Univerzita Pardubice

Fakulta ekonomicko-správní

Kyberbezpečnost a ochrana dat ve strategiích a projektech Smart Cities

Diplomová práce

2024 Bc. Tomáš Kysela

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2023/2024

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Tomáš Kysela**
Osobní číslo:	**E22455**
Studijní program:	**N0688A140007 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Kyberbezpečnost a ochrana dat ve strategiích a projektech Smart Cities**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je analyzovat problematiku kyberbezpečnosti a ochrany dat ve strategiích a projektech Smart Cities ve vybraných světových městech a na základě těchto zjištění navrhnout doporučení pro tuto problematiku.
Osnova:
- Základní pojmy a definice.
- Identifikace a porovnání přístupů a kritérií v dané oblasti.
- Analýza a vyhodnocení získaných dat.
- Návrh doporučení pro danou problematiku.

Rozsah pracovní zprávy: **cca 50 stran**
Rozsah grafických prací:
Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

KHATOUN, Rida; ZEADALLY, Sherali. Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, 2017, 55.3: 51-59.
KOLOUCH, Jan; BAŠTA, Pavel. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80--88168-31-7.
MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2.
SLAVÍK, Jakub. *Smart city v praxi: jak pomocí moderních technologií vytvářet město příjemné k životu a přátelské k podnikání*. Praha: Profi Press, 2017. ISBN 978-80-86726-80-9.
VERHULSDONCK, Gustav, et al. Smart cities, playable cities, and cybersecurity: A systematic review. *International Journal of Human–Computer Interaction*, 2023, 39.2: 378-390.

Vedoucí diplomové práce: **Ing. et Ing. Martin Lněnička, PhD.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **1. září 2023**
Termín odevzdání diplomové práce: **30. dubna 2024**

L.S.

prof. Ing. Jan Stejskal, Ph.D.
děkan

prof. Ing. Jitka Komárková, Ph.D.
garant studijního programu

V Pardubicích dne 1. září 2023

Prohlášení:

Prohlašuji:

Práci s názvem *Kyberbezpečnost a ochrana dat ve strategiích a projektech Smart Cities* jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 4. 2024

Bc. Tomáš Kysela v. r.

Poděkování

Tímto bych chtěl poděkovat Ing. et Ing. Martinu Lněničkovi, Ph.D. za vedení mé závěrečné práce, rady a odborný dohled nad mou prací. Také bych chtěl poděkovat vybraným expertům za spolupráci na metodě Delphi a výběru doporučení. Dále bych rád poděkoval své rodině za podporu při studiu.

ANOTACE

Diplomová práce se zabývá kyberbezpečností a ochranou dat ve strategiích a projektech Smart Cities ve vybraných světových městech. Práce obsahuje postup pro řešení této problematiky, který se skládá z analýzy a vyhodnocení získaných dat. Výstupem práce je seznam ověřených doporučení.

KLÍČOVÁ SLOVA

kyberbezpečnost, ochrana dat, Smart City, strategie, projekt, metoda Delphi

TITLE

Cybersecurity and data protection in Smart Cities strategies and projects

ANNOTATION

The diploma thesis deals with cybersecurity and data protection in Smart Cities strategies and projects in selected world cities. The thesis contains a procedure for solving this issue, which consists of the analysis and evaluation of the obtained data. The output of the thesis is a list of validated recommendations.

KEYWORDS

cybersecurity, data protection, Smart City, strategy, project, Delphi method

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM ZKRATEK

AI	Artificial intelligence
BMS	Building Management System
CCCS	Canadian Centre for Cyber Security
CIMI	Cities in Motion index
CISA	Cybersecurity and Infrastructure Security Agency
ČR	Česká republika
DDoS	Distributed Denial of Service
DLP	Data loss prevention
DoS	Denial of Service
EISP	Enterprise Level Security Policy
EU	Evropská unie
FBI	Federal Bureau of Investigation
GCI	Global Cities Index
GCO	Global Cities Outlook
GPCI	Global Power City Index
HKG	Hong Kong
HW	Hardware
ICT	Informační a komunikační technologie
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
ISO	International Organization for Standardization
ISSP	Issue-Specific Security Policy
ITIF	Information Technology and Innovation Foundation
ITS	Intelligent Transporting System
IZS	Integrovaný záchranný systém
LA	Los Angeles
MPC	Multi-party-computation
NCSC-UK	United Kingdom National Cyber Security Centre
NIST	Národní institut standardů a technologie

NSA	National Security Agency
NYC	New York City
OSN	Organizace spojených národů
SCG	Smart City Governments
SCI	IMD Smart City index
SCIS	Smart City Information System
SDL	Service Dominant Logic
SDN	Software-Defined Network
SF	San Francisco
SIEM	Security Information and Event Management
SW	software
SysSP	Systems-Specific Security Policy
UAV	Unmanned Aerial Vehicle
VPN	Virtual Private Network

ÚVOD

Digitalizace a využívání moderních informačních a komunikačních technologií (ICT) ovlivňuje nejenom soukromý sektor, ale i veřejný sektor a to, jak pracuje s daty a musí přistupovat k jejich zabezpečení a ochraně. Výrazný nárůst přesunu obyvatel do měst v posledních desetiletích má za následek i mnohem větší procentuální navýšení obyvatel ve městech oproti venkovu. Toto však vytváří tlak na efektivnější řízení měst a zároveň využívání moderních technologií pro samotné fungování měst, jejich zabezpečení a zamezení problémům a potenciálním rizikům, která jsou spjaté s tímto nárůstem.

Přesun obyvatel do měst má za následek mimo jiné zvýšení nákladů, které město vydává na energie, dopravu, vodu, odpad, potřebu vzdělání, využití zdravotnictví nebo veřejných prostorů. Z tohoto důvodu začala města stále více spoléhat a využívat nové technologie a došlo ke vzniku samotných projektů Smart City neboli chytrých měst. Implementace Smart City konceptů tedy napomáhá zajistit účinný a udržitelný rozvoj města, kvalitní životní styl, zajistit bezpečnost města nebo optimální využití energií. K tomuto projekty Smart City využívají ekonomických, sociálních a technologických inovací (Law a Lynch, 2019; Slavík, 2017; Vodák et al., 2021).

Je také potřebné říci, že hodnota velkých souborů dat a potenciální zranitelnosti v digitálních systémech, které lze nalézt ve Smart City, znamená, že existuje možnost zneužití k finančnímu anebo politickému zisku a také případně ke špionáži různými aktéry. Mezi tyto aktéry lze řadit jak národní státy, tak vnitřní hrozby, ale také různé kyberzločince a teroristy. Zde stále platí, že neexistuje žádná technologie nebo opatření, která by byla zcela bezpečná a zamezila ztrátě, poškození, nebo odcizení dat.

Pro zajištění zabezpečení Smart Cities dochází k vytvoření a využití přístupů založených na různých zásadách a opatřeních. Využitím kybernetických přístupů zabezpečení již při návrhu, budování a následně provozu projektů využívajících různé druhy zabezpečení může město dosáhnout jak zmírnění rizik, tak jejich následků a případně úplně předejít jejich vzniku.

