funkci organizace či státu. Mezi ně náleží například procesy plánování, organizování, vedení a kontroly informací a dat. V období pandemie COVID-19 byla aktivně řešena problematika využívání IoT ze strany složek IZS ČR pro efektivní zajišťování ochrany obyvatel a bezpečnosti veřejného pořádku, avšak ani pro tuto speciálně zaměřenou oblast neexistují jednotné standardy pro zabezpečení IoT.

V souvislosti s pandemií COVID-19 se projevila potřeba využití složek IZS ČR, a tedy také potřeba využití Smart technologií v oblasti kybernetické bezpečnosti při ochraně veřejného pořádku a obyvatel.

Bezpečnostní složky podílející se na každodenní ochraně obyvatel ve městech a obcích jsou tvořeny Policií ČR a městskou policií zřizovanou městem či obcí (Zákon č. 553/1991 Sb. , o obecní policii, 1991). Problematika bezpečnosti obyvatel a ochrany veřejného pořádku nebyla v přijatých koncepcích Smart Cities do roku 2020 řešena téměř vůbec. Bezpečnost obyvatel je velmi obecně zmíněna v metodice pro přípravu a realizaci strategie Smart Cities na úrovni měst, obcí a regionů, kde jsou složky IZS zahrnuty do části zaměřené na mobilitu, přičemž do městské mobility spadají dopravní prostředky IZS:

- HZS ČR – převážně nákladní,
- PČR – převážně osobní,
- ZZS – převážně osobní (sanitky).

Podle uvedené metodiky: *„Realizovat čistou městskou mobilitu znamená řešit a prosazovat rovnováhu mezi všemi těmito prvky městské mobility včetně požadavků na efektivní řízení dopravy zohledňující potřeby složek IZS, nouzových a havarijních služeb, městských služeb.“* (Pracovní skupina pro Smart Cities, 2018). Základní struktura městské mobility je vyobrazena na obrázku 5 dále.



Obrázek 5 Schéma městské mobility

Zdroj: Pracovní skupina pro Smart Cities MMR, 2018

Výše uvedená metodika zmiňuje složky IZS ČR, ale pouze ve spojení s mobilitou, nikoliv s ochranou bezpečnosti obyvatel a veřejného pořádku. Dokument uvádí jen strohé informace související se zapojením bezpečnostních složek IZS ČR v rámci ochrany obyvatel do části zaměřené na městskou mobilitu. Vzájemnou koordinaci z pozice krajských samospráv však metodika neobsahuje.

V období pandemie COVID-19 vznikl v ČR projekt s názvem Chytrá karanténa, který byl realizován pod záštitou českých IT firem sdružených pod názvem COVID19CZ (*Chytrá karanténa – Aktuální informace o COVID-19*, 2020). Chytrá karanténa je mobilní aplikace založená na mapování pohybu nakažené osoby za posledních pět dní na základě údajů od mobilních operátorů a údajů z kreditní karty. Takzvaná „vzpomínková mapa", jež z těchto dat vznikla, pomáhala hygienikům v trasování infikované osoby. Nástroj byl také integrován i do mobilní aplikace Mapy.cz (*Mapy.cz*, 2020).

Projektu Chytrá karanténa předcházel projekt v podobě mobilní aplikace s názvem Záchranka, která je využívána ze strany obyvatel pro každodenní ochranu zdraví. Mobilní aplikace Záchranka je využívána pro kontakt se ZZS, HZS a PČR v akutních případech, kdy osoba může využitím mobilní aplikace přímo předat na operační pracoviště souřadnice místa události (místa ohrožení, bydliště, ve kterém se nachází, případně kde se objevily akutní zdravotní problémy). Za pomoci této mobilní aplikace lze kontaktovat pomoc i ve vybraných příhraničních oblastech států sousedících s ČR. Aplikace má navíc i edukativní část, díky níž se uživatel může seznámit s postupy v různých život ohrožujících situacích (Švecová & Blažek, 2021).

Na úrovni mikroregionů byly Smart technologie především v podobě IoT včleněny do každodenního života občanů. Tyto technologie je možné nalézt v městské hromadné dopravě v podobě účtování jízdného na základě biometrické identifikace obličeje či v podobě bezkontaktních plateb. Další IoT technologie jsou propojeny s odpadkovými koši, které v případě naplnění odešlou notifikaci na centrálu pro sběr odpadu, aby naplněné kontejnery byly vyprázdněny. Právě s pomocí IoT technologií v Smart Cities je prováděno nepřetržité monitorování různých oblastí a je možné vydávat i varování před možnými katastrofami či mimořádnými krizovými událostmi (Kummitha, 2020).

K dalším technologiím, které jsou implementovány v Smart Cities pro zajištění ochrany obyvatelstva a veřejného pořádku, patří kamerové systémy, které jsou v mnoha městech integrovány na vysoké úrovni. Mnohé kamerové systémy mají implementovanou umělou inteligenci s možností biometrické identifikace.

Kamerové systémy v Smart Cities v ČR jsou provozovány městkou policií, Policií ČR, hasiči a zdravotníky. Postupnou modernizací a implementací Smart technologií jsou integrovány a vzájemně propojovány na operační střediska uvedených složek. Při vzájemném propojení systémů tak mohou všechny složky včas operativně reagovat na aktuální mimořádné události v konkrétní okamžik.

Kamerové systémy tak poskytují bezpečnostním složkám ve městech obrazové informace z různých míst ve městech a obcích. Současně je možné CCTV propojit i do systémů chytrého parkování (Smart Parking). Komplexní kamerový systém pak může být provázán s dalšími IS, a to např. pátrání po pohřešovaných osobách (PATROS), pátrání po odcizených vozidlech, dopravních nehodách či jiných incidentech.

V roce 2020 byl zahájen projekt s názvem: „Přístupy do informačních systémů Policie České republiky pro obecní policie“ (*Přístupy do informačních systémů Policie České republiky pro obecní policie - Ministerstvo vnitra České republiky*, 2019).

Podstatou výše uvedeného projektu je propojení kamerových systémů hlavních složek IZS a obecní (městské) policie pro rychlejší stanovování operativních postupů při vyhodnocování aktuální situace vyobrazené na zobrazovacích panelech v operačních střediscích a dále pro případný okamžitý efektivní zásah na místě ze strany PČR či jiných složek IZS ČR.

Vyšší dostupnost dat z informačních systémů Policie České republiky a Ministerstva vnitra velmi pomáhá ke zvýšení bezpečnosti občanů. Do CCTV se postupně implementují i prvky umělé inteligence (AI) pro automatické vyhodnocování

a predikci nahodilých mimořádných událostí bez zásahu osob. CCTV systémy tak náleží k základním prvkům (technologiím) implementovaným ve městech a obcích pro ochranu obyvatelstva, veřejného pořádku a prostranství.

Rozvoj inteligentních technologií včetně IoT lze u složek IZS nalézt třeba v podobě využívání dronů („Využití dronů pro Integrovaný záchranný systém", 2020). V rámci eHealth koncepce EU je pak možné využít integrace záchranného systému i s příhraničními oblastmi sousedících států.

Po celém světě vznikají i výzkumné projekty zaměřené na využití IoT v bezpečnostních složkách státu při současné integraci, jež jsou současně aplikovatelné v Smart Cities.

V USA byl realizován projekt s názvem „Program pro včasnou reakci na záplavy při zvednutí hladiny moře“. Program je založen na využití 3D modelování a LIDAR, anglicky *Light Detection and Ranging Data,* a je určen pro informování místních samospráv o nejrizikovějších oblastech a k zajištění včasného varování obyvatel. Na úrovni EU je realizován projekt Reverse 112, který reaguje na zavedení jednotného standardu pro pomoc varování obyvatelstva s názvem „Telefonní centrum tísňového volání“ (TCTV 112) na úrovni EU.

K budoucím vizím EU patří systémy varování obyvatelstva s využitím IoT prostřednictvím chytrých domů či chytrých spotřebičů a s návazností na inteligentní informační systémy Smart Cities (Kolektiv autorů, 2018).

K dalším využívaným technologiím u složek IZS patří bezpilotní letouny, tzv. drony, označované anglicky jako *Unmanned Aerila Vehicle* (UAV). Dron je letadlo bez posádky, které může být řízeno na dálku nebo létat samostatně pomocí předprogramovaných letových plánů nebo pomocí složitějších dynamických autonomních systémů (*Co je dron?*, 2022).

Drony byly a jsou postupně implementovány do metodik, procesů a činností bezpečnostních složek po celém světě včetně využití v komerční sféře. Policie ve Velké Británii začala drony testovat v roce 2015, později vznikla i specializovaná jednotka (Loughran, 2017). V rámci policie byl proveden výzkum, který byl zaměřen na využití dronů při sledování osob (Ward, 2016).

V rámci průzkumné studie se zaměřením na využívání dronů pro pomoc hasičům při mimořádných situacích bylo ověřeno, že využití dronů má velké výhody pro hasiče i občany. V návaznosti na provedenou studii bude v Kanadě u záchranných složek

implementována technologie 9-1-1 pro call centra u hasičů (Khan & Neustaedter, 2019).

Využití dronů nachází své uplatnění i v dalších oblastech bezpečnostní praxe. Touto oblastí je monitoring bezpečnosti silničního provozu. V roce 2017 byly v Dubaji nasazeny drony pro monitoring silniční dopravy a ulic, dále k využití průzkumu stavu vozovek, stanic metra a tramvají (Tesorero, 2021). Využití dronů při ochraně obyvatelstva je možné nalézt i u Horské záchranné služby (Holzmann et al., 2021). Drony v záchranných složkách jsou využívány pro jejich rychlost, protože mnohdy se sanitky kvůli přetížené dopravě ve velkých městech potýkají s hustým dopravním provozem a zdravotníci se velmi těžce dostávají k pacientům. Alex Monton, postgraduální student Delft University Netherlands, vytvořil sanitní dron, který může dorazit na místo nehody již za minutu po odeslání, tedy rychleji než sanitka pomocí automobilové dopravy (Lisa, 2015). Využití dronů a jejich implementace nejen v oblasti ochrany obyvatel a veřejného pořádku jsou závislé na typech činností, pro které mají být drony uplatněny. Drony jsou využívány i v komerčním sektoru v marketingu, v oblastech vzdělávání, logistice a dalších činnostech.

Organizace Cloud Security Alliance (CSA) a Securing Smart Cities zveřejnila zprávu, že v blízké budoucnosti je plánováno vytvoření programu pro zavedení bezpečných dronů v Smart Cities, a současně v programovém prohlášení zdůraznila, že drony budou hrát důležitou roli v Smart Cities (PricewaterhouseCoopers, 2021).

Státy po celém světě nebyly na pandemii COVID-19 dostatečně připraveny z pohledu ochrany obyvatel a informačních technologií, kybernetické bezpečnosti a Smart technologií. V rámci koncepcí Smart Cities a Smart Region po celém světě byla tato dílčí část často opomíjena, což mělo v počátcích pandemie negativní dopady. Negativní dopady se projevily v podobě špatné koordinace při distribuci ochranných pomůcek z důvodu chybějících IS, nepropojenosti IS s bezpečnostními složkami státu či chybějících krizových plánů a hlavně v podobě nedostatečného zabezpečení systémů kritické informační infrastruktury ve zdravotnictví z pohledu kybernetické bezpečnosti.

K velkým negativním dopadům, které se vyskytly v době první vlny COVID-19, patřily cílené kybernetické útoky na nemocnice v ČR (*Nemocnice pod náporem hackerů*, 2021). Nejednalo se jen o ČR, po celém světě čelily nemocnice intenzivní sérii útoků po dobu několika měsíců.

Rozvoj a postupné zvyšování implementace informačních a Smart technologií v souvislosti s konceptem Smart Cities a ochranou obyvatel již však započal a je implementován v Smart Cities po celém světě.

Rozvoj informačních technologií je permanentní, proto je nezbytné do problematiky bezpečnosti občanů a zvyšování kybernetické bezpečnosti s využitím IoT v Smart Cities v součinnosti s dalšími subjekty zahrnout veškeré nastupující technologie a koncepty, např. sítě 5G či řešení umělé inteligence (Švecová & Blažek, 2021).

Na základě provedené analýzy využívaných technologií v koncepci Smart Cities v návaznosti na krizové řízení byly vhodně zvoleny existující právní předpisy, bezpečnostní standardy a další související metodiky, které jsou dále rozpracovány v souladu s metodologickým postupem v rámci navržené metody pro zkoumání textu v kapitole 5.

5 POPIS ŘEŠENÍ A VÝSLEDKY VÝZKUMU

V této části disertační práce je rozpracována a popsána řešená problematika na základě provedené rešeršní strategie současného stavu, navrženy vhodné metody, ověřena validace a stanoveny přínosy práce.

Metodickým základem vědeckého zkoumání je metodologie vědy a filozofie, jejím předmětem je zkoumání metod a vědeckých postupů, je to tedy nauka o metodách. Metoda je pak nástrojem pro zkoumání stanoveného problému, kdy jsou aplikovány postupy pro dosažení stanovených cílů. Nedílnou součástí je metodika, která sice nepatří do metodologie vědy, ale bývá s touto vědou a jejími pojmy spojována. Metodika je postup, na jehož základě jsou stanoveny metody, pomocí kterých je realizována výzkumná práce. Metodický postup lze zobrazit s využitím vývojových diagramů např. BPMN (Ochrana, 2009). Tato kapitola práce je zpracována v souladu s metodickým postupem, který je popsán v kapitole 1.

Na základě provedené rešeršní strategie, stanovených cílů a metodologického postupu byly navrženy vhodné metody pro přípravu nových bezpečnostních standardů a nových právních předpisů. Struktura kapitoly je rozdělena do dílčích podkapitol, které systematicky navazují na řešenou problematiku, stanovené cíle a metodologický postup. Nejprve je rozpracován proces přípravy nových právních předpisů v ČR a EU, ověřen skutečný stav u zvolených organizací, dále jsou navrženy metody a v závěru této kapitoly jsou provedeny validace, zhodnocení a jsou definovány přínosy práce.

5.1 Proces přípravy nových právních předpisů

V této dílčí podkapitole je rozpracován proces přípravy nových právních předpisů, jejichž zpracování lze aplikovat na proces přípravy nových bezpečnostních standardů. Pro nalezení konsensu mezi navrženými metodami je nutné blíže tento proces specifikovat, aby čtenář pochopil základní části celého procesu přípravy, aniž by musel mít odpovídající odborné právní vzdělání. Tato podkapitola rozpracovává proces přípravy nových právních předpisů, avšak výklad právních předpisů není v této podkapitole ani jiných kapitolách aplikován. Práce svým zaměřením nezkoumá právní předpisy a jejich význam.

Legislativní proces je v České republice upraven ústavními zákony, zejména Ústavou ČR (Ústavní zákon č. 1/1993 Sb.), a je definován jako zákonodárný proces.

Zákonodárná činnost je základní funkcí Parlamentu a podle čl. 15 Ústavy náleží výhradně Parlamentu (Pavlíček & Kolektiv autorů, 2011). Zákonodárný proces lze rozdělit na několik stadií (Klíma, 2010):

- zákonodárná iniciativa,
- první čtení zákona,
- druhé čtení zákona,
- třetí čtení zákona, schválení zákona,
- zaslání zákona Senátu (případně nové projednání vráceného zákona),
- zaslání zákona prezidentu republiky (případně nové projednání vráceného zákona),
- vyhlášení zákona.

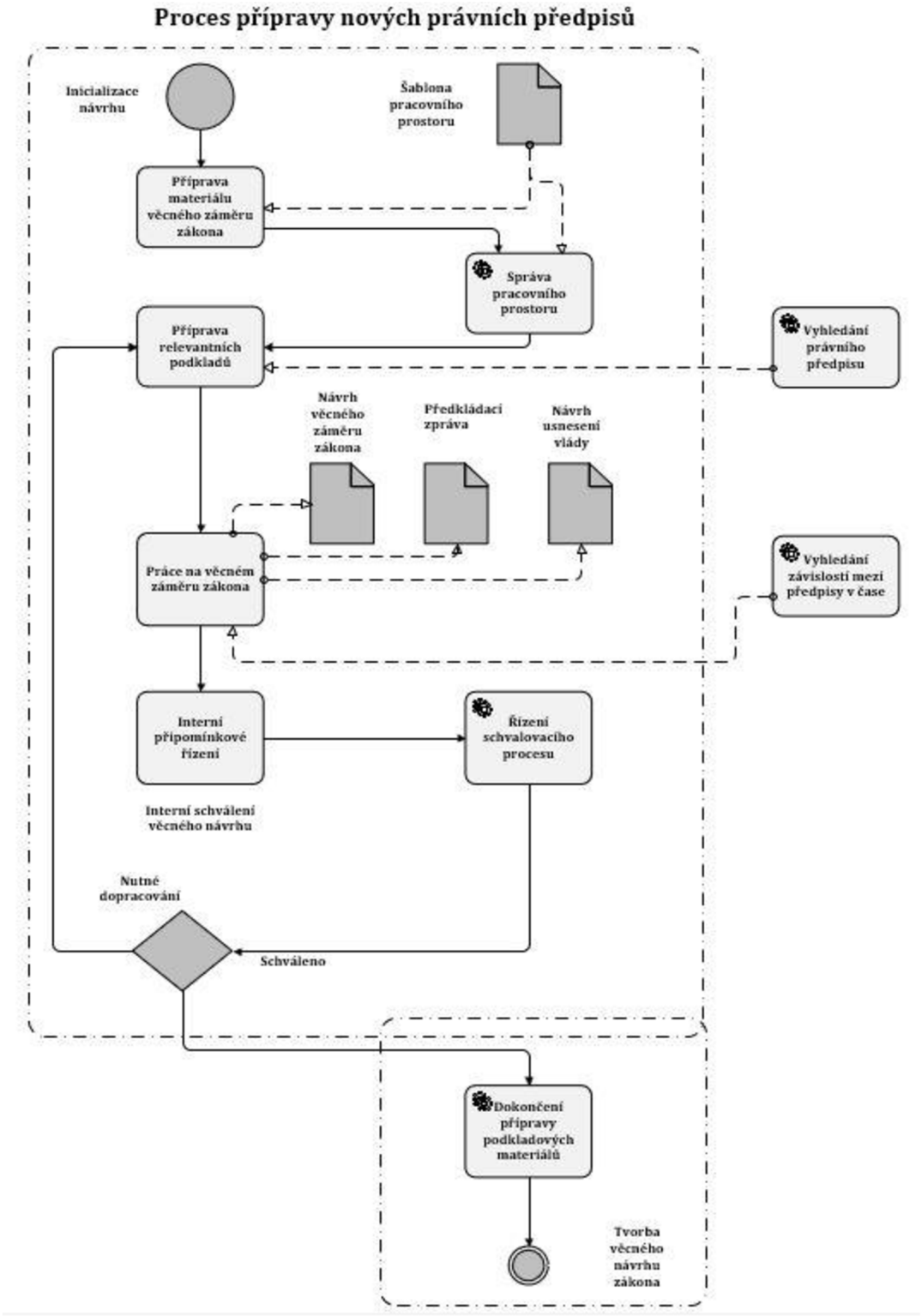
Na úrovni vlády jsou tvořeny právní předpisy ministerstvy a jinými ústředními orgány státní správy (předkladatelé). Při přípravě právních předpisů musí jejich předkladatelé postupovat v souladu s legislativními pravidly vlády, která upravují požadavky na obsah a formu připravované legislativy („Zákonodárný proces v Česku", 2022). Dalšími předkladateli návrhu zákonů mohou být podle čl. 41 odst. 2 Ústavy poslanec, skupina poslanců, Senát, vláda nebo zastupitelstvo vyššího územního samosprávného celku (Pavlíček & Kolektiv autorů, 2011).

Z hlediska zákonodárné iniciativy a celkového legislativního procesu je pro tuto práci důležitá část, která je zaměřena na přípravu materiálu návrhu zákona a dalších souvisejících činností. Pro prvotní přípravu nových právních předpisů či metodických doporučení jsou využívány kancelářské aplikace, zejména MS Office. Celý proces přípravy a následné připomínkování prvotních návrhů probíhá s využitím ruční editace při pracovních jednáních. Tato prvotní přípravná část se tak stává zdlouhavou, neefektivní a nepřehlednou. Trendem současnosti je využívání cloudových služeb, které jsou poskytovány v souvislosti s přípravou návrhu zákona, avšak opět za využití kancelářských aplikací s ruční editací připomínek při jednání pracovních skupin.

Metodické pokyny pro přípravu právních předpisů jsou v ČR vydávány Úřadem vlády ČR, který je zveřejňuje na svých webových stránkách. Proces přípravy návrhů právních předpisů je upraven v praktické příručce (Kněžínek et al., 2010) a navazuje na metodické pomůcky pro přípravu návrhů právních předpisů, rozdělenou do tří samostatných částí, které byly vypracovány autorským kolektivem Odboru vládní legislativy Úřadu vlády České republiky pod vedením Josefa Vedrala v roce 2006 (Vedral, 2006). Součástí zákonodárného procesu v rámci přípravy zákona je proces pro

hodnocení dopadů regulace, anglicky *Regulatory Impact Assessment* (RIA). Tento proces je souborem dílčích etap, jejichž cílem je hodnocení očekávaných dopadů navrhovaných právních předpisů. V České republice je RIA uplatňována u všech obecně závazných právních předpisů připravovaných ministerstvy a ostatními ústředními správními úřady podle legislativních pravidel vlády, a to včetně implementace práva EU. Při zpracování RIA úřady postupují podle vládou schválených obecných zásad pro hodnocení dopadů regulace. Základním cílem RIA je tedy zvýšení kvality právních předpisů a samozřejmě i celé jejich tvorby i na úrovni EU (*Co je hodnocení dopadů regulace | ria.vlada.cz*, 2022). Metodika pro RIA je detailně zpracována a členěna do dvou částí: Procesní pravidla a Metodika pro hodnocení dopadů regulace.

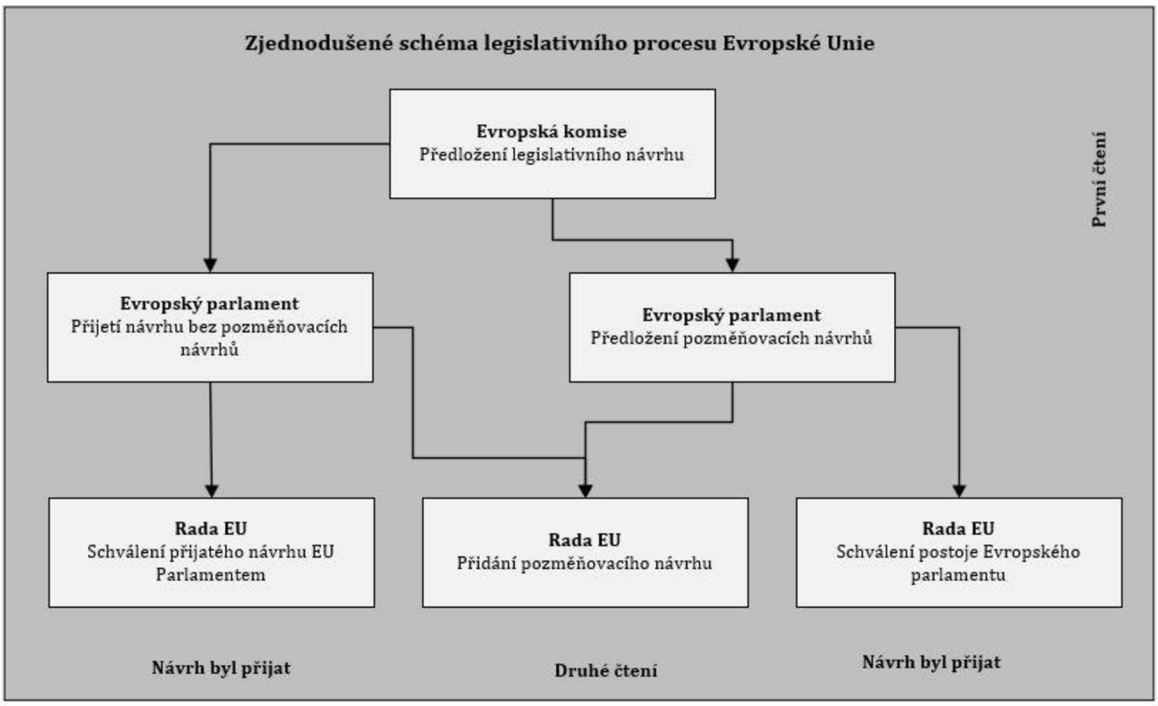
Proces tvorby návrhu, přípravy a přijetí nových legislativních předpisů jsou velmi dobře zpracovány na národní úrovni, avšak informace zaměřené na samotnou přípravu materiálů s využitím informačních technologií např. s odpovídajícím softwarem nejsou nikde obsaženy. Proces přípravy pro návrh zákona je zobrazen prostřednictvím modelu BMPN 2. Z výše uvedeného grafického schématu je relevantní pouze část související s přípravou materiálu a relevantních podkladů.