Cílem této diplomové práce je analyzovat problematiku kyberbezpečnosti a ochrany dat ve strategiích a projektech Smart Cities a na základě těchto zjištění zanalyzovat a navrhnout doporučení pro tuto problematiku. Práce je rozdělena do čtyř kapitol, které vedou od seznámení se s pojmy k danému tématu, přes identifikování přístupů a kritérií v rámci strategií a projektů Smart City až k analýze a vyhodnocení získaných dat a návrhu doporučení pro kyberbezpečnost a ochranu dat ve Smart City projektech.

První kapitola se zabývá základními pojmy a definicemi, které je potřebné znát pro tuto problematiku. Dochází zde k vysvětlení pojmů kyberprostor, kyberbezpečnost a Smart City. Kyberbezpečnost a Smart City jsou termíny, které jsou probrány více detailněji. Nejdříve je vymezena bezpečnost a kyberbezpečnost, následně jsou rozebrány principy kyberbezpečnosti a současné hrozby. Pro koncept Smart City jsou sepsány definice tohoto pojmu, základní komponenty, které se ve Smart City vyskytují a technologie, které se využívají.

Druhá kapitola práce je věnována identifikaci a porovnání principů a kritérií pro strategie a projekty Smart City. Zde jsou rozepsána existující řešení a možná rizika, která lze v rámci kyberbezpečnosti v souvisejících dokumentech nalézt. Dále je v kapitole věnována pozornost konkrétním strategiím, doporučením a politikám na mezinárodní, nadnárodní a národní úrovni. Část kapitoly je věnována vymezení a popisu rámců a indexů, které hodnotí rozvoj Smart Cities. Také jsou v kapitole rozebrány výzkumné práce a články na téma projektů Smart City.

Třetí kapitola analyzuje a hodnotí získaná data v rámci Smart City strategií a šesti komponent, kterými jsou economy, people, governance, mobility, environment a living. Nejdříve je zde představena metodika, pomocí které byla data získána, analyzována, vyhodnocena, a zároveň také ověřena za účelem získání doporučení pro danou problematiku. Následují dílčí kapitoly, kde jsou jednotlivé kroky metodiky blíže popsány, včetně výběru vzorku měst, vyhledávacích strategií a postupu analýzy dokumentů a jejich vyhodnocení.

Čtvrtá kapitola obsahuje seznam doporučení pro Smart City projekty. Pro vytvoření a ověření tohoto seznamu je využita metoda Delphi, která je zde blíže popsána a vymezen její postup. Po provedení metody Delphi jsou představeny a diskutovány konečné návrhy doporučení pro kyberbezpečnost a ochranu dat v oblasti Smart City projektů a strategií.

1 ZÁKLADNÍ POJMY A DEFINICE

Tato kapitola je zaměřena na definice základních pojmů řešené problematiky. Mezi tyto pojmy lze zařadit kyberprostor, bezpečnost, resp. kyberbezpečnost a dále pojem Smart City. Je důležité si vymezit tyto pojmy, jelikož je práce zaměřena právě na ně a bude s nimi dále pracováno.

1.1 KYBERPROSTOR

Kyberprostor odkazuje na virtuální svět nebo prostor, specificky na elektronické médium, ve kterém dochází ke komunikaci. Typicky odkazuje na větší počítačovou síť tvořenou ze celosvětových počítačových sub-sítí, které spolu komunikují a zajišťují výměnu dat. Skrze kyberprostor je možné sdílet informace, interagovat s ostatními uživateli, hrát hry, zapojovat se do diskusí nebo fór, podnikat nebo tvořit média a mnohem více. Z těchto důvodů je také nutné zajistit bezpečnost v kyberprostoru (Rouse, 2023). Jedná se o globální doménu v informačním prostředí sestávající ze vzájemně závislé sítě infrastruktur informačních technologií, včetně internetu, telekomunikační sítě, počítačových systémů spolu s procesory a řadiči. Tato definice je pro změnu více zaměřena na technologie a hardware (HW) (Cohen, 2007).

Jakožto komunikační médium, kyberprostor nabízí možnost přístupu různým formátům, které splňují požadavky uživatelů. Čas a prostor zanikají, jelikož je možné získávat informace z celého světa a kdykoliv. Pro uživatele toto není viditelné, ale každý aspekt kyberprostoru je někým vlastněn a udržován, a proto je nutné, aby byl výdělečný a dále udržitelný. Toto vlastnictví umožňuje zamezení vstupu uživatelů, datových formátů nebo informací z různých zdrojů do kyberprostoru. Příkladem je Čína, která zamezuje přístup k mezinárodním velmi populárním stránkám (Venables, 2021). Pro popis charakteristik kyberprostoru je využit čtyřvrstvý model. První vrstvou jsou lidé, kteří se účastní kybernetického světa, tedy komunikují, pracují s informacemi, rozhodují a uskutečňují plány a celkově pracují se složkami v rámci kyberprostoru. Druhou vrstvou jsou uložené, zasílané a transformované informace v rámci kyberprostoru. Třetí vrstva je složena z logických bloků, které se využívají pro služby a podporu platforem kyberprostoru. Poslední vrstvou jsou fyzické základy, které podporují logické prvky (Clark, 2010).

1.2 KYBERBEZPEČNOST

Vzhledem k tomu, že se mnohem více vše automatizovalo, ať už se jednalo o obchodní aktivity, ukládání dat, využití mnohem více počítačů, přístupy skrze nezabezpečení sítě nebo třeba

internet, bylo potřeba, aby došlo ke změnám v přístupu k zabezpečení. Toto vše dalo příčinu většímu využití kyberbezpečnosti a potřeby jí více řešit i ve veřejném sektoru (Kemmerer, 2003; Kolouch a Bašta, 2019). Kyberbezpečnost je sousloví, které je složeno ze slov kyber a bezpečnost. Slovo kyber souvisí s ICT. Kyberbezpečnost se tedy týká kohokoliv, kdo využívá jakýmkoliv způsobem ICT. Lidé jsou často tím stěžejním prvkem, který bezpečnost zaručuje anebo naopak narušuje. Bezpečnost a kyberbezpečnost není pouze spojována se státem, ale je důležitá i pro organizace nebo osoby (Kolouch a Bašta, 2019). Kyberbezpečnost je soubor technologií a procesů, které jsou navrženy tak, aby ochraňovaly počítače, sítě, programy a data od útoků, poškození anebo neautorizovaných přístupů. V dnešní době dochází k významnému posunu v rámci využívaných technologií a operací vzhledem k využití umělé inteligence, strojového učení a obecně datové vědy a datové analytiky (Sarker et al., 2020).

Kyberbezpečnost nebo ochrana dat v rámci Smart City nejčastěji souvisí s ochranou osobních údajů a zajištění soukromí pro uživatele, resp. občany. Všeobecně lze za soukromí považovat prostředí v němž se uživatel může pohybovat a do kterého nebude nikdo cizí zasahovat (Melotíková, 2018, s. 13). Tuto problematiku zároveň řeší odpovídající legislativa, např. různé zákony a nařízení týkající se ochrany osobních údajů a kyberbezpečnosti. Vždy zde musí být jasně vymezeno, co je daným pojmem myšleno, a jaká opatření je nutné implementovat a dále měřit a vyhodnocovat, aby bylo dosaženo požadovaných cílů pro daná opatření (Kolouch a Bašta, 2019; Melotíková, 2018).

1.2.1 Vymezení bezpečnosti a kyberbezpečnosti

Definovat kyberbezpečnost je složitější, stejně jako toto platí pro slovo bezpečnost. Obě slova mají více definicí, které se méně i více odlišují, zpravidla podle vybraného odvětví, ve kterém je daná definice využita.