Model BPMN 2 Proces přípravy nových právních předpisů

Zdroj: Kolektiv autorů MVČR, 2018, vlastní přepracování

Legislativní proces na úrovni EU je ve velmi zjednodušeném schématu zobrazen na obrázku 6, schéma detailního procesu je přiloženo v příloze 4.



Obrázek 6 Schéma legislativního procesu EU

Zdroj: Schreiberová, 2022, vlastní přepracování

Nejvýznamnější institucí v ČR, která se specializuje na vydávání norem, je Úřad pro normalizaci, metrologii a státní zkušebnictví. Tato organizace spolupracuje a podílí se na tvorbě i mezinárodních norem v rámci spolupráce s dalšími zahraničními organizacemi. Metodiky či praktické metodické pomůcky pro přípravu dokumentů ze strany UNMZ nejsou však pro veřejnost dostupné.

Podpora zlepšování správy a řízení v zemích střední a východní Evropy (program SIGMA) je společnou iniciativou Organisation for Economic Co-operation and Development (OECD) pro podporu iniciativy s cílem zvyšování digitalizace veřejné správy. V rámci programu SIGMA byl zpracován dokument řešící problematiku přípravy právních předpisů a regulačních nařízení ve střední a východní Evropě (Checklist on Law Drafting and Regulatory Management in Central and Eastern Europe, 1997).

Příprava prvotních návrhů nových legislativních norem a bezpečnostních standardů by měla být založena na využití prvků a procesů z oblasti informačního managementu. Samotná příprava nových návrhů legislativních norem a bezpečnostních standardů by měla obsahovat dílčí procesy:

- sběr informací,
- analýzu prvotních informací,
- zpracovávání a vyhodnocení informací,
- návrh a řízení procesů při přípravě nových zákonů,
- konzultace s odbornou veřejností,
- schvalování zákona.

Proces sběru informací by měl zahrnovat výběr vhodných dokumentů např. informace o aktuální legislativě, o praxi, o potřebách a názorech veřejnosti. Důležité je zajistit, aby informace byly získány z důvěryhodných zdrojů a aby byly získané informace správně interpretovány. Výběr vhodných dokumentů pomocí procesu sběru informací je nezbytnou a prvotní částí celého procesu přípravy.

V rámci procesu analýzy informací by měla být provedena analýza a vyhodnocení získaných informací s cílem identifikovat problémy a potřeby, na jejichž základě bude proces přípravy zahájen. Neopomenutelnou podmínkou je zajištění kvalitního zpracování získaných informací. Proces analýzy informací je možné využít v souvislosti s RIA, kde jsou prostřednictvím povinného vyhotovení RIA k návrhu nových právních předpisů analyzovány dopady na subjekty veřejné správy, rozpočet aj. Pomocí procesu analýzy informací založeného na RIA jsou zhodnoceny dopady na cílové skupiny, výhody a nevýhody pro rozpočet či další skutečnosti.

Proces zpracování a vyhodnocování informací by měl zahrnovat zpracovávání výše uvedených procesů (sběr a analýza informací). V rámci procesu zpracování informací z hlediska procesu přípravy jsou identifikovány (stanoveny) klíčové problémy a skutečnosti, které je nutno zahrnout do celkového procesu přípravy. Důležitou podmínkou je zajištění, aby kvalitně zpracované informace byly vhodně využity při procesu přípravy.

Návrh a řízení procesů v procesu přípravy by měl probíhat na základě získaných informací, které byly vhodně aplikovány v souladu s ostatní platnou legislativou.

Konzultace s odbornou veřejností by měla probíhat za účelem zapojení i odborníků z jiných odvětví. Tato dílčí podčást procesu přípravy ve formě odborných konzultací přináší do procesu přípravy zapojení širšího okruhu veřejné odbornosti, což má za následek kvalitnější zpracovávání připravovaných návrhů.

Je důležité si uvědomit, že proces přípravy materiálů a relevantních podkladů v rámci zákonodárného procesu a proces přípravy metodických doporučení, standardů a norem zahrnují velmi podobné procesy a činnosti. Na základě toho lze konstatovat,

že proces přípravy materiálů a relevantních podkladů v rámci zákonodárného procesu a proces přípravy metodických doporučení, standardů a norem zahrnují velmi podobné procesy a činnosti. A právě tento přípravný proces je zdlouhavý, neefektivní a je vhodné ho zautomatizovat a zefektivnit pomocí vhodných metod s případným využitím odpovídajícího softwaru. Při těchto procesech je tedy nutné využívat podobné postupy a postavit je na pevné metodice.

5.2 Ověření skutečného stavu

Na předchozí dílčí podkapitolu, ve které byla charakterizována a popsána specifika přípravy nových právních předpisů, navazuje tato podkapitola, jež rozpracovává část zaměřenou na zjištění skutečného stavu. Skutečný stav procesu přípravy byl ověřován v rámci stanovených organizací tak, aby bylo dodrženo základní organizační uspořádání veřejné správy a státních institucí. Pro ověření skutečného stavu byly zvoleny organizace z hlediska hierarchického uspořádání:

- Vyšší územní samosprávný celek (kraj) – Krajský úřad Pardubického kraje.
- Ústřední správní úřad – Národní úřad pro informační a kybernetickou bezpečnost.
- Ministerstvo – Ministerstvo vnitra České republiky.
- Soukromý subjekt – Soukromá advokátní kancelář Císař, Češka, Smutný, s. r. o.

Pro sběr dat byly využity metody:

- neformální rozhovor,
- písemné dotazování.

Provedení sběru dat bylo zaměřeno na zjišťování skutečného stavu u všech zvolených organizací: Krajský úřad Pardubického kraje, NÚKIB, soukromá advokátní kancelář Císař, Češka, Smutný, s. r. o., MV ČR. Byly formulovány vhodné otázky, na základě kterých byla získána relevantní vstupní data.

Písemnou formou byl osloven Krajský úřad Pardubického kraje, který má dle zákona o krajích kompetence pro podávání návrhů nových právních předpisů. Krajský úřad byl osloven prostřednictvím žádosti podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím prostřednictvím datové schránky. Odpověď ze strany Krajského úřadu Pardubického kraje byla zpracována Oddělením legislativní podpory a zaslána do datové schránky. Tato žádost včetně vyjádření je přiložena v příloze 1 a 2.

Formou neformálního rozhovoru byl v průběhu ledna 2024 osloven Národní úřad pro informační a kybernetickou bezpečnost. Na základě osobní schůzky proběhlo

setkání se zaměstnancem úřadu, se kterým byl proveden rozhovor formou otevřeného neformálního rozhovoru na základě stanovených otázek.

Dále byl skutečný stav potvrzen na základě vlastní zkušenosti, kdy autorka byla již dříve součástí pracovní skupiny, která se podílela na přípravě cloudové vyhlášky, již NÚKIB připravoval.

Formou písemné komunikace byla oslovena soukromá advokátní kancelář Císař, Češka, Smutný, s. r. o., jejíž odpověď je přiložena v příloze 3.

Pro zjištění skutečného a aktuální stavu byly položeny otázky:

1) V souvislosti s prvotní přípravou nových legislativních norem Vás žádám o poskytnutí informací v podobě popisu postupu (procesu), jakým způsobem tato prvotní příprava probíhá a jaké činnosti (aktivity) jsou ze strany zaměstnanců vaší organizace realizovány a s využitím jakého softwaru?

2) Při přípravě návrhu nových legislativních norem jsou využívány i prostředky informačních technologií, zejména software (dále SW). Jaký typ SW je využíván ze strany vašich zaměstnanců (např. textový editor, software pro sdílení dat), můžete sdělit přesný název využívaného softwaru?

3) Jaké jsou průměrná doba a počet zaměstnanců, jež jsou obvykle průměrně vynaloženy v rámci odborných konzultací při jednání ve formě on-line nebo s osobní účastí nad připravovanou novou legislativní normou, tj. před započetím samotné přípravy návrhu nové legislativní normy ze strany vašich zaměstnanců s využitím softwaru?

4) Jakým způsobem probíhá ve vaší organizaci při přípravě návrhů nových legislativních norem zavádění inovací pro zvyšování efektivity, čímž dochází současně ke snižování vynaloženého času a současně ke snižování celkových finančních nákladů? Je tato problematika řešena nebo nikoliv, či případně plánuje se zavádění inovací při náplni této pracovní činnosti, a pokud ano, v jakém časovém období a jaké inovace plánujete implementovat, v jakém časovém období, na základě jaké metody bude provedeno zhodnocení implementovaných inovací?

5) V rámci zavádění inovací jsou ve vaší organizaci využívány frameworky z oblasti informačního a znalostního managementu např. IT Governance, Enterprise Information Management či jiné?

Vyhodnocení získaných dat proběhlo metodou analytické indukce a triangulace.

Vyhodnocení odpovědí ze strany Krajského úřadu Pardubického kraje

Na základě písemné odpovědi, která je přiložena v příloze 2, byly poskytnuty informace, které nelze detailně přiřadit ke konkrétním otázkám, poněvadž odpověď byla strukturována souhrnně v obecnější rovině. Nicméně ze zaslaného vyjádření je zřejmé, že:

Pro zpracovávání návrhů pro nové právní předpisy je využíván standardní kancelářský balík MS Office, zejména Word, Excel, a dále, že pro schůzky je využíván MS Teams. Z hlediska vyčíslení času nebylo možné tuto skutečnost sdělit, poněvadž se nejedná o formalizovaný proces, každý návrh je řešen individuálně z hlediska přípravy, projednávání v rámci konzultací s jinými subjekty, dále na základě složitosti přípravy a celkového zpracování. V dodatečné emailové komunikaci byl vyjádřen zájem o řešení této problematiky v budoucnu např. v rámci další spolupráce.

Vyhodnocení odpovědí na základě poskytnutého rozhovoru se zaměstnancem NÚKIB

Rozhovor se zaměstnancem ústředního správního úřadu NÚKIB probíhal formou otevřeného rozhovoru, ve kterém byly představeny řešený problém, jeho úskalí, zjištěné skutečnosti řešené problematiky na národní a mezinárodní úrovni na základě analýzy odborné literatury.

V rámci rozhovoru byly poskytnuty informace, že tuto problematiku úřad zkoušel řešit v souvislosti s transpozicí směrnice NIS2, kdy bylo nutné přistoupit k vytvoření zcela nového návrhu zákona o kybernetické bezpečnosti. Pro návrh byla využita demoverze softwaru (název nebyl sdělen), který se dle sdělených informací neověřil jako zcela vhodný nástroj pro řešení této problematiky. Současně bylo poukázáno na to, že tato problematika by měla být v budoucnu řešena i v návaznosti na proces přípravy evropských právních předpisů.

Proces přípravy návrhu nových právních předpisů je taktéž připravován, a to především na základě využívání standardních kancelářských aplikací Word a Excel. Dále byl projeven zájem o další řešení této problematiky do budoucna. Na základě vlastních zkušeností autorky, která byla součástí pracovní skupiny pro přípravu cloudové vyhlášky, lze taktéž potvrdit, že je využíván zejména kancelářský balík MS Office pro přípravu a zpracovávání právních návrhů na tomto úřadu.

Vyhodnocení odpovědí na základě písemné formy ze strany soukromé advokátní kanceláře Císař, Čéška, Smutný, s. r. o.

Na základě poskytnutých informací ze strany soukromé advokátní kanceláře bylo sděleno, že není při samotné přípravě využíván žádný software mimo textových editorů (Word, LibreOffice aj.). V souvislosti s poskytnutím informací ohledně časové dotace pro vytvoření návrhu právní normy kancelář uvádí, že většinou je třeba časové dotace ve formě 1 manday. Stejnou odpověď kancelář poskytla v rámci dotazu ohledně poskytnutí průměrné časové dotace na pracovní jednání pro přípravu nového právního předpisu, také 1 manday. Efektivita není v rámci přípravy systematicky řešena, inovace jsou zaváděny průběžně, frameworky z oblasti informačního a znalostního managementu nejsou v organizaci implementovány. Písemné sdělení informací na základě položených otázek je přiloženo v příloze 3.

Vyhodnocení odpovědí na základě ústní formy u MV ČR

Ověření skutečného stavu u MV ČR bylo součástí procesu validace formou neformálního rozhovoru a je zpracováno v kapitole 5.5 Validace výsledků v rámci expertních skupin.

Na základě kritéria triangulace a kombinací metod byl zjištěn aktuální stav u organizací podílejících se na přípravě návrhů nových právních předpisů, kdy bylo zjištěno:

1) Formalizovaný postup – není stanoven ani implementován.
2) Využívaný software – MS Office, zejména Word, Excel, či MS Teams.
3) Průměrná časová dotace pro přípravu nového právního předpisu – nelze vyčíslit s ohledem na variabilitu a náročnost nových návrhů právních předpisů.
4) Zavádění inovací pro zvyšování efektivity – nebylo odpovězeno, lze se domnívat, že tato oblast není v dotazovaných organizacích řešena.
5) Využívání frameworků z oblasti informačního a znalostního managementu – nebylo odpovězeno nebo bylo sděleno, že nejsou využívány. Lze tedy konstatovat, že problematiku přípravy nových právních předpisů z hlediska využívání odpovídajících frameworků z oblasti IM a ZM se nikdo nezabýval.

Skutečný stav přípravy procesu nových právních předpisů byl ověřen u organizací podílejících se na procesu přípravy a současně byl aktuální stav analyzován v rámci zpracované rešeršní strategie v kapitole 3. Na základě provedeného šetření lze konstatovat, že skutečný stav byl dostatečně ověřen z hlediska různých oblastí, které navzájem souvisejí s procesem přípravy nových právních

předpisů a bezpečnostních standardů. Aktuální stav procesu přípravy je zdlouhavý, neefektivní, není založen na využívání inovativních prostředků informačních technologií ani na metodách z oblasti informačního a znalostního managementu a dalších vědních disciplín. Optimalizace a návrh vhodných metod, jež jsou rozpracovány v další dílčí podkapitole, budou přínosem pro tuto oblast s možnými pozitivními dopady v podobě budoucího rozvoje a případné formalizace prvotního procesu přípravy.

5.3 Metody pro přípravu nových bezpečnostních standardů a právních předpisů

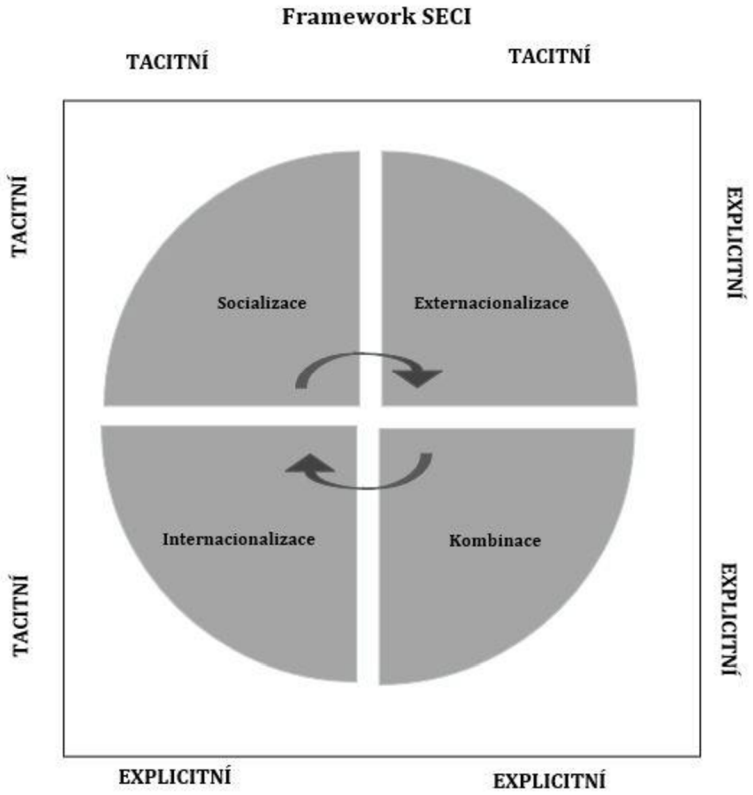
5.3.1 Metody z oblasti informačního a znalostního managementu

Pro zavádění inovací v rámci přípravy nových právních norem a bezpečnostních standardů pro zlepšení efektivity v organizaci bylo důležité zvolit vhodný přístup k řízení znalostí, který kombinuje různé aspekty a fáze životního cyklu znalostního managementu.

V rámci vhodných metod je vhodný zejména model Socialisaton, Externalisation, Internalisation a Combination (SECI), který vznikl na základě případových studií v Japonsku (Nonaka & Takeuchi, 1995).

5.3.1.1 Model SECI

Model SECI zdůrazňuje kontinuální transformaci znalostí s možnou podporou inovací a efektivity v organizaci. Model je využíván pro popis možných způsobů toho, jak mohou být znalosti v organizaci vytvářeny, přenášeny a znovu vytvářeny. Model zahrnuje čtyři fáze: Socializace (S), externalizace (E), kombinace (C) a internacionalizace (I). Transformace znalostí podle I. Nonaky zobrazuje obrázek 7 na další straně.



Obrázek 7 Framework SECI

Zdroj: Spomocnik.rvp.cz, 2016, vlastní přepracování

Model SECI je založen na tacitní a explicitní formě znalostí, kdy v rámci procesu integrace dochází prostřednictvím konverze k rozšiřování znalostí z hlediska kvality a kvantity (Bureš, 2007). Znalosti se po spirále pohybují v cyklech a oscilují mezi extrahovanými tacitními (vnitřními, osobními, nevyslovenými a neuchopitelnými) znalostmi jedince, ze kterých se stávají explicitní (veřejné, firemní, vyslovitelné a uchopitelné) znalosti, a naopak, explicitní znalosti jsou zpětně internalizovány (osobně zpracovávány) a stávají se z nich tacitní znalosti.

Konverze se označují jako socializace, externacionalizace, kombinace a internalizace a v rámci procesu šíření znalostí v kontextu prvotní přípravy nových právních norem či bezpečnostních standardů mohou konverze zahrnovat:

1. **Socializace** – z hlediska přípravy nových právních předpisů a bezpečnostních standardů tato fáze (konverze) může zahrnovat sdílení tacitních znalostí.

   „Tacitní znalosti jsou jinými slovy takové znalosti, které naplňují původní význam slovního spojení „know how“ na osobní niterní úrovni, kde se shromažďují dovednosti, které jsou založené na vlastní zkušenosti a na řadě cyklů pokus-omyl. U tacitních znalostí

také platí, že se může na první pohled jednat i o takové příklady, které bychom spíše zařadili do výčtu explicitních znalostí, avšak v takových případech je nutné rozlišovat mezi stroze předanou informací a informací, kterou její příjemce doopravdy přijme za svou a kterou po řadě pokusů a neúspěchů v praxi vnitřně zpracuje a konečně začne používat v rámci vlastních schopností.“ (Dvořák, 2013)

Tacitní znalosti v kontextu přípravy nových právních předpisů mohou zahrnovat organizování neformálních setkávání, workshopů a brainstormingových sezení, kde právníci, bezpečnostní experti a další zúčastněné strany mohou sdílet své zkušenosti, obavy a intuitivní pochopení související s novými předpisy nebo bezpečnostními otázkami. Dále pro využití různých případových studií a reálných scénářů k diskusi o minulých výzvách a úspěších, což může poskytnout cenné vhledy pro nové předpisy. Cílem této konverze je tedy sdílení znalostí v rámci konkrétních odborníků, kteří připravují nové právní předpisy a bezpečnostní standardy tak, aby došlo k efektivní vzájemné výměně odborných informací.

2. **Externalizace** pomocí tohoto procesu dochází k formulaci tacitních znalostí do znalostí explicitních. Explicitní znalosti jsou znalosti, které lze prakticky (formálně) vyjadřovat sdílet, formalizovat a systematicky uspořádávat. Převod tacitních znalostí na explicitní tedy znamená, že jsou znalosti artikulovány, zdokumentovány a sdíleny, což umožňuje jejich širší využívání.

   Z hlediska přípravy nových právních předpisů a nových bezpečnostních standardů dochází k převodu tacitních znalostí na explicitní v rámci rozpracování případové studie z právního prostředí, které mohou popisovat specifické situace nebo rozhodnutí, která byla učiněna. V rámci právní analýzy případových studií mohou být vytvořeny sady kritérií nebo analytické rámce, jež mohou být použity k hodnocení a porovnání různých návrhů právních předpisů. Na základě těchto případových studií a jejich rozboru může být vytvořen právními odborníky nový soubor směrnic či pokynů.
3. **Kombinace** – je proces, ve kterém dochází k přeměně explicitních znalostí do komplexnějších a systematických znalostí. Explicitní znalosti jsou postupně získávány prostřednictvím sběru dat v rámci interního a externího prostředí dané organizace tak, aby mohly být vhodně zpracovány v rámci životního cyklu výměny informací za účelem získání (formování) nových znalostí, které jsou následně rozšiřovány v rámci struktury organizace (sekce, odbory, oddělení).

Z hlediska přípravy nových právních předpisů a bezpečnostních standardů mohou být v rámci fáze konverze využity různé metody pro zpracování dat např. v podobě analýzy, syntézy, dedukce či jiných kvalitativních a kvantitativních výzkumných metod.

4. **Internalizace** je typ konverze, kdy dochází v rámci procesu k převodu explicitních znalostí do tacitních. Díky procesu internalizace jsou explicitní znalosti sdíleny v rámci organizace a jednotlivci konvertovány na tacitní znalosti (Bureš, 2007). Tento typ konverze lze přiřadit také k učící se organizaci, kdy získané znalosti jsou na základě učení převáděny do praxe, a po převodu do praxe jsou dále rozšiřovány a aktualizovány na základě aktuálních trendů. V návaznosti na proces přípravy nových právních předpisů a bezpečnostních standardů bude tato fáze konverze zaměřena na uplatňování získaných znalostí v praxi v rámci dané organizace, aby získané znalosti byly efektivně implementovány a využívány. Tedy tak, aby celkový proces přípravy nových právních předpisů a bezpečnostních standardů byl využíván na základě získaných nových znalostí v souvislosti s inovovanými procesy a postupy, případně s novým odpovídajícím softwarem.

Management znalostí a jeho metody jsou tedy velmi důležitou součástí při zavádění inovací do organizací nejen v rámci přípravy nových právních předpisů a bezpečnostních standardů, ale i v rámci jiných činností, do kterých se zavádějí další inovace. Při zavádění inovací při procesu přípravy nových právních předpisů a bezpečnostních standardů nelze vynechat i související vědní disciplíny, protože proces přípravy by byl neefektivní, nesourodý či nekomplexní a systematicky by nenavazoval na další vědní obory, které jsou důležité z hlediska zavádění inovací.

Obdobný postup může být realizován v rámci přípravy bezpečnostních standardů pro IoT ve Smart Cities.

5.3.1.2 IT Governance

Nejvhodnější metodou z hlediska řízení přístupu k informacím, řízení toků informací, k podpoře a rozvoji strategických cílů a k celkovému informačnímu procesu může být Information Governance.

IT Governance byl jako termín uveden v roce 2004, avšak přesný termín nebyl definován (Weill & Ross, 2004). Byl vytvořen v rámci rozvoje COBIT 3.0 v kontextu IT auditu (Harmer, 2014).

IT Governance je konceptuální model, který se zabývá správou informací organizace a zahrnuje řízení informačních toků, řízení přístupu k informacím, řízení metadat, řízení záznamů a dalších aspektů správy informací. Cílem IG je zajistit, aby

informace byly dostupné, spolehlivé, bezpečné, aby byly využívány k dosažení podnikových cílů a podporovaly procesy rozhodování na základě důvěryhodných informací (Říhová, 2018).

IT Governance se tedy zaměřuje na vytváření hodnot prostřednictvím informačních technologií, zajištění řízení rizik spojených s informačními technologiemi a zajištění souladu s právními předpisy a standardy. Rámec je klíčový pro všechny organizace, které chtějí zajistit, aby jejich investice do prostředků informačních technologií přinesly očekávané výsledky.

IT Governance může být současně i významným faktorem pro úspěšnou přípravu zákonů, protože umožňuje organizaci efektivněji a bezpečněji spravovat informace v průběhu celého procesu tvorby zákona. IT Governance tedy poskytuje holistický přístup ke správě a řízení informací k organizaci.

IT Governance se člení na tři části (De Haes & van grembergen, 2009):

- Část IT Governance struktur – organizační jednotky s vlastními pravomocemi, odpovědností, jež se vztahují k IT (sekce, odbory, oddělení).
- Část IT Governance procesů – je část vztahující se k plánování, provozu, investicím, rizikům aj. v oblasti IT.
- Část IT Governance relačních mechanismů – je část vztahující se k aktivní spolupráci představitelů organizace v oblasti IT.