Příkladem různých definic bezpečnosti je:

1. *„Ochrana osob, budov, organizací nebo zemí proti hrozbám jako je zločin nebo útoky jiných zemí.“* (Cambridge Dictionary, 2023). Definice slova bezpečnost v rámci ochrany.
2. *„Bezpečnost je stav, kdy jsou na efektivní míru omezeny hrozby pro objekt a jeho zájmy a tento objekt je k omezení stávajících i potenciálních hrozeb efektivně vybaven a ochoten při něm spolupracovat“* (Souček et al., 2005). Jedná se o definici, kterou uvádí Ministerstvo vnitra České republiky (ČR) ve svém dokumentu.

3. *„Bezpečnost v rámci informačních technologií odkazuje na metody, nástroje a personální využití pro ochranu digitálních aktiv organizací.“* (Bacon, 2021).

Definicí kyberbezpečnosti je také více. Několik příkladů je:

1. *„Opatření provedená za účelem ochrany počítače nebo počítačového systému (na internetu) proti neautorizovaným přístupům nebo útokům.“* (MerriamWebster, 2023). Definice z portálu MerriamWebster.
2. *„Kyberbezpečnost je způsob ochrany serverů, počítačů, mobilů, systémů, sítí a dat na internetu, před škodlivými útoky. Též známé jako ochrana informačních technologií.“* (Kaspersky, 2023). Tato definice je z webových stránek poskytovatele antiviru Kaspersky.
3. *„Kyberbezpečnost se týká jakékoli technologie, opatření nebo praxe pro prevenci kyberútoků nebo zmírnění dopadu. Cílem kyberbezpečnosti je ochrana individuálních a organizačních systémů, aplikací, výpočetních zařízení, citlivých dat a finančních aktiv před počítačovými viry nebo ransomware útoky.“* (IBM, 2023). Definice od IBM, poskytovatel a výrobce HW, software (SW) a s nimi spojených služeb.

1.2.2 Principy kyberbezpečnosti

Kybernetická bezpečnost využívá tři druhy principů, které jsou nazývány také triádami kyberbezpečnosti. Mezi ně patří koncept Confidentiality, Integrity a Availability (CIA), prvky kybernetické bezpečnosti a životní cyklus (Kolouch a Bašta, 2019).

CIA se originálně odkazuje na základní prvky bezpečnosti v informačních systémech. Tyto hlavní tři prvky nejen utvářely a formovaly teoretické chápání bezpečnosti informací, ale i využití v samotné praxi, kdy pomocí těchto tří prvků jsou vyvíjena a implementována bezpečnostní řešení (Samonas a Coss, 2014). CIA se tedy skládá z důvěrnosti (C), celistvosti (I) a dostupnosti (A). Aplikace pouze této triády ale není v dnešní době možná, je tedy nutné implementovat další kyberbezpečností principy. Většinou je tento princip vztahován k ochraně informací samotných. Ochrana by ale neměla být pouze vztažena na informace, je nutné zabezpečit i samotná data a počítačové systémy, které slouží pro přenos informací (Kolouch a Bašta, 2019).

Pojem důvěrnost je chápán jako přístup k datům a informacím, který je dostupný pouze autorizovaným osobám a procesům. Integrita značí, že by informace neměly být modifikovány nebo odstraněny, a to jak náhodně, tak i úmyslně. Dostupností je zde myšleno, že autorizovaní uživatelé by měli mít možnost přístupu k informacím, kdykoliv je potřebují. CIA by měl být

uplatňován v organizacích a měl by být implantován v bezpečnostních zásadách a rámcích (Fruhlinger, 2020). Jelikož CIA může být nedostačující, používá se také Parkeriánský hexad, který rozšiřuje CIA o další prvky. Rozšíření bylo nutné, jelikož CIA se nesoustředila na velmi důležitý prvek, kterým jsou samotní lidé. Bezpečnost je i o lidech, ne pouze o technologiích. Těmito prvky jsou kontrola (control), autenticita (authenticity) a využití (utility) (Pender-Bey, 2019).

Mezi prvky kybernetické bezpečnosti lze zařadit lidi, technologie a procesy, které společnou interakcí umožňují do nějaké míry tvořit kybernetickou bezpečnost (Kolouch a Bašta, 2019). Lidé se liší ve schopnosti správně vyhodnocovat riziko kybernetické bezpečnosti. Zde je uvedeno že, pouze 23 % lidí správně vyhodnotí pod 50 % hrozeb. Je také prokázáno, že lidé na internetu jsou mnohem náchylnější k dělání chyb a tím pádem jsou i zranitelnější. Stejné platí například i pro lidi, kteří využívají pracovní nebo jiné, ne svoje vlastní, počítače (Linkov et al., 2019). Technologie jsou prostředky, které umožňují připojení k internetu, sociálním sítím nebo jiným aplikacím. Dále se jedná o nástroje pro tvorbu dokumentů, sledování videa nebo hudby a další. Pro organizace jsou technologiemi zařízení pro koncové uživatele, infrastruktura celé sítě, služby až po prvky zajišťující zabezpečení, a to jak fyzické, tak v síti. Procesy jsou činnosti, které je nutné provádět, aby bylo možné pracovat s technologiemi a s nimi spojenými službami. Existují procesy jako jsou řízení aktiv a rizik, implementace ICT, správa uživatelů a rolí, autorizace a autentizace, údržby systému, testování zabezpečení, analýzy a realizace opatření, audity, školené, detekce anomálií apod. (Kolouch a Bašta, 2019).

Posledním zmíněným principem kyberbezpečnosti je jeho životní cyklus, který se skládá z přípravy, detekce a analýzy, zadržení, zničení a nápravy, aktivity po události. V přípravné fázi dochází k vytvoření plánu řízení incidentů. Tedy co se děje, jakou reakci incidenty vyvolají, po zjištění různých typů narušení, malware útoků, hackerských útoků apod. Fáze detekce a analýzy zahrnuje sběr informací a analyzování dat, aby došlo k predikci a identifikaci zdroje případného útoku. Dále zde dochází k analýze případných dopadů na systém. V kroku zadržení dochází k použití všech dostupných metod k zamezení útokům. Poté v kroku zničení a nápravy dochází k zajištění útoku a dochází ke zničení hrozby a její odstranění z prostředí. Následně dochází k nápravě neboli vrácení systému do původního stavu před útokem a napadením. Posledním krokem jsou po událostní aktivity. V tomto kroku dochází k rozboru bezpečnostního incidentu. Dochází k porozumění toho, jak došlo k incidentu, jak zamezit opakovanému objevení v budoucnosti. Naučené znalosti lze aplikovat zpětně do plánu řízení rizik (EC-COUNCIL, 2022).

1.2.3 Současné hrozby pro kyberbezpečnost

V roce 2022 vydal Evropský parlament článek, který se týkal současných hrozeb pro kyberbezpečnost. Článek odkazuje na agenturu Evropské unie (EU) pro kybernetickou bezpečnost, podle které v dnešní době existuje osm hlavních skupin hrozen v oblasti kyberbezpečnosti (Evropský Parlament, 2022). První skupinou je ransomware. Jedná se o kategorii škodlivého SW, který narušuje funkcionalitu počítače. Zobrazuje zprávy, které chtějí zaplatit nějakou částku k obnovení funkcionality. Neboli malware požaduje výkupné – ransom – od tohoto je odvození ransomware. Během let dochází i k vývoje těchto ransomwarů, kdy je mnoho technik, jak narušovat funkcionalitu počítače (O'Gorman a McDonald, 2012). Šifrování se využívá k zajištění soukromí dat během přenosu a ukládání. Zločinci si ale osvojili šifrování, které využívají pro vydírání. Toto spočívá v tom, že zašifrují data oběti a nezpřístupní je, dokud nedojde k zaplacení výkupného (O'Kane et al., 2018).

Druhou hrozbou je malware, což je škodlivý SW, který je na počítači nechtěný. Jedná o jakýkoliv kód, který je přidán, změněn nebo odstraněn ze softwarového systému, tak aby vědomě poškodil funkčnost systému (McGraw a Morrisett, 2000). Malware je charakterizován schopností replikace, šíření, poškození počítače a samočinného provozu (Saeed et al., 2013). Třetí hrozbou je sociální inženýrství, což je praktika, kdy dochází k manipulaci lidského subjektu, aby prozradil citlivé informace, přístupy anebo různé údaje. Obvykle k tomuto dochází skrze faktor lidské chyby, důvěrnosti nebo přesvědčení. Mezi sociální inženýrství například spadá phishing, email spamming, scareware atd. (Farrier, 2023).

Následují hrozby vůči datům s cílením na zdroje dat. Účelem je získat přístup a následně data zveřejnit. V dnešní době je toto velice důležité, protože vzniká velké množství dat. Hrozby v dostupnosti – odepření služby – je další hrozbou, kdy dochází k bránění v přístupu k datům a službám. Většinou se jedná o přetížení infrastruktury. Hrozby v dostupnosti internetu jsou další skupina hrozeb, která je definována jako fyzické převzetí a zničení internetové infrastruktury, která se stává nepoužitelnou a nedostupnou. Předposlední hrozbou jsou útoky na dodavatelský řetězec. Jedná se o zaměření na vztahy mezi organizacemi a dodavateli, kdy hrozí např. nedodání nějaké služby, fiktivní faktury a další hrozby vyplývající z rostoucí náročnosti správy různých podnikových systémů (Evropský Parlament, 2022).

Poslední hrozbou jsou dezinformace. Dezinformace je falešná informace, šířená úmyslně, tak aby sváděla a klamala. Cílem je ovlivnění rozhodování nebo názory lidí, kteří tyto informace přijímají (Shu et al., 2020).

1.3 SMART CITY

Po tisíce let se lidé přesouvali do měst. Do roku 2050 se odhaduje, že dvě ze tří osob budou žít ve městech nebo městských centrech. Tedy přibližně více jak 2,5 bilionu dalších lidí bude žít ve městech. Zpráva Organizace spojených národů (OSN) také predikuje, že do roku 2030 bude existovat již 43 megaměst, o 12 více jak je tomu dnes. Megaměstem je nazýváno město s více jak 10 milion obyvatel (United Nations, 2023). Také došlo k extrémnímu nárůstu a rozšíření používání internetu od začátku tohoto století. S tím i souvisí vývoj technologií. Kdy dochází k vývoji a přesunu na bezdrátové technologie. Toto vše bylo potřebné pro digitalizace měst a vznik projektů Smart City (Slavík, 2017; Townsend, 2013).

Pojem Smart City se stále vyvíjí a definice není konkrétní. Jelikož „chytrost“ města se může lišit od jednoduché až po komplikované funkce pro celé administrativní procesy. Tyto definice lze rozlišit, podle toho, zda jsou více zaměřené na technologie, aplikace, systémy, data, prostředí, ekonomiku, sociální stránku nebo další (Yin et al., 2015).

Příkladem je definice ze zprávy od autorů Gladstone et al. (2018) na téma Smart City pro střední města v Ontariu. Tato definice stanovuje Smart City jako města, která využívají digitalizace a smart technologie – mobility, energie, infrastruktury atd. Součástí Smart City by měly být technologie zamřené na networking a komunikaci, kyberfyzické systémy, Internet of Things (IoT), cloud computing, open data, big data a datová analytika. Smart City by také mělo být propojené skrze sítě ať už na regionální, národní nebo světové bázi, aby docházelo ke spojení se světem, lepší komunikací apod. Komunikace je také důležitá pro veřejnost, resp. občany daného města, pro které je primárně většina projektů určena. Využitím Smart City by také mělo dojít k udržení jedinců v městech, které tyto technologie poskytují, jelikož dochází ke zvýšení kvality života (Gladstone et al., 2018).

Dalším příkladem definice Smart City v dokument od autorů Falconer a Mitchell (2012), který říká, že je zde několik výzev, kterým je potřeba čelit v rámci měst. Zvětšující se populace měst, která vede k zatížení městské infrastruktury, pro které je poté nutné dělat přestavby a nové návrhy řešení. Polarizovaný ekonomický růst, kdy několik stovek měst tvoří více jak polovinu světové hrubého domácího produktu. Zvětšující se emise skleníkových plynů a snižující se rozpočty vzhledem k nutnosti reagovat na ekonomické klima. Tyto všechny problémy lze zmírnit, a to právě skrze použití škálovatelných řešení, které využívají ICT technologie pro zvýšení efektivity, snížení nákladů a zlepšení kvality života (Falconer a Mitchell, 2012).

Posledním příkladem je definice z knihy Smart City v praxi. Tato definice říká, že Smart City je koncept strategického řízení města, při němž jsou využívány moderní technologie. Tyto technologie ovlivňují kvalitu života ve městě. Dále také k dosahování hospodářských a sociálních cílů měst (Slavík, 2017, s. 12).

Obecně lze tvrdit, že města, která přijala některou z definic pojmu Smart City a na jejím základě vytváří související strategie a projekty, primárně propojují své občany pomocí různých sítí a komunikačních kanálů, které v různých oblastech fungování města navážejí těmto občanů služby. Ty např. optimalizují řízení dopravy, udržitelné využívání energie nebo zavádění chytré správy města. V rámci Smart City nám vznikl i pojem playable city. Tento pojem je spjatý s vytvořením Smart City, které jsou více zaměřené na člověka. Vzhledem k tomu, že Smart City jsou sociotechnické struktury, které zahrnují technologie, politiku a lidi mající vliv na bezpečnost a soukromí, má takovýto přístup také schopnost a potenciál vytvoření silných protokolů kyberbezpečnosti pro Smart City (Verhulsdonck, 2023).

1.3.1 Základní komponenty Smart City

Základní komponenty nebo charakteristiky Smart City se můžou lišit podle definice Smart City. Pro některé jsou hlavní digitální prvky a technologie, pro jiné zase lidský faktor. Další faktory formující pohled na komponenty mohou být ekonomické, enviromentální, kulturně-historické, zaměřené na otevřenost a transparentnost atd. (Sashinskaya, 2015). U pojmu Smart City je tedy klíčový důraz kladen na konkrétní komponenty a jejich charakteristiky. Jedna z prvních definic byla založena na vymezení šesti komponent, které jsou relevantní vzhledem k oblastem „chytrosti“, ze kterých je Smart City složeno. Mezi tyto charakteristiky patří: smart economy, smart people, smart governance, smart mobility, smart environment a smart living (Giffinger a Gudrun, 2010).