Klíčové aspekty IG zahrnují především:

1. Strategické plánování informací – zahrnuje především definování cílů a priorit v oblasti informační správy, vytváření politik a postupů, které budou informační správu řídit a zajišťovat zdroje pro implementaci těchto politik a postupů.

Z hlediska procesu prvotní přípravy nových právních předpisů a bezpečnostních standardů může tento klíčový aspekt zahrnovat:

- Definování cílů a priorit – stanovuje cíle pro správu informací, které jsou v souladu s cíli nových právních předpisů nebo bezpečnostních standardů.
- Vytváření politik a postupů – vypracovává politiky a postupy pro správu informací, které zahrnují požadavky nových právních předpisů a bezpečnostních standardů např. vytvoření politiky pro správu osobních údajů.
- Zajištění zdrojů – alokuje zdroje včetně financí a lidských zdrojů pro implementaci politik a postupů.

2. Správa dat – zahrnuje definici a implementaci standardů pro řízení a ochranu dat včetně zpracování, ukládání a sdílení dat, správu metadat. Z hlediska přípravy nových právních předpisů a bezpečnostních standardů tento klíčový aspekt zahrnuje:

- Definice a implementace standardů – stanovuje standardy pro řízení a ochranu dat, které jsou v souladu s novými právními předpisy, např. implementace standardů pro šifrování dat.
- Správa metadat – vytváří správu metadat, která popisují data, jejich zdroje, formát a také využívání dat.

3. Ochrana informací – zahrnuje zajišťování bezpečnosti a ochrany informací včetně správy přístupových práv a oprávnění, řízení rizik v oblasti informační bezpečnosti a plánování zálohování a obnovy dat.

Ochrana informací zahrnuje zejména procesy:

- Správa přístupových práv a oprávnění – zajišťuje přístup autorizovaným osobám, jež mají přístup k citlivým informacím.
- Řízení rizik v oblasti informační bezpečnosti – identifikuje a hodnotí rizika spojená s informačními aktivy a zajišťuje implementaci opatření pro jejich minimalizaci.
- Plánování zálohování a obnovy dat – proces je využíván pro vytváření a testování plánů pro zálohování a obnovu dat a pro případ poruchy nebo bezpečnostního incidentu.

4. Archivace a uchovávání informací – zahrnuje implementaci procesů pro uchovávání a archivaci informací, zpracování a klasifikaci dokumentů, stanovení doby uchovávání a řízení životního cyklu informací.

Zahrnuje především procesy:

- Implementace procesů pro uchovávání a archivaci – zahrnuje zavádění procesů pro správné uchovávání a archivaci informací včetně klasifikace dokumentů a stanovení doby uchovávání.
- Řízení životního cyklu informací – obsahuje správu životního cyklu informací od jejich vytvoření až po likvidaci.

5. Správa informačních technologií – zahrnuje řízení informační infrastruktury a aplikací včetně správy softwaru a hardwaru, zajišťování bezpečnosti infrastruktury a řízení nákladů v oblasti informačních technologií.

Zahrnuje zejména procesy:

- Řízení informační infrastruktury a aplikací – proces zajišťuje, že informační infrastruktura a aplikace jsou bezpečné, spolehlivé a schopné podporovat nové právní předpisy a bezpečnostní standardy.
- Zajištění bezpečnosti informační infrastruktury – zavádí implementaci opatření pro ochranu informační infrastruktury včetně firewallů, antivirových programů a dalších bezpečnostních nástrojů.
- Řízení nákladů v oblasti informačních technologií – zahrnuje monitorování a optimalizaci nákladů spojených s IT tak, aby byly v souladu s rozpočtem.

6. Řízení rizik – zahrnuje definici a implementaci procesů pro identifikaci, hodnocení a řízení rizik v oblasti informační správy včetně plánování a implementace opatření k minimalizaci rizik a řízení incidentů.

Může zahrnovat procesy:

- Definice a implementace procesů pro identifikaci rizik – pravidelné hodnocení rizik spojených s informační správou a implementace procesů pro jejich identifikaci a hodnocení.
- Plánování a implementace opatření k minimalizaci rizik – vytváření plánů pro řízení a minimalizaci identifikovaných rizik včetně plánů pro řízení incidentů a nouzového plánování.
- Řízení incidentů – zavádění procesů pro rychlou a efektivní reakci na bezpečnostní incidenty včetně incidentů souvisejících s utajovanými informacemi podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

IT Governance je využíván i v souvislosti s dalšími frameworky COBIT, ITIL, ISO/IEC 2700x a dalšími. Pro řešení výzkumného úkolu v rámci tématu disertační práce je využití uvedených frameworků nerelevantní, poněvadž souvisejí s informační bezpečností v organizaci.

Příprava nových právních předpisů a bezpečnostních standardů zavádí inovativní prvky do organizací, které se podílejí na této činnosti, a metody z oblasti ZN a IM jsou nezbytnou součástí inovačního procesu nejen v souvislosti s informačními technologiemi. Neméně důležitou část zaujímají i ekonomické vědy, které vhodně doplňují proces pro zavádění inovací v organizaci zejména z pohledu vynaložených nákladů.

5.3.1.3 Kontext ekonomických věd v návaznosti na řešené téma

Oblast ekonomických věd zahrnuje mnoho vědních disciplín čerpajících z makroekonomie a mikroekonomie. Pro řešený problém je však významné hledisko efektivity, hospodárnosti a účelnosti při zavádění inovací v rámci procesu přípravy nových právních norem a nových bezpečnostních standardů v organizaci. Z hlediska nedostatečných informací pro vyčíslení ekonomických nákladů při procesu přípravy nových právních předpisů a nových bezpečnostních standardů, kdy oslovené organizace nemají implementované vhodné metody, interní procesy ani formalizovaný postup, na základě kterého by bylo možné vyčíslit průměrné náklady, byl využit ekonomický princip (pravidlo) pro hodnocení efektivity, účelnosti a hospodárnosti. Toto pravidlo je zakotveno i v právních předpisech a metodických příručkách platných v České republice a označuje se jako 3E.

Průměrný čas a počet osob podílející se na přípravě nových právních předpisů nelze z hlediska nákladů vyčíslit, poněvadž nové právní předpisy se připravují v nesourodém pracovním kolektivu při odborných konzultacích v rámci úřadů, organizací a odborníků. Pro svou práci využívají standardní kancelářské aplikace MS Office. Inovativní software pro sdílení dat v cloudových úložištích není využíván, dále nejsou využívány ani jiné automatizované IS, které by celý proces přípravy urychlovaly. Na základě ručního zpracovávání dochází k vytížení a zvyšování personálních kapacit, čímž dochází i k celkovému nárůstu finančních nákladů v organizacích. Proces přípravy se tak stává zdlouhavým, časově náročným a neefektivním.

Ekonomický kontext v návaznosti na řešený problém v souvislosti s výše uvedenými metodami z oblasti IM a ZM je rozpracován v návaznosti právě na pravidlo 3E. Pravidlo 3E stanovuje tzv. zásady řádného finančního hospodaření neboli hospodárnost, efektivnost a účelnost a je definováno zákonem č. 320/2001 Sb., o finanční kontrole (Zákon č. 320/2001 Sb., Zákon o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), b.r.). Současně je toto pravidlo upraveno v metodické příručce s názvem „Povinnost aplikace principů 3E při hospodaření územních samosprávných celků“ (Kolektiv autorů, 2022)

„Obecně je uznáváno, že daleko příznivější prostředí pro aplikaci těchto zásad existuje v územní samosprávě (zabezpečující mimo jiné relativně měřitelné veřejné služby) než ve státní sféře. Důvodová zpráva k výše uvedenému zákonu obsahuje charakteristiku

užívaných pojmů. Daleko složitější je problematika kvantifikace účinnosti ve veřejném sektoru.“ (Stříteská, 2008)

Pravidla rozpracovává i publikace Františka Ochrany, který se zaměřil na to, zdali organizace pracuje účinně v kontextu otázek účelnosti, stanovených cílů a působností dané organizace. Při stanovení účinnosti se zaměřuje na odpověď, nakolik jsou danými výstupy naplňovány cíle zvolené organizace. Mezi účinností a efektivností existuje vztah nepřímé úměry, hlavním cílem je tedy dosažení určité rovnováhy mezi nimi (Stříteská, 2008). Princip 3E a jeho pravidla jsou rozpracovány v důvodové zprávě k zákonu č. 320/2001 Sb., o finanční kontrole, a dále v § 2 téhož zákona.

Pravidla dle P. Vyleťala (Vyleťal, 2014) jsou definována jako:

Správnost, anglicky *Accuracy,* lze definovat jako soulad s právními předpisy pro dosažení optimálního vztahu mezi hospodárností, účelností a efektivností. Správnost lze charakterizovat jako míru přesnosti, tedy rozdílu jednoho výsledku a referenční (očekávané) hodnoty, jež bývá popsána zjištěnou chybou.

Hospodárnost, anglicky *Economy,* je využívání veřejných prostředků pro zajištění stanovených úkolů, kdy dochází k co nejnižšímu vynakládání veřejných prostředků, zejména finančních, při současném dodržení odpovídající kvality plněných úkolů. Za hospodárnou činnost lze tedy považovat činnost, u které jsou minimalizovány náklady na zdroje (lidské, finanční, věcné) při současném dodržení požadované kvality zdrojů z hlediska potřeb dané činnosti. Princip hospodárnosti je založen na tom, aby zdroje, které byly využity danou organizací při provádění konkrétních činností, byly využitelné ve správný čas, v dostatečném množství a v přiměřené kvalitě za odpovídající (přiměřenou) cenu.

Efektivnost, anglicky *Effectiveness,* je chápána jako využívání veřejných prostředků, pomocí kterých je dosahováno nejvyššího možného rozsahu, kvality a přínosu stanovených úkolů v kontextu srovnání s objemem vynaložených prostředků (nákladů) na jejich splnění. Efektivní je taková činnost, která optimalizuje využívání zdrojů organizace k tvorbě výstupů, tj. dosažení maximálního výstupu z daných zdrojů či dosažení daného výstupu s minimem zdrojů a při zachování kvality výstupů. Princip efektivnosti vyžaduje dosažení co nejlepšího vztahu mezi zdroji použitými pro danou činnost a dosaženými účinky, a to jak z pohledu jednotlivé činnosti, tak i z pohledu věcně souvisejících činností projektů (tj. trvale dosahovaná efektivnost).

Další definice principu 3E je možné nalézt v různých standardech či normách řešících oblast auditů či v jiných právních předpisech národních nebo mezinárodních

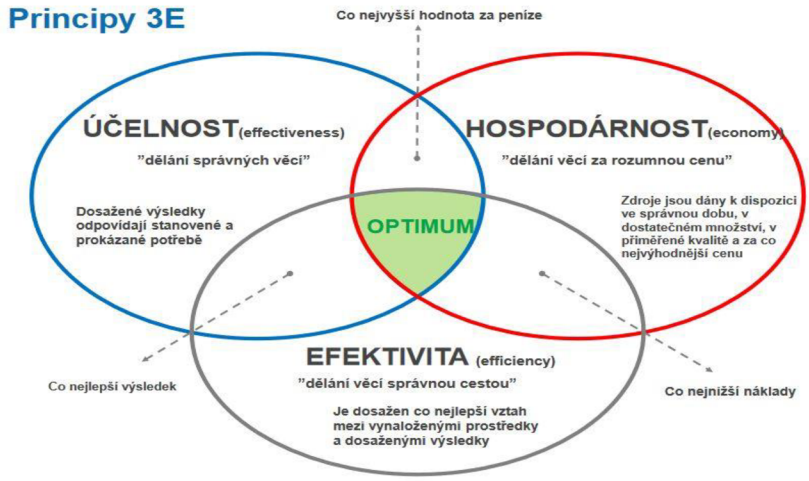
(EU). Důležitým aspektem pro vyhodnocování vstupů a výstupů z procesu, který řeší princip 3E, je schopnost pracovat s konkrétními hodnotami.

Dle Vyleťala (2014) každá hodnota, se kterou je třeba pracovat v ekonomickém prostředí, si nese s sebou následující atributy:

- Pojmenováním hodnoty je chápán konkrétní užitek např. myšlenky, služby, výrobku, tedy to, co je pro řešenou činnost důležité. Standardním příkladem může být zavádění digitálního a automatizovaného IS pro správu a sledování legislativních návrhů s cílem zvýšení transparentnosti a sledovatelnosti celého legislativního procesu s efektivním zapojením všech zúčastněných stran např. Elektronické knihovny legislativního procesu (eKLEP).
- Ekonomickým vyjádřením hodnoty se rozumí stav hodnoty, tedy její ekonomické pojmenování, např. výdaj, příjem, náklad, zisk, ekonomické ukazatele, které lze vyjádřit v peněžních jednotkách. Standardními příklady mohou být automatizovaný sběr dat a jednání pracovních skupin v rámci veřejných konzultací k návrhům nových právních předpisů nebo nových bezpečnostních standardů.
- Ekonomickým pojmenováním hodnoty může být chápáno snižování nákladů na využité personální zdroje potřebné pro manuální zpracování konzultací v rámci pracovních skupin. Standardním příkladem může být úspora v rámci zavádění automatizace, což vede k celkovým úsporám v rámci vynaložených nákladů na proces přípravy a pro zvýšení efektivity procesu.
- Identifikace hodnoty je stav hodnoty, který lze identifikovat různými aspekty např. technickými, právními aj., tedy aspekty, na základě kterých je ovlivněn konkrétní výběr. Standardním příkladem může být integrace IS nebo metodik sloužících pro nástroje pro analýzu dopadů nových právních předpisů např. RIA. Zavádění automatizovaných procesů s využitím IT nástrojů tak může efektivně umožnit komplexní analýzu dopadů, avšak i u RIA je nutno zdůraznit, že se využívá pro zpracování standardní kancelářský software MS Office, nikoliv automatizované a formalizované procesy (Vláda ČR, b.r.).
- Měření je stav hodnoty, který lze vyjádřit v měřitelných jednotkách, např. měna, hmotnost, velikost. Standardním příkladem může být implementace IS pro sledování a hodnocení efektivity při přípravě nových právních předpisů a bezpečnostních standardů s možností dalšího využití statistických dat např. v rámci kvantitativního výzkumu.

V rámci výše uvedených charakteristik dílčích atributů lze spatřovat souvislosti s hodnotami, které jsou využívány pro klasifikaci pravidel u principu 3E v kontextu inovací v procesu přípravy nových právních předpisů a nových bezpečnostních standardů tak, aby hodnota byla pojmenována, ekonomicky vyjádřena, identifikována a měřena.

Princip 3E zobrazuje obrázek 8.



Obrázek 8 Princip 3E
Zdroj: Ministerstvo financí ČE, 2019

Neméně důležitým aspektem je také to, že organizace, jež se podílejí na přípravě nových právních předpisů a nových bezpečnostních standardů, jsou převážně organizace patřící z hlediska členění do oblasti veřejné správy, ve které je princip 3E povinně také uplatňován dle platné legislativy. Organizace, jež spadají do oblastí veřejné a státní správy, hospodaří s veřejnými prostředky, které jsou do státního rozpočtu odváděny z daní obyvatel prostřednictvím přímých a nepřímých daní a dále na základě dalších zákonů o obcích, krajích. Odváděné finanční prostředky jsou přerozdělovány v rámci veřejných rozpočtů obcí, měst, krajů a dalších organizací hospodařících podle platných zákonů o hospodaření s veřejnými prostředky. Tyto organizace se nejvíce podílejí na zákonodárné tvorbě. Princip 3E lze považovat za odpovídající pro ekonomické posouzení zavádění inovací v rámci procesu přípravy nových právních předpisů a nových bezpečnostních standardů, a to i s ohledem na zjištěné a podložené zkušenosti, že celkové náklady na tuto činnost nelze na základě relevantních matematických metod vycházejících z ekonomických metod pro výpočet nákladů přesně vyčíslit.

5.3.1.4 Výhody a nevýhody SECI, IT Governance a 3E

Oblast IM a ZM včetně ekonomických věd může tedy přinášet do procesu přípravy nových právních předpisů a bezpečnostních standardů výhody, ale i nevýhody, které však mohou být v rámci konkrétních organizací odlišné. Každá organizace má jinou organizační strukturu, svou působnost, kompetence či řízení. Je tedy nutné, aby i kombinace zvolených metod a principů byla v případě implementace vhodným způsobem přizpůsobena dané organizaci. Základní výhody a nevýhody lze spatřovat v:

1. SECI (oblast ZM) – souvislost s inovací je možné spatřovat v rámci podpory sdílení, při tvorbě a aplikaci znalostí, kdy tyto aspekty jsou klíčové pro inovaci všech procesů.
   V kontextu prvotní přípravy nových právních předpisů a nových bezpečnostních standardů může SECI pomoci zachytit tacitní znalosti expertů, které následně převede na explicitní formu a integruje je do nových nebo revidovaných právních předpisů nebo bezpečnostních standardů.
   - Výhody – zlepšení kvality a významu právních předpisů a bezpečnostních standardů na základě integrace expertních znalostí včetně zvýšení inovačního potenciálu pro sdílení a kombinaci znalostí v rámci různých pracovních skupin.
   - Nevýhody – značné úsilí a zvýšené počáteční náklady při implementaci a dále při udržování nastavených procesů a metod znalostního managementu v organizacích.
2. IT Governance (oblast IM) – souvislost s inovací lze nalézt v rámci řízení procesů a metod v oblasti IT, kdy implementace IT Governance může efektivně zajistit soulad IS s celkovým řízením IT procesů v organizaci.
   V kontextu prvotní přípravy nových právních předpisů a bezpečnostních standardů napomůže implementace IT Governance celkovému zlepšení správy a sledování připravených dokumentů (nových právních předpisů a bezpečnostních standardů) a dále k sledování další spolupráce v rámci pracovních skupin.
   - Výhody – zajištění souladu s právními a regulačními požadavky a dále celkové zlepšení efektivity a transparentnosti procesů přípravy nových právních předpisů a nových bezpečnostních standardů.
   - Nevýhody – prvotní vysoké náklady na implementaci a udržování informační infrastruktury, procesů a metod, které zavádí IT Governance, a dále nutnost průběžného upgrade dle aktuálních trendů a právní regulace.

3. Princip 3E (ekonomické vědy) – v souvislosti s inovací lze nalézt u IT Governance v rámci efektivního fungování procesů a metod např. při implementaci prvků automatizace v rámci dané organizace.

   V kontextu prvotní přípravy nových právních předpisů a bezpečnostních standardů napomůže implementace IT Governance zefektivnit nastavené procesy pro správu dokumentů a sledování změn v rámci spolupráce.

   - Výhody – zlepšení efektivity a transparentnosti procesů přípravy nových právních předpisů a nových bezpečnostních standardů při využívání IT s prvky automatizace při snížení časového zatížení personálních kapacit včetně snížení osobních nákladů.
   - Nevýhody – vyšší náklady na implementaci a udržování informační infrastruktury a zavádění odpovídajících procesů a metod.

V rámci využití inovací a informačních technologií pomocí SECI byl proveden výzkum v oblasti pedagogických věd (Songkram & Chootongchai, 2020). SECI tedy rozvíjí vytváření znalostí v rámci interakcí uvnitř organizace a s jejími zainteresovanými stranami (Zhang & Huang, 2020). Současně narůstá tlak na rozšiřování strategií organizací ve veřejném sektoru v rámci zavádění nových přístupů IT Governance (Magnusson et al., 2020). Na základě vzrůstajících požadavků na zavádění nových přístupů IT Governance je nutno, aby byly propojeny kompetence v oblasti IT mezi odpovědnými osobami (Héroux & Fortin, 2018), což může přinášet různé typy problémů (Bagherzadeh et al., 2022) a rizik při zavádění inovací (Sandbrink et al., 2022).

Pro zlepšení procesu prvotní přípravy nových právních předpisů a nových bezpečnostních standardů je v současnosti nezbytným doplněním i využívání odpovídajících prostředků z oblasti informačních technologií, respektive využívání vhodného softwaru, který může zrychlit celkovou dobu procesu přípravy. Pro proces prvotní přípravy je však velmi důležité, aby byla provedena analýza platných právních norem a dalších souvisejících dokumentů. Tato analýza napomůže v celkovém procesu prvotní přípravy vygenerovat strukturu nového právního předpisu. Pro analýzu existujících právních předpisů jsou využívány metody pro zpracování textu např. obsahová analýza – kvantitativní nebo kvalitativní či kombinace obou metod nebo jiné odborné metody, která je využívána pro zpracovávání textu např. v rámci zkoumání historických dokumentů.

5.3.2 Metody pro zkoumání textů

Vhodnou metodou pro doplnění výše uvedených metod a principu 3E jsou metody pro zkoumání textu. Potvrzení vhodnosti výběru metody z exaktního hlediska lze doložit i publikovaným a přijatým článkem na zahraniční konferenci Mobiwis 2022 (Svecova, 2022).

Henry et al. (2022) zpracovali studii, ve které bylo za pomoci obsahové analýzy provedeno zkoumání účelu, obsahu a popularity mobilních aplikací. Funkce aplikací byly kategorizovány podle schématu kódování, které obsahovalo 16 kategorií. Aplikace byly zahrnuty do analýzy a byly popsány jako užitečné pro snížení používání pornografie a data byla extrahována z popisů aplikací v obchodě. Metriky, jako jsou počet uživatelských hodnocení, průměrné skóre hodnocení a počet instalací, byly analyzovány na základě jednotlivých funkcí.

Diddi & Lundy (2017) využili obsahovou analýzu pro zpracování tweetů během stanovené doby na téma rakovina prsu. Studie prokázala, že zatímco různé organizace sdílely na Twitteru hodnotný obsah související s rakovinou prsu, tak každá používala platformu sociálních médií jiným způsobem.

Cílem studie Abbaspour et al. (2018) byly identifikace a popis dílčích procesů strategického zpravodajství v analýze na organizační úrovni. Data byla shromážděna prohledáváním hlavních akademických a praktických knih, prací a časopisů v databázích Ebsco, Google Scholar a IranDoc v perštině a angličtině. Obsahovou analýzou bylo prozkoumáno devět tisíc stran textových dat. Výstupy z provedené studie poskytly užitečné informace pro implementaci strategického zpravodajského procesu vorganizacích a v závěru byla vyhodnocena efektivita využití metody.

Cílem studie Abdel-Razig et al. (2021) bylo analyzovat využívání skupinového chatu lékaře WhatsApp (WhatsApp LLC) během prvních měsíců pandemie COVID-19. Abdullah et al. (2022) obsahovou analýzu využili k prozkoumání podobností a rozdílů mezi 170 vybranými malajskými a singapurskými malými a středními podniky na základě pěti škál osobností u značky Aaker.

Abedini & Broujeni (2016) zkoumali pomocí obsahové analýzy dílčí pohledy na kreativitu pedagogů při vzdělávacím procesu na vysoké škole.

Schneider et al. (1992) využili analýzu obsahu pro analyzování obsahu stanovených témat v souvislosti s výzkumnými otázkami klimatických změn.

5.3.2.1 Kvalitativní obsahová analýza

Pro zpracování textu je využíváno více metod. Mezi nejvyužívanější metody patří obsahová analýza využívaná v rámci kvalitativního a kvantitativního výzkumu, dále diskurzní analýza či sémantická analýza.

Obsahová analýza je označována za synonymum k přesnějšímu názvu kvalitativní obsahová analýza či formální obsahová analýza. Obsahová analýza je chápána jako metoda objektivní, systematická, validní a reliabilní.

Předmětem obsahové analýzy je komunikace, která je předávána jako obraz, text či zvukový záznam. Obsahová analýza se dále dělí na konceptuální a relační analýzu (Svecova, 2022).

Hendl (2016) charakterizuje obsahovou analýzu jako metodu, v níž si autoři nejprve zvolí typy kategorií, u kterých je následně zjišťována četnost výskytu slov s využitím odpovídajících statistických metod.

Obsahovou analýzu lze také obecně definovat jako rozbor obsahu záznamu určité komunikace. Tato metoda byla vymezena pro analýzu textů či souboru textů. Hlavním cílem této metody, která vychází z tradic pozitivistické metodologie, je vyhledávání konkrétních slov a konceptů v analyzované komunikaci a stanovení četnosti jejich výskytu, významu a vzájemného vztahu (*Obsahová analýza | Katedra antropologie*, 2014).