Dalším příkladem komponent Smart City jsou čtyři úrovně a tři pilíře. Mezi tyto čtyři úrovně spadá organizace neboli institucionální struktura a plánování. Druhou úrovní je komunitní život, které značí komunikaci s občany, získávání potřebných informací a zpětné vazby na řízení města. Třetí úrovní je infrastruktura, především doprava, energetika, služby a řízení budov. Poslední úrovní je kvalita života občanů ve městě. Poté zde také jsou tři pilíře, mezi které patří ICT, inteligentní mobilita, a inteligentní energetika a služby (Slavík, 2017, s. 15-16).

Mohanty s kolegy ve své práci rozdělují komponenty Smart City do osmi kategorií. Mezi tyto kategorie patří infrastruktura, budovy, doprava, energie, zdravotnictví, technologie, vzdělávání, občané a vláda (Mohanty et al., 2016). Dále lze nalézt rozdělení komponent na technologické,

institucionální nebo lidské. Technologické faktory zahrnují všechny fyzické a infrastrukturální komponenty jako jsou digitální sítě nebo udržitelná technologická komunikace. Mezi lidské faktory spadá lidský kapitál. Do posledního institucionálního faktoru pak patří transparentnost, zapojení občanů do politiky, rozvoj veřejných míst, tvorba politiky nebo vývoj právní úpravy (Sashinskaya, 2015).

Pohled na vymezení jednotlivých komponent se tedy liší, nicméně lze identifikovat několik hlavních společných komponent, které se vyskytují napříč různými zdroji. Mezi tyto společné komponenty lze zařadit lidský faktor, dopravu a mobilita, energetiku, vládnutí a rozvoj města.

1.3.2 Technologie ve Smart City

Jedním z hlavních problémů, které se koncept Smart City snaží řešit je doprava, udržitelnost prostředí, uchování energie a přírodních zdrojů, zdravotnictví a vzdělávání. Tyto problémy lze řešit pomocí moderních ICT. Příkladem využití technologií pro zlepšení dopravy a bezpečnosti v rámci ní jsou parkovací systémy a dopravní signalizace (např. chytré křižovatky a přechody), které reagují v reálném čase na různé situace a požadavky. Dále se jedná o využití chytrých telefonů, různých aplikací a obecně senzorů, které sbírají data o stavu vozovky, prostoru nebo monitorují dopravu. Všechna tato data lze využít při řízení dopravy nebo v případě nouzových stavů (Law a Lynch, 2019).

IoT aplikace umožňují vzdáleně monitorovat, spravovat a ovládat zařízení. Také generují nová data a užitečné informace, včetně možnosti analýzy toků dat v reálném čase. Mezi rysy Smart City patří vysoký stupeň integrace ICT a komplexních aplikací a informačních zdrojů. IoT je tedy o aplikování různých typů senzorů a následném napojení na internet skrze protokoly pro komunikaci a výměnu dat (Kim et al., 2017).

Big data poskytují pro města možnost získat informace z velkého množství dat z různých zdrojů. Problémem může být to, že většinově jsou tato data nestrukturovaná. Propojením např. s cloud computingem a platformami pro zpracování a ukládání velkých objemů dat lze však zpracovávat i tato data. Pro získávání dat jsou zpravidla opět využívány různé senzory a IoT (Hashem et al., 2016). Důležité je také při tvorbě Smart City konceptu vytvoření důvěry. Pro toto se využívají inteligentní systémy. Tyto systémy jsou na bázi technologií IoT, big data a ICT. Fungování systémů, s pozitivním vlivem na důvěru, je založeno na device-to-device zařízeních, hodnoceních uživatelů, predikcí a vyhodnocování výsledků. Tyto systémy propojují město s principy Service-Dominant Logic (SDL), které v sobě zahrnuje sběr dat skrze senzory, informační integritu a znalostní databázi. Dalším typem systémů jsou pak Software-Defined

Network (SDN), které se využívají v rámci Smart City k předávání informací a komunikaci se zúčastněnými stranami, především občany a zastupiteli, případně úředníky. Centralizovaný systém tvoří bezpečné prostředí pro uživatele v reálném čase. Jako poslední typ systémů sem lze zařadit Wireless Sensor Network, který tvoří virtuální vrstvu pro přenosy dat (Vodák et al., 2021).

Využití Unmanned Aerial Vehicle (UAV) pro jiné než komerční nasazení se v poslední době zvyšuje a nejedná se o pouze armádu, která ho využívá. UAV se v rámci měst využívá tam, kde je to nebezpečné pro člověka, příliš náročné anebo se finančně nevyplatí nasazovat lidskou sílu (Ismail et al., 2018). UAV v rámci Smart City mohou být použity pro monitorování prostředí, sledování dopravy, monitoring znečištění, bezpečnostní kontroly nebo civilní kontroly občanů. Problémem zde nicméně je, že jejich implementace a využívání nejdříve vyžaduje vyřešení problémů týkajících se bezpečnosti, soukromí a ochrany osobních dat při sběru a zpracování získaných dat, ale především etického využívání těchto zařízení (Mohamed et al., 2020).

Dalším typem technologií, které jsou ve Smart City využívány, jsou bezdrátové technologie. Příkladem je 5G, které je novým typem komunikační sítě pro spojení všeho a všech, tzn. různých zařízení a lidí. Příkladem využití 5G je např. Intelligent Transporting System (ITS), kdy senzory jsou umístěny jak na vozidlech, tak na cestách nebo plochách u cest a chodníků (Gohar a Nencioni, 2021). 5G oproti předchozí 4G umožňuje 10krát až 100krát vyšší rychlost přenosu dat a také počet připojených zařízení. Nicméně pokrytí 5G stále není dostupné všude, a i zde je nutné řešit bezpečnost, soukromí a ochranu osobních dat (Gohar a Nencioni, 2021; Mohanty et al., 2016).

2 IDENTIFIKACE A POROVNÁNÍ PŘÍSTUPŮ A KRITÉRIÍ

Na základě studia literatury lze tvrdit, že města potřebují nové chytré technologie, aby naplnila podstatu konceptu Smart City. Tyto nové technologie sice zlepšují kvalitu života a přináší nové věci, ale zároveň s příchodem těchto technologií přicházejí i nové problémy a výzvy. S ohledem na propojenost projektů Smart City může jeden slabý článek ohrozit celé město a vystavit ho riziku. Proto je potřebné, aby se stejně jako technologie vyvíjela i kyberbezpečnost (Ma, 2021). Pro mnoho oblastí (komponent) v rámci Smart City, viz kapitola 1.3.1, je nutné identifikovat konkrétní specifika a za tímto účelem nastavit odpovídají řešení pro kybernetickou bezpečnost. Mezi nejzranitelnější části Smart City využívající ICT lze zařadit kritickou infrastrukturu, smart budovy, ITS, e-government, a sítě a senzory tvořící IoT (Khatoun a Zeadally, 2017).