Pomocí obsahové analýzy lze zkoumat text s ohledem na četnost vybraných znaků (písmen, slov, slovních spojení, jejich vzájemných vztahů a závislostí). Pro užší výběr zkoumaných znaků je využívána konceptuální obsahová analýza, pomocí které jsou zkoumány „koncepty“ – slova, fráze a frekvence jejich výskytu. Konceptuální analýzu je možné charakterizovat jako výzkumnou metodu, která je využívána ke kvantifikaci přítomnosti určitého znaku a také je využívána pro komparaci výskytu slov ve zkoumaném souboru. Konceptuální obsahová analýza se řadí z metodologického hlediska ke kvalitativnímu výzkumu (Svecova, 2022).

Obsahová analýza je spojována i s kvalitativním výzkumem a s relační obsahovou analýzou (označovanou také jako sémantická analýza). Relační analýza je zaměřena na výskyt konceptů (znaků) ve zkoumaném dokumentu, ale současně je zaměřena i na výzkum vztahů mezi zkoumanými koncepty (znaky, slovní spojení). Výsledkem relační analýzy jsou tzv. mentální modely, znaky, skupiny (Lombard et al., 2004).

Výzkumníci využívající relační a konceptuální analýzy uvádějí, že není důvod, aby pomocí obsahové analýzy se základní oporou vztahu v četnosti výskytu znaků nebylo možné zaznamenávat i vztahy mezi nimi (Lombard et al., 2004).

Použití metody obsahové analýzy pro prvotní analýzu existujících právních norem či bezpečnostních standardů umožňuje identifikovat klíčová témata a koncepty, jež jsou v právních předpisech a bezpečnostních standardech obsaženy, a také zjistit, jak jsou tyto prvky organizovány a prezentovány v textu. Tato analýza může poskytnout důležité informace pro tvůrce zákona při přípravě nového návrhu, a to včetně toho, jaké téma nebo koncepty mají být zahrnuty, jak mají být organizovány a jaká slovní spojení se v textu používají. Použití metody obsahové analýzy pro prvotní analýzu existujících zákonů má však také několik omezení. Tento postup může být omezen na to, co je obsaženo v textu zákona, a současně nezahrnuje informace o tom, jak se daný zákon v praxi používá nebo jaké jsou jeho dopady na společnost. Další omezení může být způsobeno subjektivní interpretací analytika, který provádí obsahovou analýzu.

Z metodologického hlediska je tedy obsahová analýza řazena do kvalitativního a kvantitativního výzkumu, avšak pro řešení stanovených cílů práce je využita kvalitativní obsahová analýza.

Metodologický postup pro zpracovávání obsahové analýzy je uváděn v odborných publikacích např.:

- Content Analysis: An Introduction to Its Methodology (Krippendorff, 2018).
- Qualitative Content Analysis: A Step-by-Step Guide (Mayring, 2021).
- Analyzing Media Messages: Using Quantitative Content Analysis in Research (Routledge Communication) (Riffe et al., 2019).
- Qualitative Content Analysis in Practice (Schreier, 2012).

Procesní postup pro zpracování kvalitativní obsahové anýzy s využitím softwaru byl pro zjednodušení rozpracován prostřednictvím Business Process Model a Notation a je zobrazen dále v rámci této dílčí podkapitoly.

Zpracování kvalitativní obsahové analýzy s využitím softwaru

Zpracování obsahové analýzy předcházela formální analýza zvaná také jako identifikační analýza, která je zaměřena na výzkum dokumentů po formální stránce (formální analýza). V rámci formální analýzy byly analyzovány existující právní předpisy, bezpečnostní standardy či jiná metodická doporučení související s oblastí využívání informačních technologií se zaměřením na kamerové systémy.

Odpovídající dokumenty a právní předpisy byly zvoleny v návaznosti na metodologický postup a provedenou analýzu v kapitole s názvem Využití Smart technologií a IT technologií u základních složek IZS ČR při zajišťování ochrany

obyvatelstva a veřejného pořádku. Identifikované právní předpisy, bezpečnostní standardy a další související dokumenty byly rovněž vybrány s ohledem na veřejnou dostupnost dokumentů na internetu.

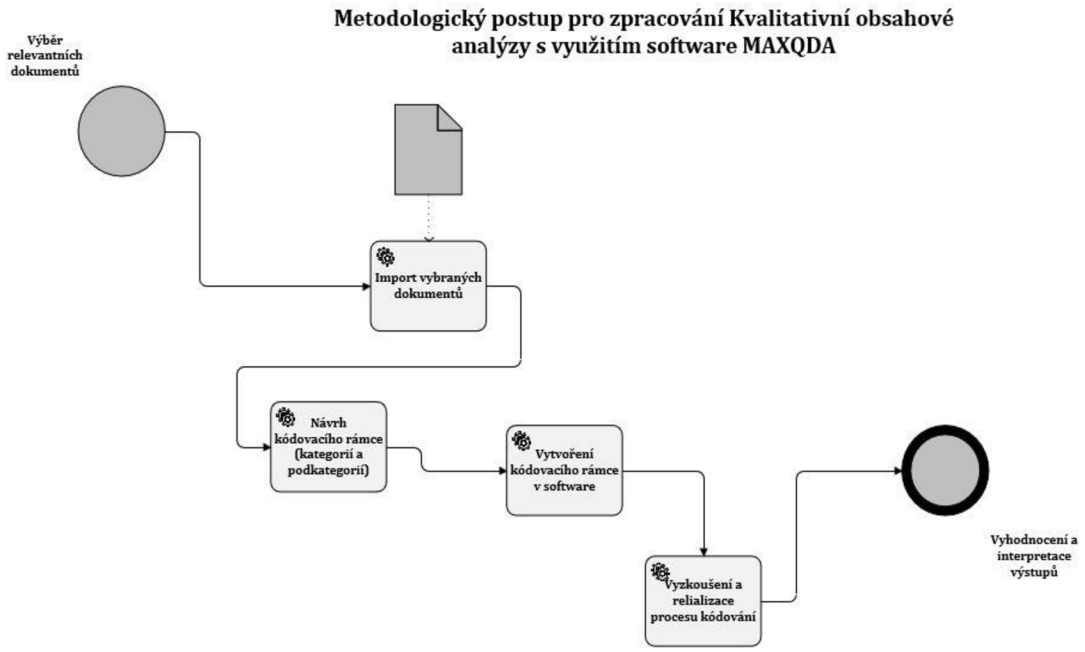
Pro automatizované zpracování prvotních návrhů nových/nového právního předpisu či návrhu nových bezpečnostních standardů pro IoT pro využití v tematicky zaměřených částech koncepce Smart Cities je možné využít vhodný software pro zpracování textu.

Na základě provedeného šetření, kdy byla analyzována existující softwarová řešení, jež by byla vhodná pro provedení tohoto procesu, byl zvolen software, který je svým zaměřením určen pro zpracování kvalitativní nebo kvantitativní obsahové analýzy, a to software s názvem MAXQDA. Tento software však lze využít nejen pro zpracování kvalitativní obsahové a kvantitativní obsahové analýzy, uvedený software obsahuje i další relevantní funkce, které lze využít pro zpracování právních textů dle aktuálních potřeb pro řešené otázky.

V souvislosti s rozšířením uvedeného softwaru byla vydána kniha, ve které jsou zpracovány praktické příklady využití tohoto softwaru, přičemž zpracovávání právních textů bylo součástí uvedených příkladů. Uvedený software obsahuje množství funkcí a záleží na řešení konkrétního problému, který výzkumník zpracovává. Software lze přizpůsobit zpracovávanému úkolu a vhodně doplnit i statistickým ověřením, pokud je statistické zpracování dat součástí řešeného úkolu.

Pro vhodnost ověření kvalitativní obsahové analýzy s využitím softwaru MAXQDA pro přípravu vzorku nových bezpečnostních standardů pro využití v koncepci Smart Cities bylo zvoleno tematické zaměření na CCTV. Pro zpracování vzorku v podobě návrhu bezpečnostních standardů pro CCTV na základě vhodně zvolených dokumentů byla využita pouze kvalitativní obsahová analýza a její funkce v tomto softwaru.

Proces pro zpracování vzorku prostřednictvím softwaru MAXQDA je zpracován prostřednictvím modelu BPMN 3 níže.



Model BPMN 3 Postup pro zpracování obsahové analýzy

Zdroj: Vlastní zpracování

Výběr relevantních dokumentů (formální analýza)

Výběr odpovídajících dokumentů souvisejících s problematikou kamerových systémů zahrnoval rešerši platných právních dokumentů, metodických doporučení a ISO/IEC norem a veřejně dostupných interních směrnic v České republice.

Relevantní dokumenty

A. Právní předpisy, bezpečnostní standardy
   - Zákon č. 110/2019 Sb., o zpracování osobních údajů (Zákon č. 110/2019 Sb., Zákon o zpracování osobních údajů, 2019).

B. Metodické doporučení, směrnice
   - Metodika k návrhu a provozování kamerových systémů z hlediska zpracování a ochrany osobních údajů (Havelda et al., 2024).
   - Vnitřní směrnice o provozování kamerového systému (Matyášek, 2019).
   - Směrnice o podmínkách provozování kamerového systému se záznamem a ochraně osobních údajů (Vološčuk, 2019).
   - Vnitřní předpis zaměstnavatele stanovící postupy v souvislosti se zavedením kamerových systémů (Velebilová, 2022).
   - Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů (Kolektiv autorů, 2012).

2. ČSN normy – nelze analyzovat – zpoplatněno.

- ČSN EN 62676-1-1 (334592) Dohledové video systémy pro použití v bezpečnostních aplikacích – Část 1-1: Systémové požadavky – Obecně.
- ČSN EN 50132-2-1 (334582) Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích – Část 2-1: Černobílé kamery – zrušena bez náhrady.
- ČSN EN 50132-5 (334582) Poplachové systémy – CCTV sledovací systémy pro použití v bezpečnostních aplikacích – Část 5: Přenos videosignálu – zrušena bez náhrady.
- ČSN EN 62676-1-2 (334592) Dohledové video systémy pro použití v bezpečnostních aplikacích – Část 1-2: Systémové požadavky – Výkonové požadavky na video přenos.
- ČSN EN IEC 63033-4 (368609) Vozidlové multimediální systémy a zařízení – Řídicí systém monitorování – Část 4: Aplikace pro kamerové monitorovací systémy.

Import dokumentů

Relevantní dokumenty byly importovány prostřednictvím automatického importu do software MAXQDA a následně byl vytvořen soubor s názvem „CCTV“, který je přiložen v rámci příloh v elektronické podobě.

Vytvoření kódovacího rámce

Z hlediska návrhu bezpečnostních standardů pro CCTV, kdy je velký důraz kladen na ochranu osobních údajů, bylo nutné tuto skutečnost zohlednit při návrhu kódovacího rámce.

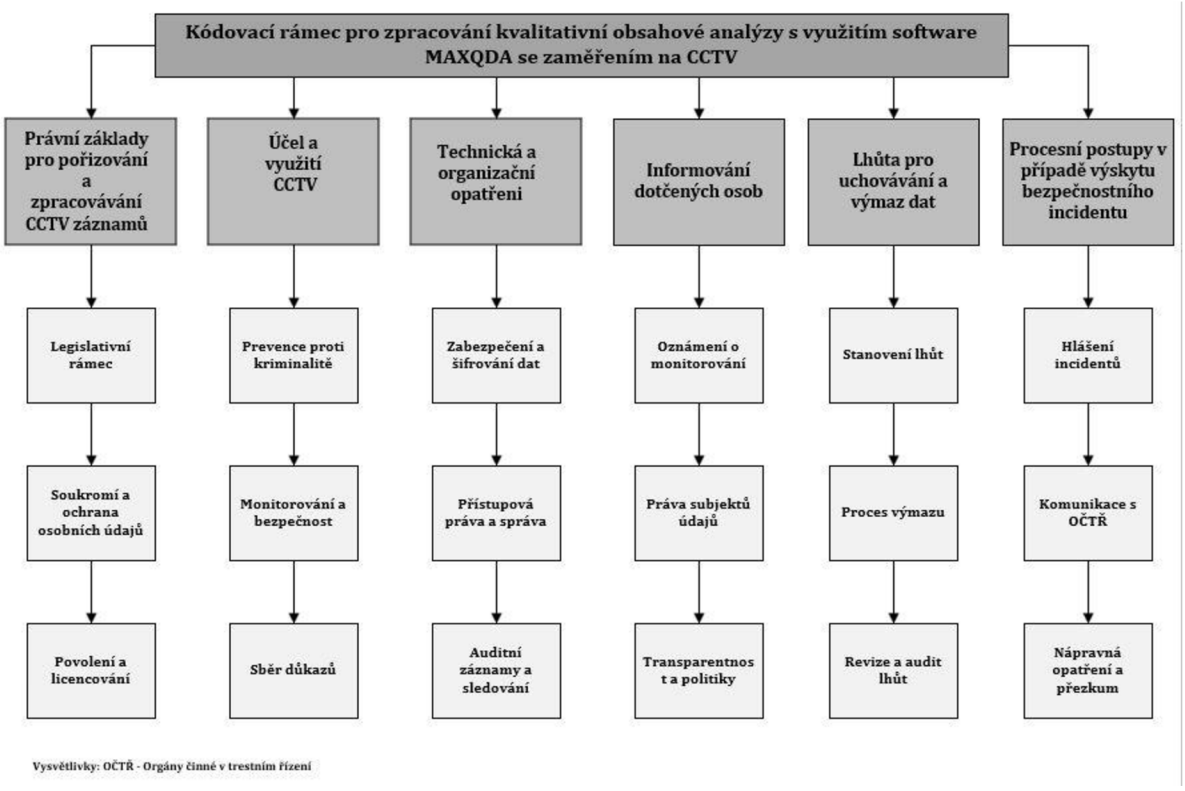
Pojem „kódování“ byl mnohokrát definován v různém pojetí. Definice tohoto pojmu se u mnohých autorů rozcházejí ve svém významu. Je nutno rozlišovat proces kódování v kvalitativním výzkumu, tedy v kvalitativní analýze dat, a proces kódování u kvalitativní obsahové analýzy dat. Taktéž je nutno rozlišovat mezi označováním a kódováním dat. Dey (2016) zdůrazňuje, že kódování je konceptuální proces, kdy vytvořením kódu je identifikována část dat jako dílčí část daného konceptu. Kódování se používá taktéž jako samostatná metoda (Coffey & Atkinson, 1996). Proces kódování lze aplikovat i v rámci zakotvené teorie při zpracovávání kvalitativní analýzy dat (Řiháček et al., 2013). Atkinson a Coffey (1996) provedli rozlišení různých způsobů kódování, kdy rozlišují kódování za účelem redukce dat a kódování jako koncepční nástroj.

Redukční kódování je proces, při kterém je kladen důraz na seskupování dat řešící stejné téma, kdy jsou vytvářeny vazby mezi různými částmi dat. Tento typ kódování je čistě popisný a využívá se pro redukci dat. Někdy bývá redukční kódování využíváno jako první etapa pro hlubší konceptuální kódování. Kódování jako konceptuální nástroj je využíváno jako nástroj, jež pomáhá přemýšlet výzkumníkům o tom, jakým způsobem může identifikovaný koncept souviset s ostatními koncepty, dále o tom, jak spolu koncepty souvisejí a jaké jsou jejich vazby mezi sebou. Tento typ kódování napomáhá výzkumníkům rozšířit získané poznatky a zjištěné informace o další nové aspekty.

Kódování v souvislosti s kvalitativní analýzou textu je využíváno jako nástroj konceptuálního kódování.

„Kódovací rámec je způsob strukturování materiálu. Skládá se z hlavních kategorií určujících příslušné aspekty a z podkategorií pro každou hlavní kategorii určujících příslušné významy týkající se tohoto aspektu.“

Nejprve byly stanoveny hlavní kategorie pro vytvoření kódovacího rámce. Hlavní kategorie kódovacího rámce představují aspekty pro tematické zaměření zpracování obsahové analýzy s využitím software MAQXDA, současně představují stanovenou prvotní strukturu návrhu nových bezpečnostních standardů. Kódovací rámec je graficky zpracován na obrázku 9 níže.



Obrázek 9 Kódovací rámec pro zpracování obsahové analýzy

Zdroj: Vlastní zpracování

Kódovací rámec byl navržen jako jednoúrovňový s rozdělením na dílčí kategorie, poněvadž cílem zpracování vzorku bezpečnostních standardů pro CTTV v této práci není komplexní zpracování do hloubky, ale představení kvalitativní obsahové analýzy s využitím SW jako vhodné metody pro prvotní zpracování nových bezpečnostních standardů nebo nových právních předpisů.

Vyzkoušení kódovacího rámce

Po zadání kódovacího rámce a stanovených kategorií bylo provedeno vlastní kódování textu všech zvolených a importovaných dokumentů. Při procesu kódování se se mohou vyskytnout i další části, které nejsou v prvotní struktuře kódování navrženy. Chybějící kategorie a podkategorie je možné doplnit na základě zpracovávání procesu kódování. Vždy záleží na konkrétní situaci, stanovených cílech a výstupech pro řešení daného úkolu. Software umožňuje více funkcí např. lemmatizaci, parafrázování, vyhledávání četnosti slov atd.

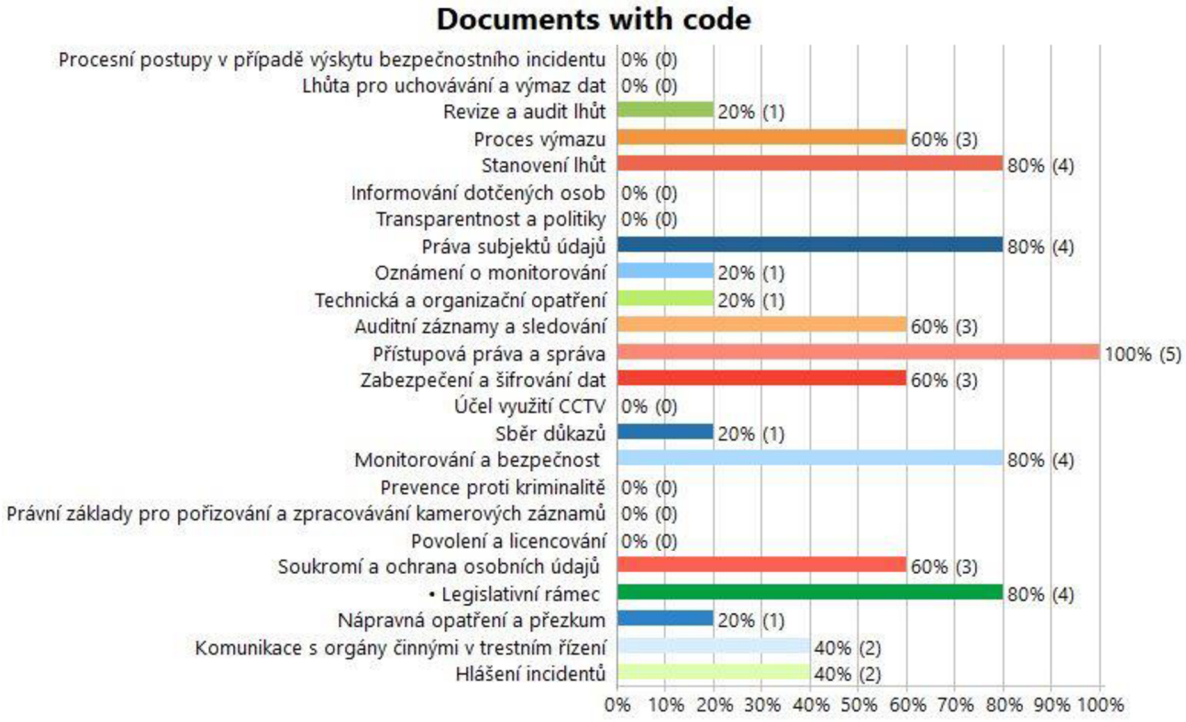
Pro automatizované kódování je možno využívat i doplňku ve formě umělé inteligence, která při samotném procesu kódování dokáže přečíst texty importovaných předpisů a současně vytvoří parafrázování kódovaného (vybraného) textu.

Kódování v rámci ověření i této metody proběhlo ručně, nikoliv s využitím AI. Výstupy z provedeného kódování lze upravovat různými funkcemi, které tento software nabízí. Výstupy z provedené analýzy textu lze jednoduše exportovat do standardních souborů pro další zpracování (MS Office).

Další možností pro interpretativní ukázku možných grafických výstupů je graf, na základě kterého lze porovnat četnost kódů a kategorií. Na základě uvedeného grafu lze vyčíst, že některé kategorie, které byly navrženy pro kódovací rámec, nejsou v některých dokumentech zahrnuty. Prázdné kategorie však nejsou chybou, ale slouží spíše k zamyšlení po odborné stránce s ohledem na řešené téma v podobě otázek. Z jakého důvodu importované dokumenty (vybrané dokumenty) tuto problematiku neobsahují? Využití této metody může mít i další přínosy, především v tom, že napomůže pro hledání dalších souvislostí či může být inovativním podnětem pro další zavádění inovací, aniž by musel být tento problém řešen např. v rámci brainstormingu s dalšími odbornými pracovníky.

Standardně lze kódy exportovat pro další úpravy do kancelářského softwaru, zejména MS Excel, na jehož základě jsou vyexportovány výstupy kódů. Tento výstup vybraných textů, jež byly kódovány v rámci kvalitativní analýzy dat, a proces kódování

lze po exportování využít pro prvotní návrh nových bezpečnostních standardů. Exportovaný soubor po zpracování je přiložen v rámci elektronických příloh k této práci v příloze 3. Výstupy jsou zobrazeny podobě grafu na obrázku 10.



Obrázek 10 Procentuální přehled výskytu kódů ve zpracovávaném vzorku

Zdroj: Vlastní zpracování

Vyhodnocení a interpretace výstupů

Prostřednictvím zpracovaného vzorku bylo provedeno systematické zkoumání textu založené na metodě abstrahování, kdy byly v rámci výše uvedených etap zpracovány relevantní informace na základě stanovené struktury kategorií a podkategorií v procesu kódování. Zpracovaný výstup poskytl relevantní informace, které jsou vhodné pro požadovaný výstup a stanovené cíle. Výstupy z provedené analýzy poskytují prvotní strukturu návrhu nových bezpečnostních standardů pro CCTV, na základě kterých bylo současně zjištěno, že některé kategorie při procesu kódování by bylo vhodné rozšířit a více rozpracovat do detailu. Dále byl ušetřen čas, v rámci kterého by bylo nutné číst do detailu všechny importované dokumenty a současně pak v textovém editoru zpracovávat poznámky, které by byly zjištěny přečtením všech relevantních dokumentů. Další přínosy a využití jsou rozpracovány v další kapitole 5.4 na základě provedení validace v rámci expertních skupin u stanovených organizací.

5.3.2.2 Alternativní metoda pro zkoumání textu

Pro zhodnocení vhodnosti výběru zvolené metody pro zpracování textu bylo nutno zvážit i jiné metody pro zkoumání textu. Alternativní metodou pro zkoumání textů je metoda pro zkoumání dokumentů.

Zkoumání dokumentů patří k metodám, které se řadí taktéž do oblastí kvalitativního výzkumu, avšak tato metoda je využívána spíše pro zkoumání historických dokumentů. Analýza textu je prováděna příslušnými odborníky, kteří posuzují historické dokumenty na základě listin v kontextu historické události. Jsou to právě dokumenty, které obsahují vědomé či nevědomé postoje, hodnoty a ideje. Analýza v rámci metody zkoumání dokumentů začíná definováním zkoumané otázky. V rámci zkoumaných otázek je třeba nalézt vhodné dokumenty ke zkoumání. Po nalezení a stanovení vhodných dokumentů ke zkoumání se provádí interní a externí posuzování dokumentů s následnou interpretací s určením hledání odpovědí na položené otázky.

Z hlediska využití této metody s řešeným tématem by právní akty, mezinárodní standardy či studie proveditelnosti byly nejprve vhodně identifikovány (nalezeny), sepsány a seřazeny z historického hlediska až po současnost. V rámci dalšího zkoumání stanovených dokumentů by byly stanoveny výzkumné otázky. Výzkumné otázky by byly formulovány podle historických souvislostí zkoumaných dokumentů současně s formulací výzkumných otázek k aktuálním dokumentům. Po provedení formulace výzkumných otázek by následovalo provedení pramenné kritiky s následnou interpretací dokumentů.

Hodnota zkoumaných právních dokumentů, mezinárodních směrnic či studií proveditelnosti by se posuzovala podle níže uvedených kritérií:

- Typ dokumentu – právní normy, mezinárodní směrnice a normy.
- Vnější znaky dokumentu – písmo, ilustrace.
- Vnitřní znaky dokumentu – význam dokumentů, směrnic.
- Intencionalita dokumentu – vědecká hodnota.
- Blízkost dokumentu – souvislosti mezi právními normami, mezinárodními směrnicemi a ostatními zkoumanými dokumenty.
- Původ dokumentu – původ vytvoření právních norem, mezinárodních směrnic.

Využití této alternativní metody lze tedy přirovnat k obdobnému a současnému využívání neautomatizovaných a neformálních procesů pro přípravu nových bezpečnostních standardů a nových návrhů právních předpisů s využitím

kancelářského softwaru Microsoft Office. Metoda je zdlouhavá a je založena na odborných personálních kapacitách bez prvků automatizace, kdy význam či kopie historických dokumentů jsou převáděny do digitální podoby pro uchovávání a zpřístupnění záznamů prostřednictvím on-line formy.

5.4 Validace výsledků v rámci expertních skupin

Zjištění skutečného stavu a validace výstupů byla ověřena v souladu s metodologickým postupem a stanovenými cíli a přínosy práce.

Pro ověření validace navrhovaných metod byla zvolena kombinace metod využívaných v kvalitativním výzkumu formou neformálního rozhovoru a písemné komunikace. Přesná metodologie neformálního rozhovoru a písemné komunikace nebyla dodržena (povoleno v kvalitativním výzkumu, podrobněji v kapitole 1 Metodologický postup), byla využita kombinace odpovídajících prvků, avšak takovým způsobem, aby postup pro ověření validity kvalitativního výzkumu byl dodržen.

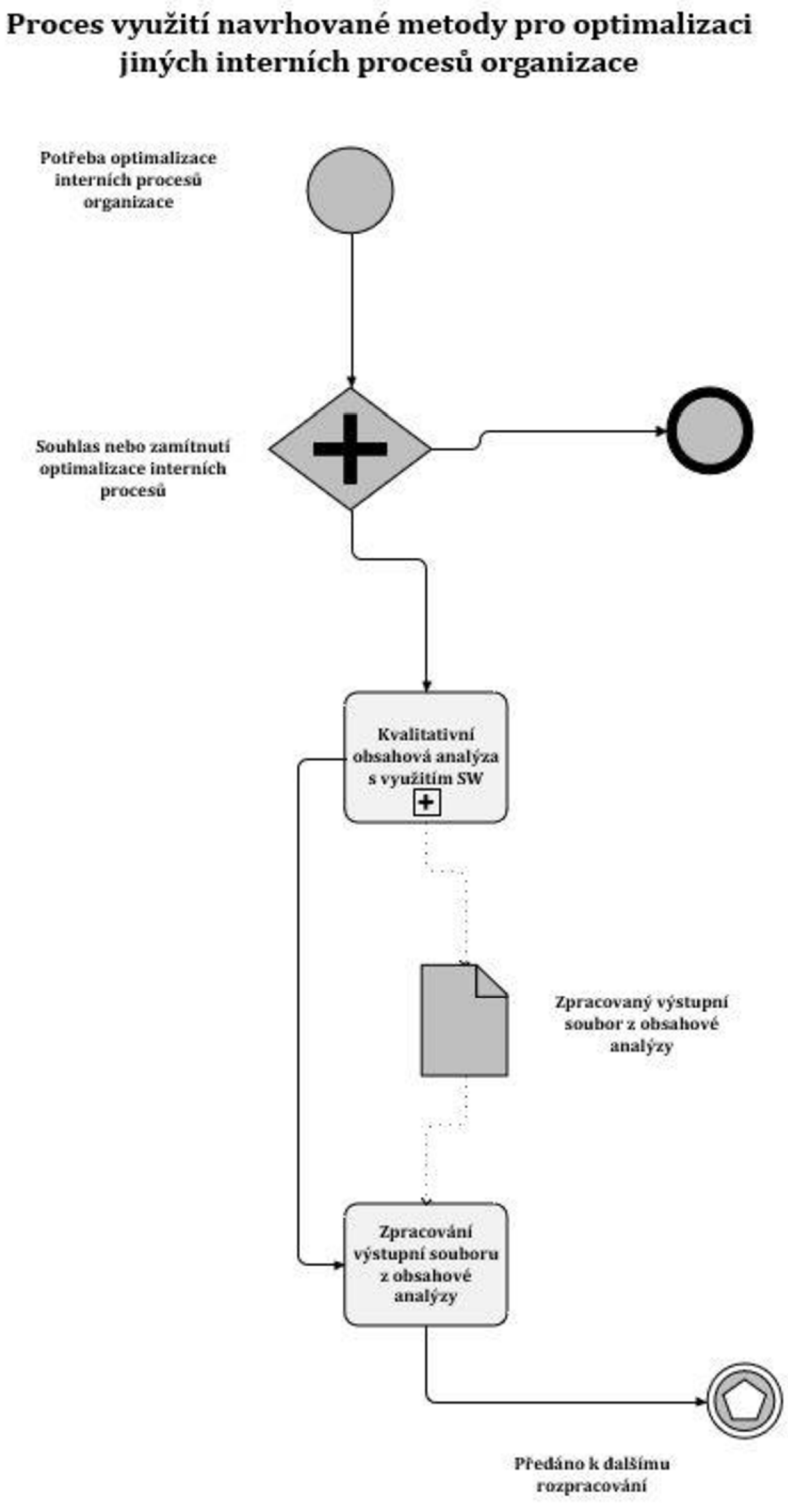
Ověření validace navržených metod a jejich kombinace proběhla s využitím neformálního rozhovoru a prostřednictví písemné komunikace s dvěma organizacemi: Ministerstvo vnitra České republiky, Odbor legislativy a koordinace předpisů, a soukromá advokátní kancelář Císař, Čéška, Smutný, s. r. o., v rámci Oddělení regulace a legislativy.

Validace navržených metod na Odboru legislativy a koordinace právních předpisů proběhla na základě rozhovoru, kde byly představeny řešený problém, stanovené cíle a přínosy práce, dále proběhlo seznámení se současným stavem na zahraniční a národní úrovni a současně byly vysvětleny navrhované metody. Dále byla ukázána metoda pro řešení obsahové analýzy s využitím softwaru MAXQDA. V závěru jednání byl představen výstup ze zpracovaného vzorku pro návrh bezpečnostních standardů pro CTTV. Dále proběhl rozhovor na základě aktuálně řešených problémů procesu přípravy nových právních předpisů, kde bylo sděleno, že probíhá neveřejné interní testování nového softwaru s názvem E-legislativa. Tento software by měl v budoucnu zdigitalizovat celý proces přípravy nových právních předpisů. S ohledem na řešený problém však bylo konstatováno, že prvotní návrh nových právních předpisů, který byl řešen v této práci, v uvedeném řešení E-legislativa není zahrnut.

V průběhu jednání byly identifikovány další možnosti využití navrhovaných metod pro zefektivnění jiných souvisejících procesů, které probíhají v rámci uvedeného odboru v souvislosti s legislativou. Další využití bylo navrženo v kontextu

zpracovávání obsahové analýzy formou uvedeného softwaru a využití AI při zpracovávání odborných stanovisek k novým právním předpisům, které čítají desítky stran, přičemž pro jednání do Poslanecké sněmovny se předkládají stanoviska max. na dvě strany A4. Pro využívání navrhovaných metod spolu s metodou pro zpracování textu a odpovídajícím softwarem bylo taktéž konstatováno, že potřebný čas pro zpracovávání stanovisek se podstatně sníží, a současně, že tato stanoviska může zpracovávat i pracovník, u kterého není nutné odborné právní vzdělání, poněvadž zpracované stanovisko k novému právnímu předpisu v počtu max. 2 strany A4 bude předáno pracovníkovi s odborným právním vzděláním k doplnění až po zpracování metodou obsahové analýzy s využitím softwaru. Na základě integrace inovace ve formě navrhované metody při procesu zpracovávání odborných stanovisek by tedy bylo možné snížit časové zatížení odborných personálních kapacit u pracovníků, kteří musejí v současnosti obsáhlá právní stanoviska číst a ručně zpracovávat s využíváním MS Word.

Díky metodě a softwaru sloužícímu pro zpracovávání obsahové analýzy by tedy materiály mohl zpracovávat pracovník s nižším odborným vzděláním, s nižším platovým zařazením, čímž by organizace mohla ušetřit finanční prostředky vynaložené na mzdové náklady. Tato varianta je jednou z možností, jak by bylo možné využít navrhované metody. Využití navrhovaných metod pro zlepšení jiných interních procesů v organizaci je vždy individuální. Využití navrhované metody pro zlepšení efektivity jiných interních procesů organizace zobrazuje model BPMN 4 níže.



Model BPMN 4 Využití metody pro jiné interní procesy

Zdroj: Vlastní zpracování

Validace u další organizace Advokátní kancléř Čéška, Císař, Smutný, s. r. o., proběhla na základě osobní schůzky a dále na základě písemné formy (podrobněji v kapitole 5.2 a v přílohách), která byla doložena prostřednictvím písemné komunikace. Písemná forma je součástí přiložených příloh, v rámci písemné komunikace proběhlo současně i ověření skutečného stavu.

V rámci rozhovoru byly představeny navrhované metody a jejich využití v organizaci pro zlepšení interních procesů. U soukromých advokátních kanceláří však rozsah přípravy nových právních předpisů není realizován v takovém rozsahu jako u všech výše uvedených organizací (krajský úřad, ústřední správní úřad, ministerstvo). Soukromé advokátní kanceláře připravují a zapojují se do přípravy nových právních předpisů na základě veřejných zakázek nebo obchodních požadavků. Nicméně i tato oblast pro ověření validace je velmi důležitou součástí celého procesu validace, poněvadž příprava nových právních předpisů a bezpečnostních standardů probíhá v rámci připomínkového řízení ze strany soukromých subjektů, ke kterým patří i soukromé advokátní kanceláře. Možnost využití navrhovaných metod pro zlepšení jiných interních procesů organizace nebyla zavrhnuta. Představené metody byly hodnoceny pozitivně a byl projeven zájem na případné další budoucí spolupráci v této oblasti.

Pro přehledné zpracování zjištěných informací při ověřování skutečného stavu a následné validaci u zvolených organizací byla zpracována SWOT analýza, která systematicky identifikuje a shrnuje pozitiva a negativa navrhovaných metod.
SWOT analýza je důležitým nástrojem, který je využíván v kvalitativním výzkumu a z hlediska celkového postupu pro řešení daného problému byla zvolena tato metoda jako metoda nejvhodnější.
„SWOT analýza je komplexní metodou kvalitativního vyhodnocení veškerých relevantních stránek pro řešení dané problematiky, resp. fungování nějakého systému (popř. problémů, řešení, projektů atd.). Je vhodným nástrojem pro celkovou analýzu vnitřních i vnějších činitelů a v podstatě zahrnuje postupy technik strategické analýzy.“ (Mašínová et al., 2008)
„Analýzou vzájemné interakce jednotlivých faktorů silných a slabých stránek na jedné straně vůči příležitostem a nebezpečím na straně druhé lze získat nové kvalitativní informace, které charakterizují a hodnotí úroveň jejich vzájemného střetu. Podstatná kvalita analýzy SWOT vychází z předpokladu, že organizace dosáhne strategického

úspěchu maximalizací předností a příležitostí a zároveň minimalizací nedostatků a hrozeb.“ (Šrámková, 2007)

„Analýzou vzájemné interakce dílčích aspektů silných a slabých stránek na jedné straně vůbec příležitostem a nebezpečím, na straně druhé lze získat nové kvalitativní informace, jež současně kvalifikují a hodnotí úroveň vzájemného střetu.“ (Mašínová et al., 2008)

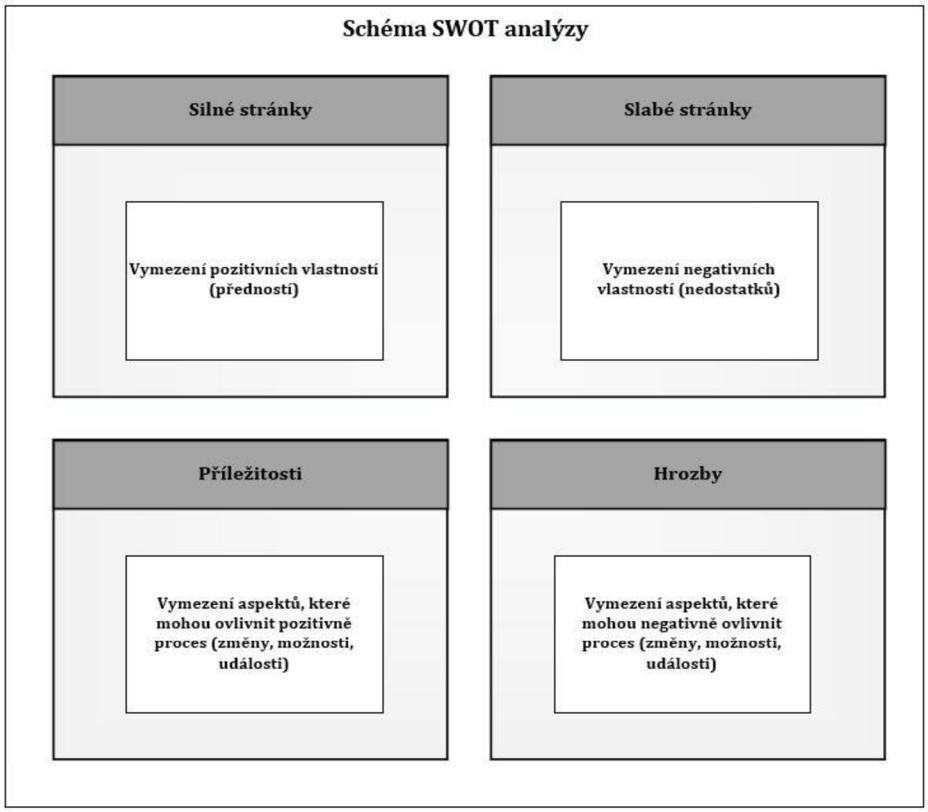
Analýza SWOT byla tedy využita ve spojitosti s prvotním procesem přípravy nových právních předpisů a nových bezpečnostních standardů, a to zejména proto, že umožňuje nastavení systematického logického rámce pro hodnocení současného stavu z hlediska slabých a silných stránek a dále z hlediska budoucích příležitostí a možných hrozeb.

Pro organizace, které se podílejí na přípravě, implementaci a následné aktualizaci interních předpisů v organizacích, je SWOT analýza důležitá především v aspektech:

- Zlepšení výkonnosti organizace.
- Aktualizace strategických aktivit (alternativ).
- Strategický rámec pro hodnocení současné efektivity procesů v organizaci.

SWOT analýza se využívá i jako podklad pro rozhodování mezi více variantami nebo jako podklad pro návrh nových opatření (Půček, 2020). Analýza hodnotí daný jev v okamžiku zpracovávání na základě zjištěných skutečností. Vhodnost zvolené metody pro validaci lze nalézt ve znacích pro správné rozhodnutí, jehož znaky byly charakterizovány prostřednictvím hodnotového rámce rozhodovatele na základě souladu s právními předpisy, interními postupy, které účinně vedou k dosažení stanovených cílů nebo splnění zadaných úkolů (Půček, 2020).

Schéma SWOT analýzy zobrazuje obrázek 11.



Obrázek 11 Schéma SWOT analýzy

Zdroj: Vlastní zpracování

Postup pro zpracování SWOT analýzy zahrnoval části dle Půčka (Půček, 2020):

- Plánování.
- Shromáždění a prověření.
- Stanovení silných a slabých stránek, příležitostí a hrozeb.
- Hodnocení silných a slabých stránek, příležitostí a hrozeb a kontrola vazeb.
- Ověření analýzy jako celku.
- Schválení analýzy a její využití.

Analýza příležitostí a rizik

Analýza příležitostí a rizik umožňuje rozlišit pozitivní a negativní příležitosti, které mohou organizacím přinést výhody a nevýhody, přičemž současně mohou být identifikovány další související problémy. Při posuzování příležitostí je důležité, aby byly příležitosti posuzovány z hlediska možného výskytu a pravděpodobnosti pozitivních dopadů. Při posuzování rizik je důležité posuzovat rizika z hlediska vážnosti a pravděpodobnosti výskytu negativních dopadů. Analýza příležitostí a rizik

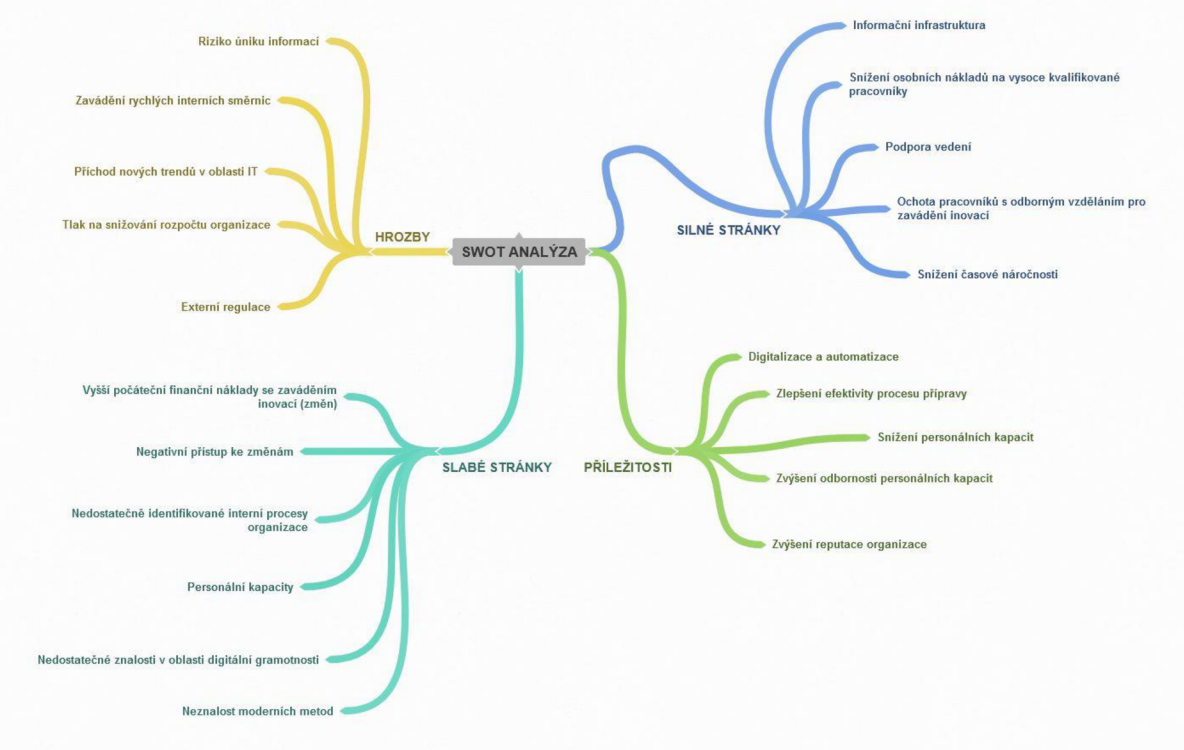
umožňuje rozlišit pozitivní a negativní příležitosti, které mohou organizaci přinést výhody a nevýhody, přičemž současně může napomoci identifikovat další související problémy.

Analýza slabých a silných stránek

Silné stránky jsou všechny činnosti, které mají pozitivní dopady na fungující organizaci. Slabé stránky jsou činnosti, které mají negativní dopady na fungující organizaci.

Při provádění hodnocení slabých a silných stránek je důležité, aby každý aspekt byl odstupňovaný podle důležitosti a podle intenzity vlivu.

Je však nutno zmínit, že silné stránky se nemusejí vždy změnit ve výhodu, důvodem může být nízká důležitost. Obdobným způsobem lze nahlížet na překonávání slabých stránek, nemusejí přinášet organizaci očekávané pozitivní dopady, pokud náklady na změnu slabých stránek převýší celkový užitek. Grafické zpracování SWOT analýzy ve formě myšlenkové mapy zobrazuje obrázek 12.



Obrázek 12 Zpracovaná SWOT analýza ve formě myšlenkové mapy

Zdroj: Vlastní zpracování

Silné stránky, anglicky *Strengths*

Informační infrastruktura – kvalitní informační infrastruktura organizace umožňuje rychlejší implementaci IT Governance a SECI ve formě podpory integrace různých nástrojů pro správu znalostí. Zlepšení všech procesů v organizaci spojených se zaváděním inovací může ovlivnit i jiné interní procesy v organizaci, čímž dojde k celkovému zlepšení efektivity řízení procesů organizace spojených s využíváním prostředků informačních technologií.

Snížení časové náročnosti – metody zavádějí možnosti pro snížení celkové časové náročnosti a celkového vytížení pracovníků v rámci prvotního procesu přípravy s využitím navržených metod.

Snížení osobních nákladů na vysoce kvalifikované pracovníky – metody zahrnují i možnost využití méně odborně kvalifikovaných pracovníků při provádění činností souvisejících s využíváním metod a softwaru v oblasti informačních technologií.

Podpora vedení – pro integraci metod je důležitá podpora vedení, která je klíčová pro zajištění potřebných zdrojů a motivace zaměstnanců k adopci nových procesů.

Ochota odborných zaměstnanců organizace pro zavádění inovací – důležitým aspektem při zavádění inovací v organizacích je ochota ke spolupráci.

Snížení časové náročnosti – snížení celkové časové náročnosti a celkového vytížení pracovníků v rámci prvotního procesu přípravy s využitím navržených metod může být přínosem pro organizaci.

Slabé stránky, anglicky *Weaknesses*

Vyšší počáteční finanční náklady se zaváděním změn – mohou být zvýšené počáteční náklady se zaváděním metod z oblastí informačního a znalostního managementu a dále se zaváděním nových SW řešení pro zpracovávání textu. Finanční, lidské a technologické zdroje mohou bránit efektivní implementaci a udržitelnosti IT Governance a SECI modelu.

Negativní přístup ke změnám – může být negativní přístup pracovníků organizace k zavádění změn v oblasti znalostního a informačního managementu spojených s postupnou formalizací prvotního procesu přípravy a využíváním nových informačních systémů.

Nedostatečně identifikované interní procesy organizace – nedostatečně identifikované interní procesy organizace, chybějící interní směrnice, jež by

formalizovaly proces přípravy nových bezpečnostních standardů a nových právních předpisů, mohou být slabinou interních procesů.

Personální kapacity – nedostatečný počet kvalifikovaných pracovníků, kteří jsou přetíženi, může být slabinou při zavádění inovací do interních procesů.

Nedostatečné znalosti v oblasti digitální gramotnosti – nedostatečný počet kvalifikovaných pracovníků v oblasti digitální gramotnosti na právních odděleních, kteří by využívali pro zefektivnění pracovního procesu inovativních prostředků informačních technologií, může být slabinou organizace.

Neznalost moderních metod – neznalost vědních disciplín spojených se zaváděním procesu znalostí, prvků informačního managementu pro efektivní řízení organizace může být taktéž slabinou organizace.

Příležitosti, *anglicky Opportunities*

Digitalizace a automatizace – rozvoj a integrace nových technologií a metod (metody pro zkoumání textu) mohou výrazně inovovat stávající interní procesy a napomoci organizacím v automatizaci interních procesů s pozitivními dopady na správu znalostí a řízení informací a využívání vhodných metod.

Zlepšení efektivity procesu přípravy – implementace IT Governance a SECI modelu může výrazně zlepšit efektivitu procesu přípravy nových bezpečnostních standardů a nových právních předpisů, dále může zlepšit celkový proces strategického rozhodování v organizaci a konkurenceschopnost organizace.

Snížení personálních kapacit – zavedením vhodných metod a aktualizací interních procesů budou zavedeny efektivní postupy a prvky informačních technologií, které mohou snížit požadavek na počet zaměstnanců.

Zvýšení odbornosti personálních kapacit – integrací vhodných metod do interních procesů organizací bude zvýšena odbornost zaměstnanců, kteří se díky integraci nových metod do organizace naučí nové poznatky spojené s využíváním digitálních technologií v zaměstnání.

Zvýšení postavení organizace – implementace moderních metod do procesů organizace může zvýšit celkové postavení organizace včetně know-how a reputace.