Příkladem je kritická infrastruktura, do které lze zařadit jaderné elektrárny, chemické závody, ropné rafinérie, železniční signalizační systémy, větrné turbíny, ve které dochází k využití komunikačních zařízení, protokolů a kanálů. Příkladem mohou být servery, telefonní linky, komunikační protokoly a další. Původně tyto protokoly byly navrženy bez zabezpečení, a proto je nutné řešit jejich bezpečnost (Khatoun a Zeadally, 2017). Dalším příkladem mohou být smart budovy, které jsou definované jako struktury, ve kterých dochází k využití automatizovaných procesů a zařízení k řízení a monitorování provozu. Jelikož jsou tyto systémy elektronické a jsou připojené k systémům a internetu, mohou představovat hrozbu a je nutné je zabezpečit proti případným útokům (Brisson et al., 2019).

Také je nutné říci, že dnešní moderní doba je velice ovlivněna rozvojem technologií a aplikací, které využívají umělou inteligenci, strojové učení, IoT nebo robotická zařízení. Smart City využívají umělou inteligenci pro sběr dat. Tyto metody jsou velice efektivní, ale problém nastává, pokud vznikne chyba, která může být zneužita a přeměněna na hrozbu, a dále průnik prostřednictvím elektronických útoků a kybernetická kriminalita. Je tedy nutné provádět kybernetickou bezpečnost pro kontrolu těchto útoků souvisejících se zneužitím elektronického prostředí pomocí technik umělé inteligence, včetně strojového učení (Mijwil et al., 2022).

Důležitým prvkem pro zabezpečení informací jsou zásady bezpečnosti informací. Jedná se o soubor pravidel pro ochranu informačních aktiv. Tyto zásady musí být brány v potaz pro všechny plány, návrhy a nasazení bezpečnosti informací. Měly by být zavedeny politiky, které poskytují návody, jak řešit problémy a jak využívat technologie. Lze definovat tři vrstvy informační bezpečnosti. Nejvyšší vrstvou je Enterprise Level Security Policy (EISP), střední

vrstvou je Issue-Specific Security Policy (ISSP) a nejnižší vrstvou je Systems-Specific Security Policy (SysSP). Do EISP spadá celková bezpečnost, ICT bezpečnost a informační bezpečnost na vyšší úrovni. ISSP jsou politiky zaměřené na zaměstnance, jak se mají chovat, jak využívat technologie a nastavené procesy. SysSP funguje jako standard nebo proces, který se používá při konfiguraci nebo údržbě systému (Wu et al., 2020).

Příklady řešení různých charakteristik v rámci zabezpečení inteligentní budovy jsou zobrazeny v Tabulce 1. Zde jsou rozepsána možná řešení a doporučení pro čtyři charakteristiky v rámci inteligentního systému Building Management System (BMS) (Khatoun a Zeadally, 2017).

Tabulka 1: Řešení kybernetické bezpečnosti v BMS. Zdroj: Khatoun a Zeadally (2017).

Charakteristika	**Řešení**
Organizační	• Vytvoření plánu zálohy a obnovy. • Správa hesel. • Otevřená zpětná vazba. • Definovat standardy, nástroje, bezpečnostní procedury a pravidla. • Vytvoření politik ohledně hesel a konfigurací.
Technické	• Fyzické zabezpečení. • Šifrování síťového provozu robustním symetrickým algoritmem. • Využití bezpečného připojení jako je Virtual Private Network (VPN) pro vzdálený přístup. • Zabezpečení bezdrátové sítě pomocí Wi-Fi Protected Access 2. • Využití Intrusion Detection System (IDS) v budově. • Centralizovaný server pro ověření, autorizaci a účtování. • Nastavení firewallu. • Silné metody ověření, biometrické nebo čipové karty.
Lidé	• Trénovací program pro vývojáře a administrátory. • Informovat a zvýšit povědomí o bezpečnosti. • Upozorňovat uživatele na hrozby. • Vytvoření plánu kontinuity a obnovy.
Právní	• Respektovat legální aspekty bezpečnosti. • Využití standardů a doporučení národní agentury pro kybernetickou bezpečnost. • Osvědčené postupy.

Výzkumná studie, která se zabývala tématikou kyberbezpečnosti v projektech Smart City analyzovala toto téma a autoři zjistili, že je potřebné využití pokročilých přístupů a technologií. Z této studie je patrné, že dochází k využití pěti přístupů a technologií, které jsou rozepsané v Tabulce 2 (Alamer a Almaiah, 2021).

Tabulka 2: Technologie řešení kyberbezpečnosti. Zdroj: Alamer a Almaiah (2021).

Technologie	Vysvětlení
Blockchain technologie	Blockchain umožňuje transparentní, decentralizované a bezpečné služby bez potřeby třetí strany. Využití pro identifikace a ověření identity, jelikož využívá implementace digitálních identifikačních metod.
Data-driven přístup	Principy a techniky založené na datech získaných a zanalyzovaných ze systémů nebo aplikací. Cílem je využití technologií k získání, ukládání a organizování dat ze Smart City aplikací a následné použití strojového učení a datové analytiky.
Hybrid Smart City Cyber Security Architecture metoda	Metoda analyzující hrozby v systémech a aplikacích s respektem k důležitým faktorům jako jsou cenná data, ukládání dočasných dat v paměti, obnovení dat a dobře řízená správa sítě a architektura systému.
Pravděpodobnostní model	Přidělení datových objektů mezi různými agenty pomocí Bigraphu. Cílem je zabezpečit kritická data odhalením viníka, který způsobil únik.
ICADS ontologie	ICADS je integrovaná vrstvená architektura pro Smart City zabezpečení. Využití dvou ontologií – OntoICADS a Secure-OntoICADS – pro vypořádání se s dynamikou a bezpečností Smart City.

2.1 STRATEGIE A PROJEKTY SMART CITIES

Existují doporučení a různé koncepty, které shrnují, jak přistupovat k budování, rozvoji a správě projektů Smart City, ať už se jedná o různé strategie, iniciativy, best practices a různé další dokumenty, které vznikly ve veřejném nebo soukromém sektoru, kam lze zařadit různé konzultační organizace. Zároveň se může jednat o doporučení a různé koncepty, které cílí globálně na všechny státy světa, na konkrétní oblasti nebo skupiny států, nebo jen na konkrétní stát a jeho města. Hlavní důvodem je, že různé oblasti, resp. města v daném státě mají svoje specifika, které často vychází z podobných podmínek nebo nadnárodních či národních cílů.

V tomto případě je tak jednodušší stanovit kritéria požadavků na Smart City projekty, sledovat je a vyhodnocovat. Často sem vstupuje také legislativa, která především pro oblast bezpečnosti a kyberbezpečnosti umožňuje sjednotit sledované požadavky. Tato kapitola se zabývá těmito koncepty a shrnuje obecná doporučení pro různé sektorové pohledy.

2.1.1 Mezinárodní sektor

Co se týká mezinárodního pohledu, tak zde vydalo World Economic Forum v roce 2021 white paper na téma řízení Smart Cities. Věnuje se významu etického a odpovědného vývoje Smart Cities v post covidovém období a utlumené globální ekonomice. Bylo využito srovnávacích měření vypracovaných G20 Global Smart Cities Alliance, ve které bylo porovnáváno 36 měst. Práce je rozdělena do pěti kapitol.

Obsah těchto kapitol je následující (World Economic Forum, 2021):

- Dig Once pro digitální infrastrukturu – bezdrátová i drátová. Cílem Dig Once politiky je zjednodušení a urychlení zavádění digitálních technologií do praxe, skrze spolupráce měst, konektivity poskytovatelů, společností, veřejných služeb atd. Související činnosti by měly být založeny na informovanosti a udržování komunikace se zúčastněnými stranami, stejně jako by mělo dojít k propojování těchto technologií např. přes IoT.
- Dostupnost ICT a souvisejících veřejných služeb pro všechny občany, včetně osob, která mají různá fyzická omezení nebo neovládají lokální jazyk daného města.
- Otevřená data je nutné využívat pro Smart City. Toto umožňuje větší integraci politik a datové infrastruktury pro dosažení efektivnějších toků dat přes všechny organizační složky města. Vymezení a nastavení opatření pro řízení dat vede k určení odpovědností za kvalitu dat, dodržování standardů atd. Zároveň je nutné zmínit rostoucí objemy dat a aplikace, která s nimi umí pracovat. Data jsou klíčový zdroj pro fungování Smart City.
- Je také potřebné vnímat důležitost soukromí a ochranu dat. Je nutné kontrolovat vliv nových technologií na soukromí a bezpečnost především tehdy, když je město ze zákona povinné řešit tuto oblast. Pro je se musí vytvořit související politiky a definovat, jak se město bude zapojovat s komunitou a být transparentní.
- Být odpovědný za kyberbezpečnost. Dokument zde doporučuje vytvoření struktury, resp. týmů s odborníky, kteří budou odpovědní za kyberbezpečnost ve svých oblastech v rámci Smart City, tzn. nastavení, měření, reakce v případě napadení a obnovení fungování dané služby, případně zálohy dat.

2.1.2 Nadnárodní sektor

Evropská komise vytvořila zprávu v rámci Smart City Information System (SCIS), která má sdílet získané klíčové poznatky a poskytovat doporučení, jak vytvářet a podporovat Smart City projekty. Cílem SCIS je podporovat a stimulovat úspěšné, funkční a inovativní technologie. Všechny tyto body, které zpráva Evropské komise doporučuje, lze zařadit do bezpečnostních potřeb, jelikož se na bezpečnosti také určitou mírou podílí (European Commision, 2017).

Doporučení, která zmiňuje Evropská komise v rámci této zprávy, jsou následující (European Commision, 2017):

- Přezkoumání struktury víceúrovňové správy, aby došlo k zajištění, že budou dostatečné pravomoci, které umožňují účinný a racionální proces dekarbonizace.
- Městská administrativa by měla využívat manažerských trénovacích programů a sdílet best practices s ostatními městy.
- Městská administrativa by měla zajistit, že požadavky všech městských částí jsou v souladu s moderními technologiemi. Je rovněž potřebné se vyhnout zdlouhavým byrokratickým postupům.
- Nařízení ohledně historických částí a estetických hodnot musí být v souladu s moderní technikou, aby se předešlo zbytečným omezením.
- Veřejné zakázky by měly být sladěny s potřebami inovativních řešení a jejich zadávání by mělo umožnit větší konkurenci i spolupráci mezi zúčastněnými stranami.
- Mělo by dojít k přezkoumání úrovně rozdělení pravomocí v souladu se zásadou subsidiarity pro lepší zavádění inteligentních řešení.
- Musí být posíleny příležitosti a schopnosti zřizovat úspěšná partnerství veřejného a soukromého sektoru.

Agentura Spojených států amerických s názvem Cybersecurity and Infrastructure Security Agency (CISA) společně s dalšími institucemi jako Federal Bureau of Investigation (FBI), National Security Agency (NSA), United Kingdom National Cyber Security Centre (NCSC-UK) nebo Canadian Centre for Cyber Security (CCCS) vytvořila dokument, který se zabývá osvědčenými postupy pro zabezpečení Smart City projektů. Tento dokument obsahuje pokyny, které poskytují doporučení pro soulad mezi inovačními cíli a výkonem v oblasti kyberbezpečnosti, ochrany soukromí a národní bezpečnosti. CISA doporučuje, aby docházelo ke předávání dat a informací v souladu s konkrétními požadavky na kyberbezpečnost tak, aby došlo k zajištění bezpečného provozu infrastrukturních systémů (CISA, 2023).

Doporučení, která plynou z tohoto dokumentu jsou následující (CISA, 2023):

- Bezpečné plánování a projektování. Tento bod v sobě zahrnuje doporučení aplikace principu nejnižších oprávnění, vynucování vícefaktorového ověřování, implementování architektury nulové důvěry (zero trust), spravování změny rizik interní architekturou, bezpečnou správu aktiv Smart City, zlepšení bezpečnosti zranitelných přístrojů, ochranu internetových služeb, aktualizovat aplikace v určeném časovém rozmezí a přezkoumání legálních, bezpečnostních a soukromích rizik spojených s nasazením.
- Proaktivní řízení rizik dodavatelského řetězce. Zde se jedná o dodavatelský řetězec softwaru, hardwaru a IoT zařízení, a poskytovatele spravovaných služeb a cloudových řešení.
- Provozní odolnost je poslední část, kterou je v tomto dokumentu zmíněna. Obsahuje doporučení pro zálohovací systémy a data, provádění školení zaměstnanců, vypracování a procvičování plánů obnovy a reakce na incidenty.

2.1.3 Národní sektor

Ministerstvo pro místní rozvoj ČR vydalo v roce 2018 dokument, který se zabývá metodikou pro vývoj a vznik Smart City projektů. Tento dokument obsahuje rozpis více aspektů, které je důležité brát v potaz při tvorbě Smart City. První oddíl dokumentu se zabývá infrastrukturou, do které patří mobilita, energetika a služby, a ICT. Pro čistou městkou mobilitu je potřebné řešit rovnováhu mezi všemi typy vozidel, ať už se jedná o motorové, osobní, nákladní, nebo cyklisty či chodce. Mělo by také dojít k zohlednění složek integrovaného záchranného systému (IZS), havarijních služeb a městské hromadné dopravy. Lze přitom využít moderních ICT nebo IoT. Dále se jedná o využití těchto technologií pro inteligentní energetiku, kde se dá využít například pro řízení spotřeby energie, hospodaření budov, využití prvků smart grid v rozvodné soustavě města a regionu, inteligentní řízení městských služeb k lepšímu využití energie a přírodních zdrojů. Také je zde kladen důraz na využití ICT technologií, které slouží jako podpora jak infrastruktury, tak i procesů řízení. Spadá sem komunikace města s občany skrze aplikace, monitorování a bezpečnostní systémy pro ochranu majetku a občanů, diagnostické systémy pro včasnou detekci poruch, inteligentní platební systémy v městských službách, koordinace informací o objektech a pozemcích se sdíleným využitím. Všechny výše zmíněné prvky vyžadují bezpečnostní řešení a mohou být považována za zranitelná (problémová) místa. Dále tato metodika také zmiňuje využití zelené infrastruktury ve městech. Je nutné mít také vytvořený strategický dokument Smart City, který by měl obsahovat koncept města, výchozí

situaci, formulaci cílů, analýzy a návrhy projektů, zhodnocení financí, realizace a monitoring (Ministerstvo pro místní rozvoj ČR, 2018).