Hrozby, *anglicky Threats*

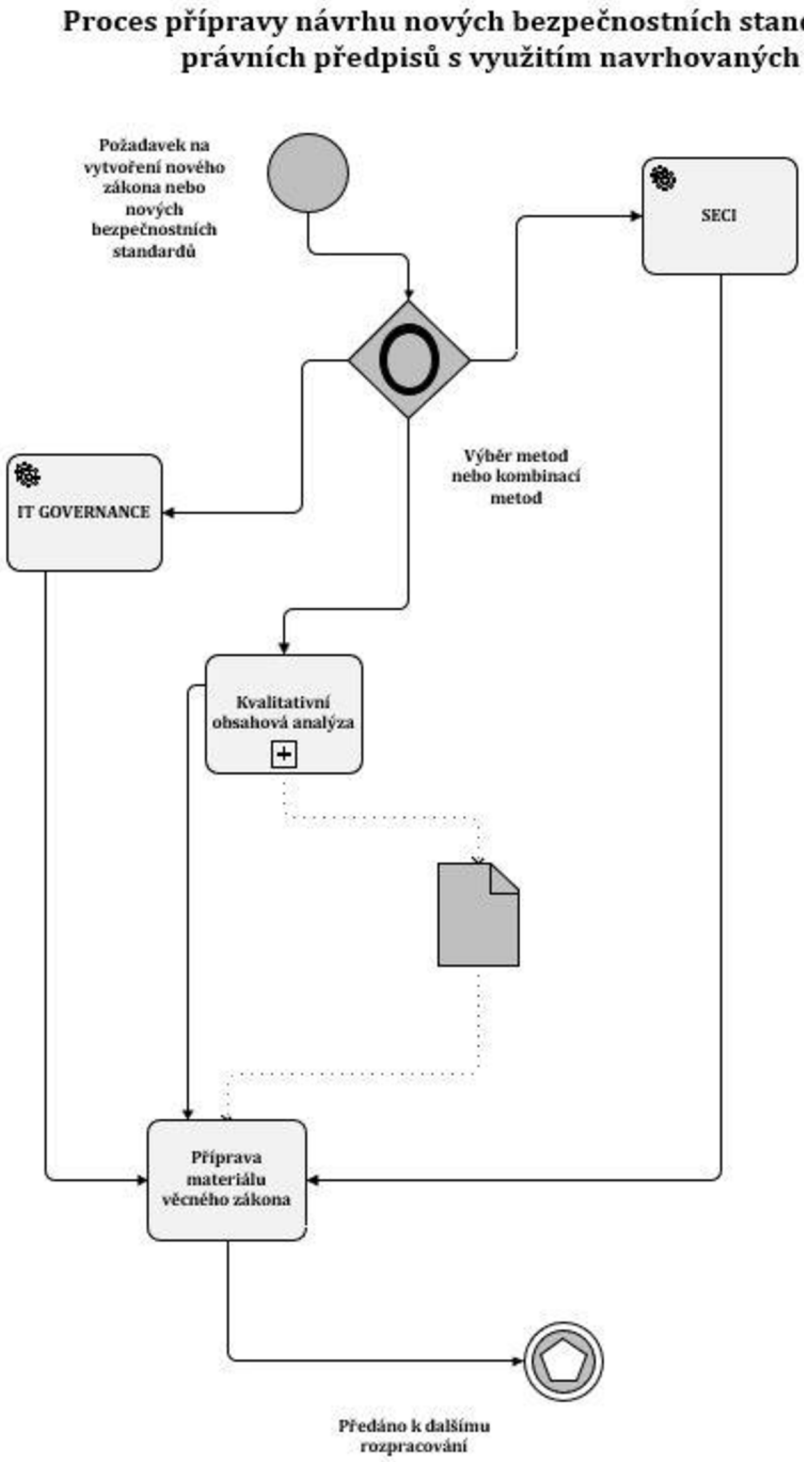
Zavádění rychlých interních změn – odborně nesprávně připravená implementace nových metod s cílem zavedení inovativních prvků do celkového procesu přípravy může být hrozbou pro organizaci, nikoliv příležitostí.

Příchod nových trendů v oblasti IT – nahrazení využívaných prostředků informačních technologií modernějšími technologiemi s umělou inteligencí může být hrozbou, pokud pracovníci nemají odpovídající znalosti v oblasti digitální gramotnosti.
Tlak na snižování rozpočtu organizace – v souvislosti s narůstajícími požadavky v oblasti kybernetické bezpečnosti dle platné legislativy se může vyskytnout tlak na snižování celkového rozpočtu organizace, která nebude mít dostatečné finanční prostředky na zavádění inovací v jiných procesech organizace např. v procesu přípravy.
Rychlý vývoj technologií může způsobit, že implementované systémy rychle zastarají, což vyžaduje neustálé investice do aktualizací a školení.
Externí regulace – zvýšené požadavky na dodržování předpisů a standardů v oblasti IT mohou komplikovat implementaci a provoz nových metod při zavádění.
Riziko úniku informací – při sdílení a správě znalostí v organizaci se mohou vyskytovat rizika spojená s únikem informací, která mohou mít vážné důsledky pro organizaci, což mohou být např. ztráta know-how, ztráta reputace aj.

Na základě zpracované SWOT analýzy byly identifikovány zdroje a kapacity organizace zahrnující finanční, interní, personální zdroje organizace, dále byl identifikován budoucí potenciál pro organizace ve formě příležitostí, jež může organizace využít pro budoucí rozvoj. Současně byly identifikovány hrozby, které se mohou vyskytnout z hlediska zavádění inovací ve formě navrhovaných metod.

Zpracovaná SWOT analýza může být využita i pro další organizace, které se podílejí na přípravě nových právních předpisů, nových bezpečnostních standardů nebo chtějí inovovat i jiné interní procesy. Využití navrhovaných metod je vždy individuální, poněvadž každá organizace má vlastní interní předpisy a pravidla, jež patří pod příslušné právní předpisy na základě odborného zaměření dané organizace.

Navrhované metody a jejich kombinace pro využití v organizacích je zpracována prostřednictvím modelu BPMN 5 dále a systematicky doplňuje oficiální model BPMN pro proces přípravy zpracovávání nových právních předpisů, který je zobrazen v modelu BPMN 2.



Model BPMN 5 Metody pro přípravu nových bezpečnostních standardů a nových právních předpisů

Zdroj: Vlastní zpracování

Z hlediska vhodnosti řešeného problému byl zvolen model pro hodnocení kritérií validity podle Lincolna a Guby, jež zahrnuje čtyři kritéria: důvěryhodnost, přenositelnost, hodnověrnost, potvrditelnost (Denzin & Lincoln, 2018).

Důvěryhodnost – v rámci důvěryhodnosti je dokazováno, zdali byl předmět zkoumání přesně identifikován a popsán. Pro ověření tohoto kritéria bylo navrženo několik dílčích podkritérií: dostatečné trvání studie, konzultace, kontrola subjektem nebo členem skupiny nebo triangulace.

Přenositelnost – kritérium přenositelnosti je interpretováno jako využití závěrů z konkrétního případu pro jiný obdobný případ, odpovědnost zobecnění je přenášena na osobu, která zobecnění provedla.

Hodnověrnost – toto kritérium dokládá, že provedený výzkum je považován za důvěryhodný, přičemž lze důvěryhodnosti dosáhnout např. triangulací.

Potvrditelnost – v rámci tohoto kritéria je prováděno ověřování, zdali řešený problém zahrnuje dostatečný počet informací, aby bylo možné na základě uvedených informací posoudit řešený problém a současně i získané poznatky v podobě nových přínosů a využitelnosti.

Ověření validity

Kritérium důvěryhodnosti – z hlediska dodržení kritéria důvěryhodnosti byl zvolen princip triangulace, který zahrnoval více metod pro sběr dat z více různých zdrojů od různých tazatelů. V rámci tohoto kritéria se provádí hodnocení souvisejících aspektů řešené problematiky. Splnění tohoto kritéria je rozpracováno v kapitole 4 Analýza současného stavu, která detailně rozpracovává řešenou problematiku prostřednictvím rešeršní strategie. Dále bylo provedeno zjišťování skutečného stavu na základě vhodně zvolených organizací s využitím stanovených metod. Výsledky provedeného šetření jsou popsány v dílčí podkapitole 5.2 Ověření skutečného stavu. Kritérium důvěryhodnosti lze považovat za splněné, poněvadž hlavní a související aspekty byly řádně identifikovány, doloženy a popsány.

Kritérium přenositelnosti – bylo ověřeno v rámci využití konkrétních závěrů ze zjišťování a ověřování skutečného stavu, na jehož základě je řešen proces přípravy nových právních předpisů. Řešený problém byl zkoumán a zpracováván v návaznosti na proces přípravy nových právních předpisů s možností aplikace principu přenositelnosti na proces přípravy nových bezpečnostních standardů pro IoT s možností dalšího využití v tematicky zaměřených částech koncepce Smart Cities.

Rozdílnost lze nalézt pouze v právní interpretaci závaznosti, kdy právní předpisy jsou právně závazné po řádném ukončení zákonodárného procesu. Bezpečnostní standardy mohou být pouze doporučeními nebo mohou být rozšířením interních předpisů organizace, v rámci kterých by byly nové bezpečnostní standardy implementovány.

Kritérium přenositelnosti lze považovat za splněné, využití konkrétních závěrů je možné zobecnit a přenést na oblast prvotního procesu přípravy nových bezpečnostních standardů.

Kritérium hodnověrnosti – hodnověrnost byla doložena na základě ověřování skutečného stavu u organizací, jež se podílejí na přípravě nových právních předpisů. Kritérium hodnověrnosti je splněno, problematika byla ověřena na základě důvěryhodnosti a triangulace u odborných organizací.

Kritérium potvrditelnosti – v rámci tohoto kritéria bylo provedeno ověření navržených metod prostřednictvím písemné a ústní formy u dvou organizací, MV ČR a Advokátní kanceláře Císař, Čéška, Smutný s. r. o. Pro ověření navržených metod, jež byly komunikovány v rámci výše uvedených expertních skupin, byla zpracována SWOT analýza, jež je rozpracována výše včetně myšlenkové mapy. Na základě zpracování SWOT analýzy lze konstatovat, že i toto kritérium bylo splněno.

Podmínka pro ověření validity na základě stanovených kritérií vycházejících z kvalitativního výzkumu byla splněna.

Uvedený problém byl v minulých desetiletích řešen, i když minimálně, a tato práce svým rozsahem i publikační činností autorky systematicky navazuje na řešený problém v ČR. Současně dál rozšiřuje v daleko vyšší míře možnosti pro automatizované zpracování právních textů, návrhů nových právních předpisů, návrhů nových bezpečnostních standardů s možností dalšího rozvoje v blízké budoucnosti. Zájem o další rozvoj a spolupráci byl potvrzen ze strany všech oslovených organizací, které se podílely na zjišťování skutečného stavu. V současnosti dochází k zavádění prvků umělé inteligence a neuronových sítí, na základě čehož je zřejmé, že řešení této problematiky bude v budoucnu řešeno i v rámci výzkumných projektů podporovaných z veřejných finančních zdrojů určených pro výzkumnou činnost.

5.5 Zhodnocení řešeného problému, přínosy

Pro hledání a navrhování efektivnějšího řešení zkoumaného problému byla využívána i hodnotová analýza, jejímž kritériem je efektivnost s cílem dosažení optima užitku při co nejnižších nákladech (Vlček, 2008). Objektem v tomto konkrétním

případě byl proces prvotní přípravy nových právních předpisů a nových bezpečnostních standardů. Hodnota pro organizaci byla identifikována jako poměr mezi úrovní uspokojení potřeby a celkovými náklady na využívání (Princip 3E).

Návrh vhodných metod a jejich kombinace přinášejí pro organizace podílející se na přípravě nových právních předpisů především pozitivní přínosy.

Základní přínos vyplývá intuitivně z aktuálního stavu řešeného problému, tedy z celkové neefektivnosti prvotního procesu přípravy nových bezpečnostních standardů a nových právních předpisů. Celková novost v části prvotní přípravy systematicky navazuje na tzv. organizační inovace, kdy dochází ke zlepšení stávajících metod a postupů či k zavádění zcela nových formalizovaných postupů, technik a nástrojů v oblasti procesních postupů v organizaci. Systematická návaznost na jiné vědní disciplíny pro využití a následný rozvoj tak stanovuje další předpoklady pro budoucí rozšiřování řešené problematiky v praktickém využití či v dalším rozvoji ve VaV projektech.

Další přínos lze nalézt v oblasti přípravy nových bezpečnějších standardů pro využití v tematicky zaměřených částech koncepce Smart Cities. Při implementaci dílčích částí koncepce Smart Cities do měst, obcí a krajů jsou využívány kombinace různých digitálních technologií (IoT, USB zařízení, IS, aj.) a v rámci každé organizace tak vznikají nové požadavky pro tvorbu či pro rozšiřování stávajících interních směrnic, kdy je nutno nové požadavky efektivně a účelně zapracovat. Navrhované metody přinášejí v rámci tohoto procesu přínos pro efektivní zpracovávání vzniklých požadavků organizace.

Vedlejší přínos lze nalézt v možnostech využití navrhovaných metod pro zavádění inovací do jiných interních procesů organizace tak, jak bylo ověřeno na základě validace u zvolených organizací v rámci expertních skupin.

Přínosy tedy zahrnují především oblasti:

- Zlepšení prvotního procesu přípravy.
- Zlepšení řízení informací v organizacích.
- Zlepšení spolupráce mezi subjekty.
- Zlepšení jiných interních procesů organizace.
- Využívání nových moderních technologií.

Na základě analýzy současného stavu, skutečného ověření a validace navržených metod v rámci expertních skupin lze konstatovat, že stanovené výzkumné otázky potvrzeny nebo na ně nebylo možné jednoznačně odpovědět.

Výzkumné otázky

VO1: Mohou zvolené metody z oblasti informačního a znalostního managementu a metody pro zkoumání textu inovovat neformalizovaný proces přípravy nových právních předpisů a nových bezpečnostních standardů?

Zvolené metody z oblasti informačního a znalostního managementu byly potvrzeny na základě zjištění skutečného stavu a následného ověření navržených metod v rámci expertních skupin.

VO2: Může využití kvalitativní obsahové analýzy s vhodným softwarem zkrátit potřebnou dobu pro přípravu nových právních předpisů a bezpečnostních standardů?

Využití kvalitativní obsahové analýzy s vhodným software může zkrátit potřebnou dobu pro přípravu nových právních předpisů a bezpečnostních standardů, na základě zjištění skutečného stavu a následného ověření navržených metod v rámci expertních skupin.

VO3: Jsou navržené metody IT Governance (informační management), SECI (znalostní management) a využití kvalitativní obsahové analýzy v souladu s principem 3E?

Na tuto výzkumnou otázku nelze jednoznačně odpovědět.

VO4: Bude zefektivnění prvotního procesu přípravy nových právních předpisů a bezpečnostních standardů přínosné pro další uplatnění v praxi při formalizování procesu přípravy nových právních předpisů?

Zefektivnění prvotního procesu přípravy nových právních předpisů a nových bezpečnostních standardů bude přínosné pro další uplatnění v praxi, a dále v rámci další rozvoje při spolupráci s oslovenými vládními organizacemi.

Navržené metody nebo jejich kombinace vnášejí do prvotního procesu přípravy inovativní prvky, které celý proces prvotní přípravy zefektivňují, zrychlují a současně inovují i celkový proces zavádění znalostí a informací do organizací. Současně navržené metody potvrzují i možnost využití pro zefektivnění jiných interních procesů v organizacích. Dále byl od všech dotázaných organizací projeven souhlas pro řešení této problematiky i v budoucnosti.

Stanovený cíl práce a dílčí podcíle práce byly splněny v souladu se stanoveným metodologickým postupem. Řešený problém a návrh nových metod pro vytváření nových bezpečnostních standardů pro využití v tematicky zaměřených částech koncepce Smart Cities byl ověřen na obdobném procesu přípravy pro přípravu nových právních předpisů. Navrhované metody mohou zavést do organizací celkové zefektivnění interních procesů a snížení zatížení vysoce kvalifikovaných personálních

kapacit z časového hlediska, čímž současně může docházet i k úspoře celkových nákladů organizace. Současně mohou navrhované metody být využity i pro optimalizaci jiných interních procesů v organizacích. Oblast informačního a znalostního managementu bude i v budoucnosti aktuálním tématem, zejména při postupném zavádění digitalizace a automatizace interních procesů pro zvýšení efektivity práce a šetření celkových rozpočtů organizací.

6 ZÁVĚR

V dnešní době jsme svědky vzrůstajícího pokroku v oblasti informačních a komunikačních technologií, který má zásadní vliv nejen na jednotlivce, ale i na oblast soukromého a veřejného sektoru. Schopnost efektivně sdílet data, informace a znalosti se stává klíčovým prvkem pro efektivní řízení organizací, které hledají nové možnosti pro zlepšování interních procesů s návazností na úsporu celkových nákladů.

Současně s touto integrací dochází v organizacích k aktualizacím stávajících interních předpisů a k implementaci nových předpisů. Tyto činnosti však skýtají náročné procesní změny, které je nutno aplikovat postupně, aby proces integrace nových změn nenarušil celkovou činnost organizace a současně kulturu organizace. S touto problematikou souvisí i zavádění změn do procesu prvotní přípravy nových bezpečnostních standardů a nových právních předpisů v podobě inovativních metod, jež celý proces inovují, zefektivňují a formalizují.

Důležitým aspektem je však v každé organizaci odpovídající odborné vzdělání pracovníků, kteří při navrhování a následné implementaci dokáží rozlišovat rozdíly a souvislosti mezi inovacemi a invencemi a jejich milníky v rámci organizace. S postupnou integrací metod však souvisí řada změn, které souvisejí i s postupnou změnou využívaných prostředků informačních technologií. Tyto prostředky je nutno obměňovat, upgradovat, což přináší zvyšování nákladů pro dlouhodobé investice.

Na základě analýzy současného stavu u odpovídajících organizací bylo zjištěno, že příprava nových bezpečnostních standardů či návrhů zákona v rámci legislativního procesu je neefektivní, neformalizovaná a při zpracovávání jsou využívány standardní kancelářské aplikace MS Office.

Výstupem této práce byl návrh vhodných metod a jejich kombinace, které inovují prvotní proces přípravy nových bezpečnostních standardů pro IoT s využitím v tematických částech koncepce Smart Cities v České republice a dále inovují prvotní proces přípravy nových právních předpisů. Navržené metody a jejich kombinace byly současně ověřeny u vhodně zvolených organizací, které současně potvrdily i případný zájem o další rozvoj a řešení této problematiky.

Stanovený cíl a dílčí podcíle této práce byly splněny v souladu se stanoveným metodologickým postupem.

Motivací pro zpracování návrhu vhodných metod v návaznosti na vědní disciplíny z oblastí znalostního, informačního managementu a ekonomických věd byly praktické zkušenosti autorky, které získala v rámci pracovního zařazení na Národním

úřadu pro kybernetickou a informační bezpečnost a dále působením v pracovní skupině pro Smart Cities v krajském městě Pardubice.

Přínosy práce budou využitelné při inovování interních procesů v rámci organizací nejen při inovování prvotního procesu přípravy nových bezpečnostních standardů a nových právních předpisů. Metody mohou nalézt uplatnění i u menších organizací v případě zavádění inovativních procesů, byť jen v případě využití metody pro zpracovávání textu. Vždy záleží na velikosti organizace, finančních možnostech a ochotě vedení inovovat interní procesy dané organizace.

Další přínos lze nalézt v návaznosti na studovaný obor, kdy oblast informačního a znalostního managementu a jejich metod vnáší do procesu přípravy nových právních předpisů a nových bezpečnostních standardů inovativní prvky s možností využití ve vládních organizacích a bezpečnostních složkách. Navrhované metody z oblastí informačního a znalostního managementu mohou být prvotním aspektem pro budoucí implementace těch či jiných metod u vládních organizací a bezpečnostních složek státu, u kterých byla tato problematika doposud převážně opomíjena či řešena minimálně.

Celkové přínosy práce naleznou uplatnění pro oblast prvotní přípravy nových bezpečnostních standardů, nových právních předpisů, dalších interních procesů a současně napomohou dalšímu rozvoji při zavádění metod a prvků z oblastí znalostního a informačního managementu v doposud opomíjených vládních organizacích a bezpečnostních složkách státu a dále při implementaci dílčích tematických částí koncepce Smart Cities v krajích, městech a obcích.

Tato práce může být současně i přínosem pro další rozvoj řešené problematiky například v souvislosti s postupnou implementací prvků umělé inteligence do oblasti přípravy nových právních předpisů v České republice.

7 INFORMAČNÍ ZDROJE A AUTORSKÉ PUBLIKACE

7.1 Informační zdroje

2.17 Internet of Things Cybersecurity Improvement Act of 2020. (2020). https://www.cio.gov/handbook/it-laws/iot/

181/2014 Sb. Zákon o kybernetické bezpečnosti, Pub. L. No. 181/2014 (2015). https://www.zakonyprolidi.cz/cs/2014-181

Abbaspour, A., Amirkhani, A. H., Ezzat, A. A. P., & Hozori, M. J. (2018). Identifying and describing sub-processes in the strategic intelligence process by qualitative content analysis in an inductive way. *Journal of Intelligence Studies in Business*, *8*(1), 16–24. https://doi.org/10.37380/jisib.v8i1.302

Abdalla, W., Renukappa, S., & Suresh, S. (2023). Managing COVID-19-related knowledge: A smart cities perspective. *Knowledge and Process Management*, *30*(1), 87–109. https://doi.org/10.1002/kpm.1706

Abdel-Razig, S., Anglade, P., & Ibrahim, H. (2021). Impact of the COVID-19 Pandemic on a Physician Group's WhatsApp Chat: Qualitative Content Analysis. *Jmir Formative Research*, *5*(12), e31791. https://doi.org/10.2196/31791

Abdullah, Z., Anumudu, C. E., & Raza, S. H. (2022). Examining the digital organizational identity through content analysis of missions and vision statements of Malaysian and Singaporean SME company websites. *Bottom Line*, *35*(2/3), 137–158. https://doi.org/10.1108/BL-12-2021-0108

Abedini, S., & Broujeni, R. B. (2016). Teacher Creativity in University Students' Views: A Content Analysis. *International Journal of Pharmaceutical Research and Allied Sciences*, *5*(3), 379–386.

Andrukiewicz, E., Cadzow, S., & Górniak, S. (2018). *IoT Security Standards Gap Analysis*. European Union Agency For Network and Information Security.

Ashley, K. D. (2017). *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*. Cambridge University Press. https://doi.org/10.1017/9781316761380

Bagherzadeh, M., Gurca, A., & Brunswicker, S. (2022). Problem Types and Open Innovation Governance Modes: A Project-Level Empirical Exploration. *IEEE Transactions on Engineering Management*, *69*(2), 287–301. https://doi.org/10.1109/TEM.2019.2942132

Baseline Security Recommendations for IoT. (2017). [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

Bass, I., Pothong, K., & Hasham, M. (2020). *Navigating and Informing the IoT Standards Landscape*. BSI Standards Ltd.

Beaulieu, R. (2020, srpen 11). *Automation and the Future of Legal Drafting Technology*. SCL Student Bytes. https://bytes.scl.org/automation-and-the-future-of-legal-drafting-technology/

Buheji, M., Al-Hasan, S., Thomas, B., & Melle, D. (2014). The Influence of Knowledge Management on Learning in Government Organisations. *American Journal of Industrial and Business Management*, *04*(11), Article 11. https://doi.org/10.4236/ajibm.2014.411071

Bureš, V. (2007). *Znalostní management a proces jeho zavádení: Průvodce pro praxi* (1. vyd). Grada.

Burns, M. J. (2018). *IES-City Framework*. 150.

Butler, T., Feller, J., Pope, A., Emerson, B., & Murphy, C. (2008). Designing a core IT artefact for Knowledge Management Systems using participatory action research in a government and a non-government organisation. *The Journal of Strategic Information Systems*, *17*(4), 249–267. https://doi.org/10.1016/j.jsis.2007.10.002

Cilliers, L., & Flowerday, S. (2014). Information security in a public safety, participatory crowdsourcing smart city project. *World Congress on Internet Security (WorldCIS-2014)*, 36–41. https://doi.org/10.1109/WorldCIS.2014.7028163

Clark, A. (1992). Information Technology in Legal-Services. *Journal of Law and Society*, *19*(1), 13–30. https://doi.org/10.2307/1410026

Co je dron? (2022). Droneweb. http://www.droneweb.cz/co-je-dron

Co je hodnocení dopadů regulace | ria.vlada.cz. (2022). https://ria.vlada.cz/ria/

Code of Practice for Consumer IoT Security. (2018). GOV.UK. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security

Coffey, A., & Atkinson, P. (1996). *Making sense of qualitative data: Complementary research strategies*. Sage Publications.

Collective of authors. (2017). *Internet of Things Security Guideline*. IoT Alliance Austria. https://www.iot.org.au/wp/wp-content/uploads/2016/12/IoTAA-Security-Guideline-V1.2.pdf

collective of authors. (2019). *IMDA IoT Cyber Security Guide Version 1*. IMDA.

CSA IoT Security Controls Framework. (2019). CSA. https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/

Cyber Resilience Act | Shaping Europe's digital future. (2022, září 15). https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

Častorál, Zdeněk. (2008). *Strategický znalostní management a učící se organizace* (1. vyd). Vysoká škola finanční a správní.

Davenport, T., & Prusak, L. (1998). Working Knowledge: How Organizations Manage What They Know. In *Ubiquity* (Roč. 1). https://doi.org/10.1145/348772.348775

De Haes, S., & van grembergen, W. (2009). An Exploratory Study into IT Governance Implementations and its Impact on Business/IT Alignment. *IS Management*, *26*, 123–137. https://doi.org/10.1080/10580530902794786

Denzin, N. K., & Lincoln, Y. S. (Ed.). (2018). *The SAGE handbook of qualitative research* (Fifth edition). SAGE.

Dey, I. (2016). *Qualitative data analysis: A user-friendly guide for social scientists*. Routledge, Taylor & Francis Group.

Diddi, P., & Lundy, L. K. (2017). Organizational Twitter Use: Content Analysis of Tweets during Breast Cancer Awareness Month. *Journal of Health Communication*, *22*(3), 243–253. Scopus. https://doi.org/10.1080/10810730.2016.1266716

Dolák, R. (2018). *Informační management: Distanční studijní text*. Slezská univerzita, Obchodně podnikatelská fakulta v Karviné.

Dvořák, L. (2013, únor 21). *Management znalostí: Využívání tacitních a explicitních znalostí*. https://www.hrnews.cz/lidske-zdroje/rozvoj-id-2698897/management-znalosti-vyuzivani-tacitnich-a-explicitnich-znalo-id-1799523

Emil Berg, M., Dean, G., Gottschalk, P., & Terje Karlsen, J. (2008). Police management roles as determinants of knowledge sharing attitude in criminal investigations. *International Journal of Public Sector Management*, *21*(3), 271–284. https://doi.org/10.1108/09513550810863178

ETSI TS 103 645 Cyber Security for Consumer Internet of Things. (2019). https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

Eurosmart | The voice of the Digital Security Industry | Eurosmart IoT Certification Scheme. (2019). https://www.eurosmart.com/eurosmart-iot-certification-scheme/

Fekete, B., & Bubori, B. (2019). *Legislative Processes and ICT*.

Force, J. T. (2020). *Security and Privacy Controls for Information Systems and Organizations* (NIST Special Publication (SP) 800-53 Rev. 5). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-53r5

Goller, I., & Bessant, J. R. (2017). *Creativity for innovation management: Ina Goller and John Bessant* (First published 2017). Routledge.

Good Practices for Security of Internet of Things in the context of Smart Manufacturing. (2018). [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot

Grega, L., Miškolci, S., & Zdráhal, I. (2018). *Analýza aktuální úrovně zapojení ČR do konceptu smart city a smart region v souvislosti s novými trendy, včetně návrhů opatření*. Mendelova univerzita v Brně. https://www.vlada.cz/assets/evropske-zalezitosti/aktualne/Zaverecna-zprava_Smart_City_a_Smart_Region.pdf

Grublová, E., & Franek, Jiří. (2014). *Inovace a znalosti* (1. vyd). Univerzita Palackého v Olomouci.

Harmer, G. (2014). *Governance of Enterprise IT based on COBIT 5: A Management Guide*. IT Governance Ltd. https://www.perlego.com/book/5793/governance-of-enterprise-it-based-on-cobit-5-a-management-guide-pdf

Havelda, Z., Burian, D., & Pořízka, A. (2024). *Metodika k návrhu a provozování kamerových systémů z hlediska zpracování osobních údajů*. Úřad pro ochranu osobních údajů. https://uoou.gov.cz/media/clanky/dokumenty/metodika-kamerove-systemy-webpdf.pdf

Hendl, J. (2005). *Kvalitativní výzkum: Základní metody a aplikace*. Portál.

Hendl, J. (2016). *Kvalitativní výzkum: Základní teorie, metody a aplikace*.

Henry, N., Donkin, L., Williams, M., & Pedersen, M. (2022). mHealth Technologies for Managing Problematic Pornography Use: Content Analysis. *JMIR Formative Research*, *6*(10). Scopus. https://doi.org/10.2196/39869

Héroux, S., & Fortin, A. (2018). The moderating role of IT-business alignment in the relationship between IT governance, IT competence, and innovation. *Information Systems Management*, *35*(2), 98–123. https://doi.org/10.1080/10580530.2018.1440729

Hollands, R. G. (2008). Will the real smart city please stand up? *City*, *12*(3), 303–320. https://doi.org/10.1080/13604810802479126

Holzmann, P., Wankmüller, C., Globocnik, D., & Schwarz, E. J. (2021). Drones to the rescue? Exploring rescue workers' behavioral intention to adopt drones in mountain rescue missions. *International Journal of Physical Distribution & Logistics Management*, *51*(4), 381–402. https://doi.org/10.1108/IJPDLM-01-2020-0025

Checklist on Law Drafting and Regulatory Management in Central and Eastern Europe (SIGMA Papers 15; SIGMA Papers, Roč. 15). (1997). https://doi.org/10.1787/5kml6g2zl0bw-en

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., Pardo, T. A., & Scholl, H. J. (2012). Understanding Smart Cities: An Integrative Framework. *2012 45th Hawaii International Conference on System Sciences*, 2289–2297. https://doi.org/10.1109/HICSS.2012.615

Chytrá karanténa – Aktuální informace o COVID-19. (2020). https://koronavirus.mzcr.cz/chytra-karantena/

IoT Cybersecurity Certification. (2019). CTIA Certification. https://ctiacertification.org/program/iot-cybersecurity-certification/

IoT Product Criteria. (2021). *NIST*. https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/iot-product-criteria

IoT Security Assessment. (2020). *Internet of Things*. https://www.gsma.com/iot/iot-security-assessment/

Jirotková, S., Dzurilla, V., & Kratochvíl, J. (2019). *Inovační strategie České republiky 2019—2030*. https://www.vyzkum.cz/FrontClanek.aspx?idsekce=866015

Joh, E. E. (2019). Policing the smart city. *International Journal of Law in Context*, *15*(2), 177–182. https://doi.org/10.1017/S1744552319000107

Khan, Md. N. H., & Neustaedter, C. (2019, květen). Exploring Drones to Assist Firefighters During Emergencies. *1st International Workshop on Human-Drone Interaction*. https://hal.archives-ouvertes.fr/hal-02128386

Khoumeri, E.-H., Cheggou, R., & Farhah, K. (2018). IoT-Safety and Security System in Smart Cities. In M. Hatti (Ed.), *Artificial Intelligence in Renewable Energetic Systems* (s. 25–33). Springer International Publishing. https://doi.org/10.1007/978-3-319-73192-6_3

Klíma, K. (2010). *Ústavní právo* (4., rozšířené vydání). Vydavatelství a nakladatelství Aleš Čeněk, s.r.o.

Knapp, V. (1963). *O možnosti využití kybernetických metod v právu* (1., Roč. 1963). Československá akademie věd.

Kněžínek, J., Mlsna, P., & Vedral, J. (2010). *Příprava návrhů právních předpisů: Praktická pomůcka pro legislativce* (1. vyd). Úřad vlády České republiky.

Knowledge Management in Law Enforcement: Knowledge Views for Patrolling Police Officers—Stefan Holgersson, Petter Gottschalk, Geoff Dean, 2008. (b.r.). Získáno 16. březen 2024, z https://journals.sagepub.com/doi/abs/10.1350/ijps.2008.10.1.76

Kokeš, M. (2020). *Temná zákoutí legislativního procesu: Příprava vládních návrhů zákonů v ČR* (Vydání první). Leges.

Kolektiv autorů. (2012). *Metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů*. Úřad pro ochranu osobních údajů. file:///C:/Users/Hanka/Downloads/P%C5%99%C3%ADloha+%C4%8D.+4+Smlouvy+Kamerov%C3%BD+syst%C3%A9m+metodika.pdf

Kolektiv autorů. (2018). *Emergency calls in the upcoming EU-legislation*. European Emergency Number Association – EENA 112. https://www.ctif.org/sites/default/files/news_files/2018-11/EECC_briefing_FINAL(1).pdf

Kolektiv autorů. (2019). *Metodická doporučení krajům pro aktualizace krajských RIS3 strategií v programovém období 2021+ | MPO*. https://www.mpo.cz/cz/podnikani/ris3-strategie/krajska-dimenze/metodicka-doporuceni-krajum-pro-aktualizace-krajskych-ris3-strategii-v-programovem-obdobi-2021--247029/

Kolektiv autorů. (2021a). *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025*. NÚKIB.

Kolektiv autorů. (2021b). *Národní výzkumná a inovační strategie pro inteligentní specializaci České republiky 2021 – 2027*.

https://www.mpo.cz/assets/cz/podnikani/ris3-strategie/dokumenty/2021/1/A_RIS3-Strategie.pdf

Kolektiv autorů. (2022). *Metodická příručka: Povinnost aplikace principů 3E při hospodaření územních samosprávných celků*. Ministerstvo financí České republiky. https://www.mfcr.cz/assets/attachments/2022-09-26_CHJ-MP-23-Povinnost-aplikace-principu-3E.pdf

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (Fourth Edition). SAGE.

Kummitha, R. K. R. (2020). Smart technologies for fighting pandemics: The techno- and human- driven approaches in controlling the virus transmission. *Government Information Quarterly*, 101481. https://doi.org/10.1016/j.giq.2020.101481

Laihonen, H., & Mäntylä, S. (2018). Strategic knowledge management and evolving local government. *Journal of Knowledge Management*, *22*(1), 219–234. https://doi.org/10.1108/JKM-06-2017-0232

Liebowitz, J. (2004). Will knowledge management work in the government? *Electronic Government, an International Journal*, *1*(1), 1–7. https://doi.org/10.1504/EG.2004.004133

Lisa, A. (2015). *6 ways people are using aerial drones for good*. https://inhabitat.com/6-of-the-best-uses-for-aerial-robot-drones/

Lloyd, I. J. (2020). *Information Technology Law* (Ninth edition). Oxford University Press.

Lombard, M., Snyder-Duch, J., & Campanella Bracken, C. (2004). *Practical Resources for Assessing and Reporting Intercoder Reliability in Content Analysis Research Projects*. https://www.researchgate.net/publication/242785900_Practical_Resources_for_Assessing_and_Reporting_Intercoder_Reliability_in_Content_Analysis_Research_Projects

Loughran, J. (2017, červenec 14). *Two police forces introduce drone units in "historic" first for law enforcement*. https://eandt.theiet.org/content/articles/2017/07/two-police-forces-introduce-drone-units-in-historic-first-for-law-enforcement/

Lubua, E. W. (2017). E-Governance and the ICT Legislative Framework. *The International Journal of Engineering and Science*, *06*(03), 116–121. https://doi.org/10.9790/1813-060301116121

Lukáš, L., Hrůza, P., & Kný, M. (2008). *Informační management v bezpečnostních složkách* (1. vyd). Ministerstvo obrany České republiky.

Magnusson, J., Koutsikouri, D., & Päivärinta, T. (2020). Efficiency creep and shadow innovation: Enacting ambidextrous IT Governance in the public sector. *European Journal of Information Systems*, *29*(4), 329–349. https://doi.org/10.1080/0960085X.2020.1740617

Manning, P. K. (1992). Information Technologies and the Police. *Crime and Justice*, *15*, 349–398. https://doi.org/10.1086/449197

Mapping of IoT security recommendations, guidance and standards. (2018). GOV.UK. https://www.gov.uk/government/publications/mapping-of-iot-security-recommendations-guidance-and-standards

Mapy.cz. (2020). Mapy.cz. https://mapy.cz/?

Mašínová, L. K., Herbstová, H., & Krejčí, T. (2008). *Analýza a mapování potřeb uživatelů a práce s informacemi v komunitním plánování*. Centrum komunitní práce Ústí nad Labem. https://www.mpsv.cz/documents/20142/225517/05_metodika.pdf/c272dc02-77e4-78f5-d5f2-b930d6944069

Matula, J. (2017). *Informační management: Normy, frameworky a nejlepší praxe v řízení služeb IT (ITSM)* (První vydání). Slezská univerzita, Filozoficko-přírodovědecká fakulta v Opavě, Ústav bohemistiky a knihovnictví.

Matyášek, D. (2019). *Vnitřní směrnice o provozování kamerového systému*. Štítina. http://zsstitina.cz/wpweb/wp-content/uploads/2019/09/Sme%CC%8Crnice-kamerove%CC%81ho-syste%CC%81mu.pdf

Mayring, P. (2021). *Qualitative content analysis: A step-by-step guide*. SAGE Publications.

Misra, D. C., Hariharan, R., & Khaneja, M. (2003). E-Knowledge Management Framework for Government Organizations. *Information Systems Management*. https://doi.org/10.1201/1078/43204.20.2.20030301/41469.7

Misuraca, G., & Viscusi, G. (2015). Shaping public sector innovation theory: An interpretative framework for ICT-enabled governance innovation. *Electronic Commerce Research*, *15*(3), 303–322. https://doi.org/10.1007/s10660-015-9184-5

Moore, T. (2019). The Upgraded Lawyer: Modern Technology and Its Impact on the Legal Profession. *University of the District of Columbia Law Review*, *21*(1), 27.

Moses, L. B., & Chan, J. (2014). Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools. *University of New South Wales Law Journal*, *37*(2), 642–677.

Mousmouti, M. (2019). Which tools for effective lawmaking? In *Designing Effective Legislation* (s. 108–128). Edward Elgar Publishing. https://www.elgaronline.com/display/9781788118224.00011.xml

Nam, T., & Pardo, T. (2011). *Conceptualizing smart city with dimensions of technology, people, and institutions*. 282–291. https://doi.org/10.1145/2037556.2037602

Národní úřad pro kybernetickou a informační bezpečnost—Jednotná pravidla kybernetické bezpečnosti subjektů EU jsou opět o něco blíž. (2022). https://nukib.cz/cs/infoservis/aktuality/1910-jednotna-pravidla-kyberneticke-bezpecnosti-subjektu-eu-jsou-zase-o-neco-bliz/

Nemocnice pod náporem hackerů: Jak proběhly nejznámější kyberútoky na české nemocnice? (2021). https://blog.avast.com/cs/nemocnice-pod-naporem-hackeru-jak-probihaji-kyberutoky-na-ceske-nemocnice

Nencková, L., & Bízková, R. (2021). *Koncepce Smart Cities—Odolnost prostřednictvím SMART řešení pro obce, města a regiony*. *2021*.

NISTIR 8259 Series | NIST. (2020). https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press.

Obsahová analýza | Katedra antropologie. (2014). http://www.antropologie.org/cs/metodologie/obsahova-analyza

Oddělení bezpečnostního výzkumu MVČR. (2017). *Meziresortní koncepce podpory bezpečnostního výzkumu ČR 2017–2023 s výhledem do roku 2030*. Ministerstvo vnitra ČR, úsek veřejné správy.

Odusanya, K. (2019, leden 1). *Knowledge management in smart city development: A systematic review*.

Ochrana, F. (2009). *Metodologie vědy* (První). Karolinum.

Palmirani, M. (2022). Hybrid AI to Support the Implementation of the European Directive. *Lecture Notes in Computer Science (Including Subseries Lecture Notes*

in Artificial Intelligence and Lecture Notes in Bioinformatics), *13429 LNCS*, 110–122. Scopus. https://doi.org/10.1007/978-3-031-12673-4_8

Pavlíček, V., & Kolektiv autorů. (2011). *Ústavní právo a státověda, II. díl. Ústavní právo České republiky.* (1. vyd.). Leges.

Pitra, Z., & Mohelská, H. (2015). *Management transferu znalostí: Od prvního nápadu ke komerčně úspěšné inovaci* (1. vyd). Professional Publishing.

Plecas, D., McCormick, A. V., Levine, J., Neal, P., & Cohen, I. M. (2011). Evidence-based solution to information sharing between law enforcement agencies. *Policing: An International Journal of Police Strategies & Management*, *34*(1), 120–134. https://doi.org/10.1108/13639511111106641

Pracovní skupina pro Smart Cities. (2018). *Metodika pro přípravu a realizaci konceptu Smart Cities na úrovni měst, obcí a regionů*. Ministerstvo pro místní rozvoj ČR. https://mmr.cz/getmedia/f76636e0-88ad-40f9-8e27-cbb774ea7caf/Metodika_Smart_Cities.pdf.aspx?ext=.pdf

PricewaterhouseCoopers. (2021, prosinec 21). *Drones in Smart Cities*. PwC. https://www.pwc.pl/en/drone-powered-solutions/Articles/drones-in-smart-cities.html

Přístupy do informačních systémů Policie České republiky pro obecní policie—Ministerstvo vnitra České republiky. (2019). https://www.mvcr.cz/clanek/pristupy-do-informacnich-systemu-policie-ceske-republiky-pro-obecni-policie.aspx

Ptašnik, A. (2007). *Automatizované zpracování právních textů* (Vyd. 1). Key Publishing.

Ptitsyna. (2022, říjen 19). The Role of Legal Tech in Drafting & Reviewing Energy Documents. *Artificial Lawyer*. https://www.artificiallawyer.com/2022/10/19/the-role-of-legal-tech-in-drafting-reviewing-energy-documents/

Půček, J. (2020). *Techniky efektivního řízení měst a obcí: Část SWOT analýza (metodika)*. Národní síť Zdravých měst ČR. https://www.dataplan.info/img_upload/f96fc5d7def29509aeffc6784e61f65b/analyza-swot-metodika.pdf

Radziszewska, A. (2023). Data-Driven Approach in Knowledge-Based Smart City Management. *European Conference on Knowledge Management*, *24*(2), Article 2. https://doi.org/10.34190/eckm.24.2.1600

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA Relevance), Pub. L. No. 32019R0881, 151 OJ L (2019). http://data.europa.eu/eli/reg/2019/881/oj/eng

Riffe, D., Lacy, S., Watson, B. R., & Fico, F. (2019). *Analyzing media messages: Using quantitative content analysis in research* (Fourth edition). Routledge, Taylor & Francis Group.

Rodiyah, R., Damayanti, R., Wedhatami, B., Arifin, R., & Sulistiyono, T. (2022). *The future impact of technological advancement in the legal drafting process: A human and technology analysis*. *2573*. Scopus. https://doi.org/10.1063/5.0104135

Řiháček, T., Čermák, I., & Hytych, R. (2013). *Kvalitativní analýza textů: Čtyři přístupy*. Masarykova univerzita.

Říhová, Z. (2018). *Úvod do IT Governance* (Vydání první). Oeconomica, nakladatelství VŠE.

Sandbrink, J., Hobbs, H., Swett, J., Dafoe, A., & Sandberg, A. (2022). *Differential technology development: An innovation governance consideration for navigating technology risks* (SSRN Scholarly Paper 4213670). https://doi.org/10.2139/ssrn.4213670

Sartor, G. (2011). Introduction: ICT and Legislation in the Knowledge Society. In G. Sartor, M. Palmirani, E. Francesconi, & M. A. Biasiotti (Ed.), *Legislative XML for the Semantic Web: Principles, Models, Standards for Document Management* (s. 1–10). Springer Netherlands. https://doi.org/10.1007/978-94-007-1887-6_1

Seba, I., & Rowley, J. (2010). Knowledge management in UK police forces. *Journal of Knowledge Management*, *14*(4), 611–626. https://doi.org/10.1108/13673271011059554

Schneider, B., Wheeler, J. K., & Cox, J. F. (1992). A passion for service: Using content analysis to explicate service climate themes. *Journal of Applied Psychology*, *77*, 705–716. https://doi.org/10.1037/0021-9010.77.5.705

Schreier, M. (2012). *Qualitative content analysis in practice*. SAGE.

Směrnice Evropského parlmentu a Rady ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice

(EU) 2016/1148 (2022). https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2555&from=CS

Smith, S. M., & Aamodt, M. G. (1997). The relationship between education, experience, and police performance. *Journal of Police and Criminal Psychology*, *12*(2), 7–14. https://doi.org/10.1007/BF02806696

Songkram, N., & Chootongchai, S. (2020). Effects of pedagogy and information technology utilization on innovation creation by SECI model. *Education and Information Technologies*, *25*(5), 4297–4315. https://doi.org/10.1007/s10639-020-10150-2

SP 800-213 Series. (2021). *NIST*. https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/sp-800-213-series

Stříteská, M. (2008). *Balanced Scorecard jako inovativní nástroj strategického managementu obcí a regionů* [Disertační práce, Univerzita Pardubice]. https://dk.upce.cz/bitstream/handle/10195/34524/Dizertace_Striteska.pdf;sequence=1

Střížová, V. (2007). *Systémové pojetí (hospodářské) organizace* (Vyd. 1). Oeconomica.

Svecova, H. (2022). Design of a Method for Setting IoT Security Standards in Smart Cities. In I. Awan, M. Younas, & A. Poniszewska-Marańda (Ed.), *Mobile Web and Intelligent Information Systems* (s. 118–128). Springer International Publishing. https://doi.org/10.1007/978-3-031-14391-5_9

Swimmer, G. (1974). The Relationship of Police and Crime. *Criminology*, *12*(3), 293–314. https://doi.org/10.1111/j.1745-9125.1974.tb00637.x

Špaček, F. (2009). *Integrovaný záchranný systém—Hasičský záchranný sbor České republiky*. https://www.hzscr.cz/clanek/integrovany-zachranny-system.aspx

Šrámková, H. (2007). *Možnosti využití systémů pro podporu zákazníků v prostředí univerzity* [Disertační práce]. Univerzita Hradec Králové.

Švecová, H., & Blažek, P. (2021). The Impact of Cybersecurity on the Rescue System of Regional Governments in SmartCities. *Recent Challenges in Intelligent Information and Database Systems*, *2021*.

Tesorero, A. (2021, prosinec 21). *Drones to monitor Dubai roads in 2017*. Khaleej Times. https://www.khaleejtimes.com/uae/drones-to-monitor-dubai-roads-in-2017

Ústavní zákon č. 1/1993 Sb., Pub. L. No. 1/1993 (1992).

Vedral, J. (2006). *Metodická pomůcka pro přípravu návrhů právních předpisů (I*. Úřadu vlády ČR.

Velebilová, T. (2022). *Vnitřní předpis zaměstnavatele stanovící postupy v souvislosti se zavedením kamerových systémů*. Linksoft. https://www.linksoft.eu/media/documents/Smernice-kamerovy-system-CZ.pdf

Vláda ČR. (b.r.). *RIA - Hodnocení dopadů regulace*. Získáno 31. leden 2024, z https://vlada.gov.cz/cz/ppov/lrv/ria/hodnoceni-dopadu-regulace-160402/#

Vlček, R. (2008). *Management hodnotových informací*. Management Press.

Vogiatzaki, M., Zerefos, S., & Hoque Tania, M. (2020). Enhancing City Sustainability through Smart Technologies: A Framework for Automatic Pre-Emptive Action to Promote Safety and Security Using Lighting and ICT-Based Surveillance. *Sustainability*, *12*(15), Article 15. https://doi.org/10.3390/su12156142

Vološčuk, D. (2019). *Směrnice o podmínkách provozování kamerového systému se záznamem a ochraně osobních údajů*. ARMAT s.r.o. https://armat.cz/wp-content/uploads/2019/05/Sm%C4%9Brnice-kamerov%C3%BD-syst%C3%A9m.pdf

Vyhláška č. 82/2018 Sb., obezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), Pub. L. No. 82/2018 (2018).

Vyleťal, P. (2014). *Přístupy k hodnocení akvizic—Efektivnost, hospodárnost, účelnost*. https://moodle.unob.cz/pluginfile.php/43093/mod_resource/content/2/Prezentace%20-%20P%C5%99%C3%ADstupy%20k%20hodnocen%C3%AD%20akvizic.pdf

Vymětal, J., Diačiková, A., & Váchová, M. (2005). *Informační a znalostní management v praxi* (1. vyd). LexisNexis CZ.

Využití dronů pro Integrovaný záchranný systém. (2020). *Smart City Plzeň*. https://smartcity.plzen.eu/projekty-ziti/vyuziti-dronu-pro-integrovany-zachranny-system/

Ward, V. (2016). *Police to use drones to aid criminal investigations* [Http://www.telegraph.co.uk/]. http://www.telegraph.co.uk/news/uknews/crime/12081915/Police-to-use-drones-to-aid-criminalinvestigations.html

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Zákon č. 110/2019 Sb., Zákon o zpracování osobních údajů (2019).

Zákon č. 320/2001 Sb., Zákon o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole). https://www.e-sbirka.cz/sb/2001/320/

Zákon č. 553/1991 Sb. , o obecní policii (1991). https://www.zakonyprolidi.cz/cs/1991-553#f1395038

Zákon o krizovém řízení a o změně některých zákonů (krizový zákon), Pub. L. No. 240 (2000).

Zákonodárný proces v Česku. (2022). In *Wikipedie*. https://cs.wikipedia.org/w/index.php?title=Z%C3%A1konod%C3%A1rn%C3%BD_proces_v_%C4%8Cesku&oldid=20795572

Zháněl, J., Hellebrandt, V., & Sebera, M. (2014). *Metodologie výzkumné práce* (1.). Masarykova univerzita.

Zhang, Z., & Huang, F. (2020). An extended SECI model to incorporate inter-organisational knowledge flows and open innovation. *International Journal of Knowledge Management Studies*, *11*(4), 408–419. https://doi.org/10.1504/IJKMS.2020.110671

7.2 Autorské publikace a VaV projekty související s tématem

7.2.1 Výstupy typu J

DŮBRAVOVÁ Hana, BUREŠ Vladimír. Smart City Information Systems: Research on Information Published for Citizens and Design of Effective Content in the Czech Republic. Smart Cities Journal. 2023, Volume 6, Issue 5, page 2960-2981. ISSN 2624-6511.

7.2.2 Výstupy typu D

DŮBRAVOVÁ, Hana a Vladimír BUREŠ, Lukáš VELFL. Drones as an Example of the Use of Smart Technologies in Cooperation with the State Security Forces in the Context of the Smart Cities Concept in the Czech Republic. International Conference on International Conference on Industry Science and Computer Sciences Innovation. Lisabon 2023. Elsevier, 2024.

DŮBRAVOVÁ Hana, Kristyna HOLUBOVÁ, Jan ČÁP a Lukáš HŘIBŇÁK. Artificial Intelligence as an Innovative Element of Support in Policing. International Conference on International Conference on Industry Science and Computer Sciences Innovation. Lisabon 2023. Elsevier, 2024.

ŠVECOVÁ, Hana. Design of the Content Part of the Information System in Smart Cities from the Perspective of Regional Governments and Security of Residents. Innovations in Smart Cities Applications. Volume 6. SCA 2022. Lecture Notes in Networks and Systems, vol 629. Springer, Cham. https://doi.org/10.1007/978-3-031-26852-6_17

ŠVECOVÁ, Hana. Design of a Method for Setting IoT Security Standards in Smart Cities. Mobile Web and Intelligent Information Systems. MobiWIS 2022. Lecture Notes in Computer Science, vol 13475. Springer, Cham. https://doi.org/10.1007/978-3-031-14391-5_9

SOBESLAV Vladimír, Jan HORÁLEK, Tomáš SVOBODA a Hana ŠVECOVÁ. Security Consideration of BIA Utilization in Smart Electricity Metering Systems. Computational Collective Intelligence. ICCCI 2022. Lecture Notes in Computer Science (), vol 13501. Springer, Cham. https://doi.org/10.1007/978-3-031-16014-1_46

MIKULECKÝ, Peter et al. An Architecture for Intelligent e-Learning Platform for Student's Lab Deployment. Springer International Publishing, 2021:ICTCC 2020. Lecture Notes of the Institute for Computer Sciences. Social Informatics and Telecommunications Engineering. s. 288-299. https://link.springer.com/chapter/10.1007/978-3-030-67101-3_23

ŠVECOVÁ, Hana a Pavel BLAŽEK. The Impact of Cybersecurity on the Rescue System of Regional Governments in SmartCities. Springer, 2021. Communications in Computer and Information Science: sborník z konference Asian Conference on Intelligent Information and Database Systems. s. 365-375. ISBN 9789811616853. https://doi.org/10.1007/978-981-16-1685-3_30

7.2.3 VaV projekty související s tématem

Projekt 2021–2022: APLIKACE VIII. - CZ.01.1.02/0.0/0.0/20_321/0024477, „Smart Parking & Charging". Role – člen řešitelského týmu.

Projekt 2021–2022: TAČR GAMA – TP01010032 – Security baseline pro energetické řídicí systémy stanic. Role – člen řešitelského týmu.

Projekt 2023–2027 OPSEC VK01020187 Odolnost příslušníků Policie České republiky vůči dezinformačním vlivům a možnosti posilování jejich rezistence prostřednictvím vzdělávání. Role – člen řešitelského týmu.

Projekt DiForPol – mezinárodní projekt řešený v rámci sasko-české spolupráce v rámci Interreg zaměřený na spolupráci při přípravě vzdělávacích materiálů a školení pro policejní složky v rámci spolupráce Policejní akademie ČR v Praze a Hochschule Mittweida University of Applied Sciences. Poznámka: termín schválení nebo zamítnutí březen/duben 2024.

PŘÍLOHA 1 – Žádost podle zákona o svobodném přístupu k informacím – Krajský úřad Pardubického kraje

ŽÁDOST O POSKYTNUTÍ INFORMACE

podle zákona č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů

Žadatel: Ing. Bc. Hana Důbravová, 20.10. 1982

Adresa (bydliště nebo sídlo): Na Obci 396, Moravany 533 72

Telefon: +420 723 905 183 **e-mail:** dubravova@polac.cz (Policejní akademie ČR v Praze)

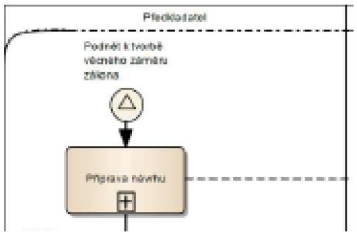
žádá: Krajský úřad Pardubického kraje, Odbor organizační, a právní a krajský živnostenský úřad, Oddělení legislativní podpory o poskytnutí informací podle zákona č. 106/1999 Sb. v souvislosti s řešením výzkumného cíle v rámci zpracovávání disertační práce.

Vážená paní, Vážený pane,

V souvislosti s řešením výzkumného úkolu při zpracovávání disertační práce Váš žádám o poskytnutí relevantních informací k řešené problematice uvedené níže. Z hlediska komplexního řešení dané problematiky, je tato problematika současně řešena i na národní úrovni, obdobná žádost tedy bude zaslána i organizacím podílejícím se na přípravě návrhu nových legislativních norem i na národní úrovni.

Z hlediska zákonodárného procesu se Krajský úřad Pardubického kraje (dále KrÚ Pk) podílí na přípravě návrhů nových legislativních norem a jiných právních předpisů (zákonodárná iniciativa krajů). V souvislosti s prvotní přípravou nových legislativních norem a dalších právních předpisů Vás žádám o poskytnutí informací v podobě popisu postupu (procesu) jakým způsobem tato prvotní příprava probíhá a jaké činnosti (aktivity) jsou ze strany zaměstnanců Vašeho úřadu výše uvedeného odboru realizovány a s využitím jakého software.

Z hlediska grafického schématu celého procesu přípravy a schvalování nových legislativních norem je myšlena konkrétně část grafického schématu, jehož část přikládám níže, a současně je toto schéma dostupné ve veřejném dokumentu na obr. č. 82 v kapitole 6.2.1.1.1 Příprava návrhu (Aktiva) na straně 296 v dokumentu s názvem *„Detailní návrh technického řešení informačních systémů e-Sbírka a e-Legislativa"*, který je veřejně dostupný v Registru smluv pro zobrazení celého schématu na https://smlouvy.gov.cz/smlouva/soubor/9402067/Ver_P2_1ANON.pdf



Při přípravě návrhu nových legislativních norem a dalších právních předpisů jsou využívány i prostředky informačních technologií zejména software (dále SW). Jaký typ SW je využíván ze strany Vašich zaměstnanců např. textový editor, software pro sdílení dat, můžete sdělit přesný název využívaného software?

V souvislosti s výše uvedeným dotazem Vás dále žádám o sdělení informací z hlediska finančních nákladů při přípravě návrhů nových legislativních norem, a dalších právních předpisů: Jaká obvyklá průměrná časová dotace je vynaložena (v počtu hodin na osobu) a v jakém počtu zaměstnanců tato prvotní příprava návrhu nové legislativní normy či jiného nového právního předpisu s využitím software probíhá?

Dále pak prosím o vyčíslení celkového času a počtu zaměstnanců, který je obvykle průměrně vynaložen v rámci odborných konzultací při jednání ve formě on-line nebo s osobní účastí nad připravovanou novou legislativní normou či jiným novým právním předpisem, tj. před zahájením samotné přípravy návrhu nové legislativní normy ze strany Vašich zaměstnanců s využitím software.

Dále žádám o sdělení informací, jakým způsobem probíhá na Vašem úřadu při přípravě návrhů nových legislativních norem či jiných právních předpisů zavádění inovací pro zvyšování efektivity, čímž dochází současně ke snižování vynaloženého času a současně ke snižování celkových finančních nákladů. Je tato problematika na KrÚ Pk řešena nebo nikoliv, či případně plánuje se zavádění inovací při náplni této pracovní činnosti, pokud ano, v jakém časovém období a jaké inovace plánujete implementovat v jakém časovém období na základě jaké metody bude provedeno zhodnocení implementovaných inovací? Je při implementaci inovací postupováno v souladu s Metodickým pokynem CHJ č. 23 Ministerstva Financí České republiky (Povinnost aplikace principů 3E při hospodaření územních samosprávných celků)?

Dále, zdali jsou v rámci zavádění inovací na Vašem úřadu využívány frameworky z oblasti Informačního a Znalostního managementu např. IT Governance (IG), Enterprise Information Management (EIM) či jiné?

Děkuji za Vaši pomoc a spolupráci při řešení výzkumného úkolu. V případě potřeby pro doplnění mé žádosti mě prosím kontaktuje prostřednictvím uvedeného emailu nebo telefonicky.

S úctou a přáním hezkého dne

Ing. Bc. Hana Důbravová

Způsob poskytnutí informace:

b) zaslat do datové schránky – ID 862md3f

Ing. Hana Důbravová

Digitálně podepsal Ing. Hana Důbravová
Datum: 2023.12.14

Dne: 14.12. 2023 **Podpis:** .....

PŘÍLOHA 2 – Odpověď na žádost podle zákona o svobodném přístupu k informacím ze strany Krajského úřadu Pardubického kraje – ověření skutečného stavu

KUPAX017ASTN

KRAJSKÝ ÚŘAD
Pardubického kraje
odbor organizační a právní a krajský živnostenský úřad
oddělení legislativní a právní podpory

Číslo jednací: KrÚ 102123/2023
Spisová značka: SpKrÚ 100963/2023 OOPKŽÚ OLP
Reg. č.:
Vyřizuje: Mgr. Pavlína Venzarová, MPA
Telefon: 466026170
E-mail: pavlina.venzarova@pardubickykraj.cz
Mobil:

Ing. Bc. Hana Důbravová
Na Obci 396
533 72 Moravany

Datum: 19.12.2023

Poskytnutí informace

Dne 14. 12. 2023 obdržel Krajský úřad Pardubického kraje (dále jen „krajský úřad") Vaši žádost o informace ve smyslu zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „InfZ"). Touto žádostí jste požadovala poskytnutí informací týkajících se přípravy návrhů nových legislativních norem a dalších právních předpisů ze strany Krajského úřadu Pardubického kraje.

K Vaší žádosti sdělujeme, že příprava zákonodárných iniciativ Pardubického kraje náleží do činnosti oddělení legislativního a právní podpory, odbor organizační a právní a krajský živnostenský úřad. Oddělení má tři zaměstnance, přičemž agenda přípravy zákonodárné inciativy je jen jednou z mnoha činností vykonávaných tímto oddělením. Pro ilustraci přikládáme náplň činnosti oddělení dle organizačního řádu. Vyčíslení času věnovaného přípravě návrhu zákona (novely zákona) nelze sdělit, jelikož se nejedná o formalizovaný proces. Každý návrh se liší nejen svým rozsahem, ale také způsobem projednávání, složitostí přípravy a zpracování. Ke zpracování návrhu nemá krajský úřad speciální softwarové vybavení. Zaměstnanci oddělení pracují se standardními nástroji - textovým editorem Word, případně s tabulkovým procesorem EXCEL a při své činnosti využívají právní informační systémy (Aspi, Beck-online, Codexis). Při online konzultacích s jinými kraji, případně s Asociací krajů ČR, je využíván MS Teams.

Od 1. 1. 2025 budou návrhy zákonů, tedy i zákonodárné iniciativy podávány prostřednictvím e-Legislativy. Předpokládá se, že zaměstnanci oddělení budou ze strany Ministerstva vnitra pro práci v tomto prostředí proškoleni.

S pozdravem

Mgr. Pavlína Venzarová, MPA
vedoucí oddělení legislativního a právní podpory
odbor organizační a právní a krajský živnostenský úřad

Příloha: dle texu

PŘÍLOHA 3 – Císař, Čéška, Smutný s. r. o. – ověření skutečného stavu prostřednictvím písemné formy

Ing. Bc. Hana Důbravová

Od: Barbora Vlachová <vlachova@akccs.cz>
Odesláno: čtvrtek 22. února 2024 22:40
Komu: Ing. Bc. Hana Důbravová
Předmět: RE: Validace výstupů disertační práce - inovace v oblasti přípravy legislativního procesu

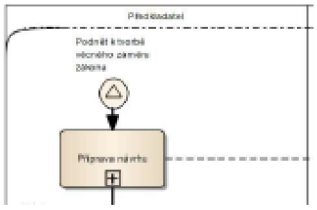
Vážená paní kolegyně,

níže si dovoluji zaslat odpovědi na Vaše otázky, kdy tyto jsou označeny červenou barvou.

V souvislosti s prvotní přípravou nových legislativních norem Vás žádám o poskytnutí informací v podobě popisu postupu (procesu) jakým způsobem tato prvotní příprava probíhá a jaké činnosti (aktivity) jsou ze strany zaměstnanců Vaší kanceláře realizovány a s využitím jakého software?

Pokud se naše advokátní kancelář podílí na přípravě legislativních norem, jsou nejprve především definovány cíle dané legislativní normy. Text je vytvářen za využití a v souladu s Legislativními pravidly vlády. Při samotné přípravě právních předpisů není žádný software využíván.

Z hlediska grafického schématu celého procesu přípravy a schvalování nových legislativních norem je myšlena konkrétně část grafického schématu, jehož část přikládám níže, a současně je toto schéma dostupné na obr. č. 81 nebo obr. č. 81 Příprava návrhu str. 296 „*Detailní návrh technického řešení informačních systémů e-Sbírka a e-Legislativa*", MVČR 2018 dostupné na URL https://smlouvy.gov.cz/smlouva/soubor/9402067/Ver_P2_1ANON.pdf



Při přípravě návrhu nových legislativních norem jsou využívány i prostředky informačních technologií zejména software (dále SW). Jaký typ SW je využíván ze strany Vašich zaměstnanců např. textový editor, software pro sdílení dat, můžete sdělit přesný název využívaného software?

Při přípravě legislativních norem je využíváno pouze textových editorů, žádný jiný software není potřeba.

V souvislosti s výše uvedeným dotazem Vás dále žádám o sdělení informací z hlediska finančních nákladů při přípravě návrhů nových legislativních norem: Jaká obvyklá průměrná časová dotace je vynaložena (v počtu hodin na osobu) a v jakém počtu zaměstnanců tato prvotní příprava návrhu nové legislativní normy s využitím software probíhá?

Uvedené samozřejmě závisí na rozsahu právní normy a účelu, kterého má být novou právní normou dosaženo. Průměrně lze však říci, že na přípravu jedné strany právní normy je třeba časová dotace v délce 1 manday.

Dále pak prosím o vyčíslení celkového času a počtu zaměstnanců, který je obvykle průměrně vynaložen v rámci odborných konzultací při jednání ve formě on-line nebo s osobní účastí nad připravovanou novou legislativní normou, tj. před započením samotné přípravy návrhu nové legislativní normy ze strany Vašich zaměstnanců s využitím software.

To opět závisí na rozsahu právní normy a účelu, kterého má být novou právní normou dosaženo. Průměrně lze však říci, odborné konzultace v rámci přípravy právní normy je třeba časová dotace v délce 1 manday na jednu stranu právní normy.

Dále žádám o sdělení informací, jakým způsobem probíhá na ve Vaší kanceláři při přípravě návrhů nových legislativních norem zavádění inovací pro zvyšování efektivity, čímž dochází současně ke snižování vynaloženého času a současně ke snižování celkových finančních nákladů. Je tato problematika řešena nebo nikoliv, či případně plánuje se zavádění inovací při náplni této pracovní činnosti, pokud ano, v jakém časovém období a jaké inovace plánujete

implementovat v jakém časovém období na základě jaké metody bude provedeno zhodnocení implementovaných inovací?

Systematicky není efektivita v rámci přípravy legislativních norem řešena. Inovace jsou zaváděny průběžně, naposled se to týkalo např. využívání umělé inteligence.

Dále, zdali jsou v rámci zavádění inovací ve Vaší kanceláři využívány frameworky z oblasti Informačního a Znalostního managementu např. IT Governance (IG), Enterprise Information Management (EIM) či jiné?

Tyto nástroje nejsou v rámci inovací v naší kanceláři využívány.

Rádi jsme se do výzkumu zapojili a věříme, že Vám naše odpovědi pomohou při Vašem výzkumu.

S pozdravem

JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.
vedoucí advokát

E | vlachova@akccs.cz
M | +420 603 174 997

CÍSAŘ, ČEŠKA, SMUTNÝ s.r.o., advokátní kancelář
CITY TOWER, Hvězdova 1716/2b, 140 00 Praha 4
W | www.akccs.cz **T |** +420 224 827 884

From: Ing. Bc. Hana Důbravová <dubravova@polac.cz>
Sent: Thursday, February 22, 2024 11:42 AM
To: vlachova@akccs.cz
Subject: Validace výstupů disertační práce - inovace v oblasti přípravy legislativního procesu
Importance: High

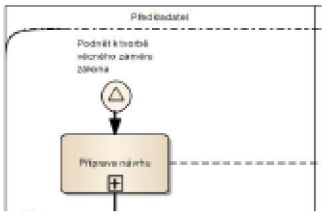
Vážená paní doktorko,

Na základě naší telefonické komunikace Vám zasílám bližší informace k řešené problematice týkající se validace výstupů z mé disertační práce.

V souvislosti s řešením výzkumného úkolu při zpracovávání disertační práce Váš prosím o poskytnutí relevantních informací k řešené problematice uvedené níže. Z hlediska komplexního řešení dané problematiky, je tato problematika současně řešena i na národní úrovni. Obdobná žádost tedy bude zaslána či přímo konzultována i s dalšími organizacemi podílejícími se na přípravě návrhu nových legislativních norem i na národní úrovni.

V souvislosti s prvotní přípravou nových legislativních norem Vás žádám o poskytnutí informací v podobě popisu postupu (procesu) jakým způsobem tato prvotní příprava probíhá a jaké činnosti (aktivity) jsou ze strany zaměstnanců Vaší kanceláře realizovány a s využitím jakého software?

Z hlediska grafického schématu celého procesu přípravy a schvalování nových legislativních norem je myšlena konkrétně část grafického schématu, jehož část přikládám níže, a současně je toto schéma dostupné na obr. č. 81 nebo obr. č. 81 Příprava návrhu str. 296 *„Detailní návrh technického řešení informačních systémů e-Sbírka a e-Legislativa“*, MVČR 2018 dostupné na URL https://smlouvy.gov.cz/smlouva/soubor/9402067/Ver_P2_1ANON.pdf



Při přípravě návrhu nových legislativních norem jsou využívány i prostředky informačních technologií zejména software (dále SW). Jaký typ SW je využíván ze strany Vašich zaměstnanců např. textový editor, software pro sdílení dat, můžete sdělit přesný název využívaného software?

V souvislosti s výše uvedeným dotazem Vás dále žádám o sdělení informací z hlediska finančních nákladů při přípravě návrhů nových legislativních norem: Jaká obvyklá průměrná časová dotace je vynaložena (v počtu hodin na osobu) a v jakém počtu zaměstnanců tato prvotní příprava návrhu nové legislativní normy s využitím software probíhá?

Dále pak prosím o vyčíslení celkového času a počtu zaměstnanců, který je obvykle průměrně vynaložen v rámci odborných konzultací při jednání ve formě on-line nebo s osobní účastí nad připravovanou novou legislativní normou, tj. před započetím samotné přípravy návrhu nové legislativní normy ze strany Vašich zaměstnanců s využitím software.

Dále žádám o sdělení informací, jakým způsobem probíhá na ve Vaší kanceláři při přípravě návrhů nových legislativních norem zavádění inovací pro zvyšování efektivity, čímž dochází současně ke snižování vynaloženého času a současně ke snižování celkových finančních nákladů. Je tato problematika řešena nebo nikoliv, či případně plánuje se zavádění inovací při náplni této pracovní činnosti, pokud ano, v jakém časovém období a jaké inovace plánujete implementovat v jakém časovém období na základě jaké metody bude provedeno zhodnocení implementovaných inovací?

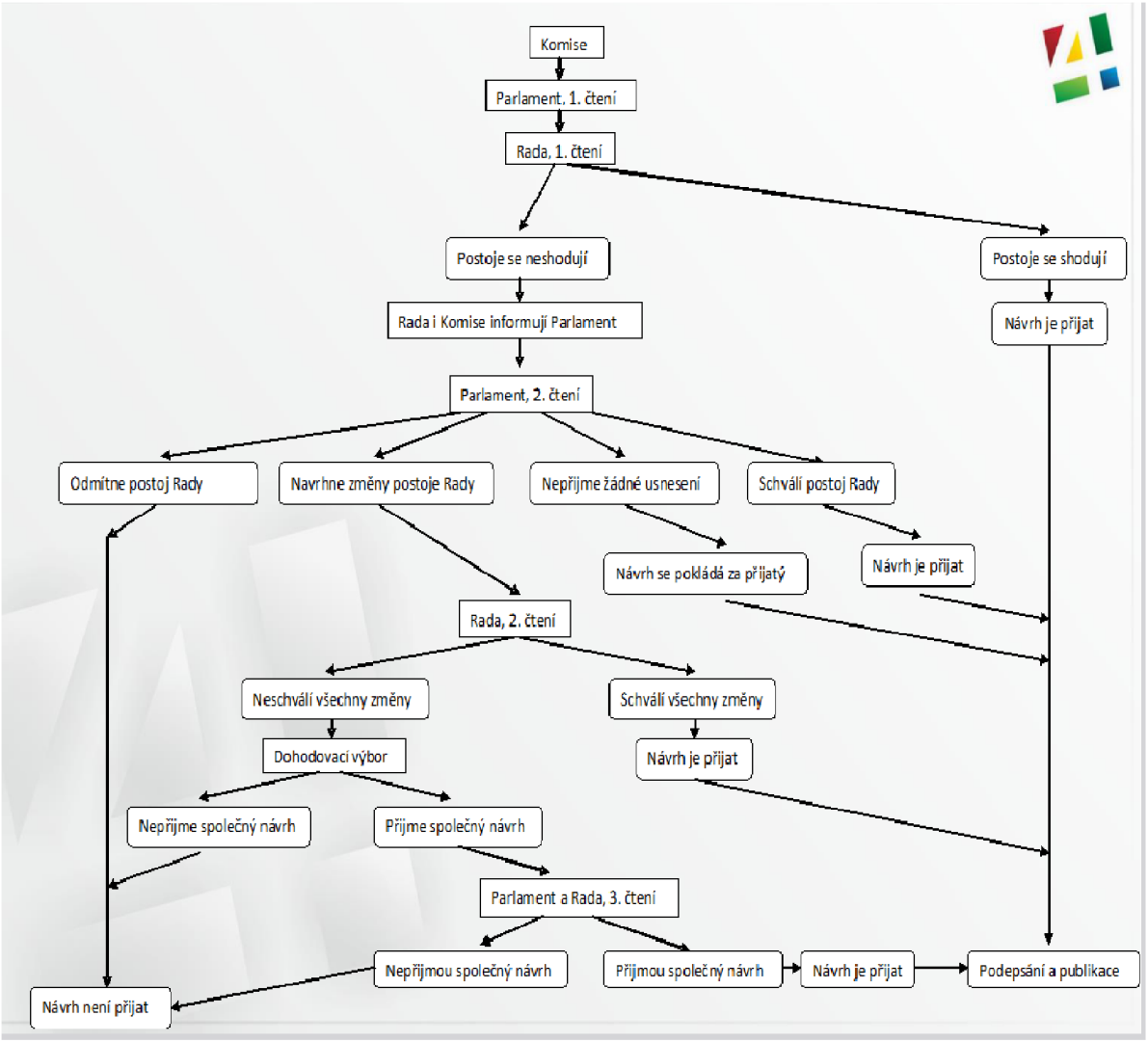
Dále, zdali jsou v rámci zavádění inovací ve Vaší kanceláři využívány frameworky z oblasti Informačního a Znalostního managementu např. IT Governance (IG), Enterprise Information Management (EIM) či jiné?

Děkuji za Vaši pomoc, odpověď a spolupráci při řešení výzkumného úkolu.

Ing. Bc. Hana Důbravová

Policejní akademie České republiky v Praze
Fakulta bezpečnostního managementu
Katedra managementu a informatiky
Email: dubravova@polac.cz

PŘÍLOHA 4 – Podrobné schéma legislativního procesu EU



PŘÍLOHA 5 – Soubor pro zpracování vzorku návrhu nových bezpečnostních standardů v software MAXQDA

Příloha je přiložena v elektronické formě na CD.