Ministerstvo investicí, regionálního rozvoje a informatizace Slovenské republiky vydalo v roce 2023 dokument s názvem metodika k tvorbě inteligentních projektů. Tento dokument se věnuje rozvoji a metodice Smart Cities na Slovensku. Budování Smart City je zde rozděleno do 12 kroků. Prvním krokem je identifikace místních potřeb, které jsou očekávány od inteligentního projektu. V druhém kroku dochází k vypracování sady klíčových ukazatelů výkonnosti (key performance indicators) pro kvalitu života a nastartování změn. Třetím krokem je určení správných zúčastněných stran. Čtvrtým krokem je investice do zásad plánování a nových způsobů využití Smart City. Pátým krokem je přehodnocení relevantních strategií a vytvoření vlastního modelu Smart City. Šestým krokem je vytvoření dlouhodobého investičního plánu. Těchto prvním šest kroků spadá do první fáze, která se zabývá přípravou strategie. Druhá fáze je vytváření projektů pro Smart City. Do této fáze patří sedmý krok, kterým je vytvoření projektu ve smyslu základních cílů, konceptů a vazeb mezi nimi. Osmý krok v této fázi se zabývá přípravou a finalizací projektu na financování. Poslední fáze je chytré řízení a podpora pro Smart Cities. Do této fáze patří devátý krok, kterým je kapacita a podpora pro inteligentní samosprávu. Desátým krokem je podpora pro inovační trh. Jedenáctým krokem je monitorování a hodnocení. Posledním krokem je replikace postupů a škálování pro lepší optimalizaci (Ministerstva investícií, regionálneho rozvoja a informatizácie SR, 2023).

V roce 2017 byl německým spolkovým ministerstvem vnitra a komunity (Bundesministerium des Innern und für Heimat, BMI) vydán dokument, který definuje model inteligentního města orientovaného na budoucnost. Dokument představuje čtyři klíčové pokyny pro přeměnu měst na Smart City. Prvním pokynem je potřeba vytvoření cílů, strategií a struktur pomocí integrace digitální transformace do měst, identifikace oblastí aplikace a adaptace organizačních struktur ve městech. Druhým pokynem je být transparentní a využívat spoluúčasti a komunikace se zúčastněnými stranami. Třetím pokynem je vytvoření infrastruktury, dat a služeb. Zde je kladen důraz také na tvorbu a zabezpečení přístupu k digitální infrastruktuře, zodpovědné generování dat, zachování integrity a zajištění dlouhodobé udržitelnosti propojených infrastruktur a služeb. Čtvrtým pokynem je využití zdrojů, dovedností a kooperace. Jedná se získání dostatečných zdrojů pro lokální administrativu, vytváření digitálních dovedností a promování dlouhodobého učení, tvorbu inovativních postupů, tvorbu hodnot a posílení lokálních znalostí. Dále tento dokument obsahuje doporučení pro zúčastněné strany. Zde se jedná o vytvoření odpovídající strategie a generování sociální debaty, propojení digitálních a analogových procesů, provádění

analýz potřeb, rizik a dopadů, posílení místní ekonomiky a sousedství, vytvoření vhodného regulačního rámce, pilotní testování Smart City řešení, tvorbu a možnost využití open dat, komunikační aktivity pro digitální transformaci, zajištění dostatečných financí, podporu nezbytně nutné standardizace a užší zapojené uživatelů, sledování meziodvětvových dopadů Smart City projektů a výměna best practices a zkušeností (Bundesministerium des Innern und für Heimat, 2017).

Na webu vlády Spojeného království byla koncem roku 2021 vydána sada několika dokumentů (naposledy aktualizováno v červenci 2023), které se zabývají doporučeními pro zabezpečení propojených míst neboli Smart City projektů. Prvním dokumentem jsou základy pro pokyny pro zabezpečená propojená místa. Tento dokument v sobě obsahuje scénáře, které slouží jako podpora pro městskou administrativu. Obsahuje čtyři zdroje pro kyberbezpečnost na témata správy, zadávání veřejných zakázek a řízení dodavatelského řetězce a provádění analýz. Dále nalezneme zásady zabezpečení Smart City. Tato část je rozdělena do tří sekcí. První sekcí je porozumění, kde je důležité znát a vymezit případná rizika, znát požadavky na správu procesů spadající pod kyberbezpečnost, a porozumět právním a regulačním požadavkům. Druhou sekcí je design a architektura propojeného místa, kde probíhá zpravování a ukládání dat tak, aby snižovalo riziko narušení bezpečnosti, ochraňovalo data, bylo odolné a škálovatelné a zároveň zde bylo možné celý systém monitorovat. Třetí je správa propojeného místa, kde je nutné vzít v úvahu legislativu a práva, dodavatelský řetězec, správu procesů, a také plán odezvy a obnovy (Gov.uk, 2023).

2.1.4 Soukromý sektor

Information Technology and Innovation Foundation (ITIF) je americký neziskový think tank neboli instituce zaměřující se na mezioborový výzkum s cílem poskytnutí odborného pohledu. Tato instituce vydala v roce 2023 dokument, který poskytuje doporučení ohledně soukromí a inovací ve Smart City. V tomto dokumentu lze nalézt tři hlavní části. Těmi jsou sběr dat, ochrana osobních údajů a rovnováha soukromí při sběru dat pro různé oblasti. První část se zabývá technologiemi a aplikacemi pro sběr dat, která jsou dále využívány pro fungování a budování Smart City. Tyto technologie je doporučené využívat, ale je zde také nutné dávat pozor na soukromí s ohledem na to, jaká data o občanech dané technologie sbírají. Jedná se o inteligentní sítě, osvětlení, odpadkové koše, monitorování spotřeby vody, monitorování prostředí, inteligentní semafory, pokročilá veřejná doprava, chytré parkování, zpoplatnění přetížení nebo detekce střelby. Druhá část doporučuje využívat data, využívat vládního dohledu

a využívat dostatečné zabezpečení dat, jelikož město sbírá personalizovaná data o svých občanech. Ztráta dat rovněž může vést k finančním ztrátám a poškození image. Poslední část dokumentu je věnována balancování ostatních aspektů. Je totiž nutné všechny prvky města propojit a nesoustředit se pouze na jeden. Zde je kladen důraz na udržitelnost, náklady a další možnosti využití nasbíraných dat (Johnson, 2023).

Roland Berger je konzultační společnost, která v roce 2017 vydala dokument na téma Smart City. Tento dokument se zabývá mimo jiného i doporučeními pro rozvoj Smart City projektů. V tomto dokumentu je rozepsáno deset doporučení pro rozvoj a komplexní přístup. Toto vzniklo z důvodu toho, že mnoho měst má nejednotný přístup ke smart strategii, která se pouze zaměřuje jen na vybrané oblasti, a ne na celek. Prvním doporučením je přehodnocení role města a jeho správy a řízení. Toto je míněno vzhledem k využití nových chytrých technologií. Dále se jedná o zapojení občanů a dalších zúčastněných stran. Města by se měla vyhnout izolovaným řešením, propojovat služby v rámci e-governmentu a využívat již osvědčené postupy. Mnoho měst se soustředí pouze na individuální řešení, a ne na integrované. Rovněž je nutné podporovat občanské iniciativy, soběstačné obchodní modely a využívat příspěvky ze soukromého sektoru. S ohledem na datovou infrastrukturu by měly být vytvořeny komplexní datové strategie a různé datové platforem, jako např. open data portály. Je vhodné zřizovat inovační laboratoře pro podporu ekosystému Smart City, kde bude podporován celostní pohled na nové projekty. Velice důležitým bodem je zajištění bezpečnosti využívaných dat. Města by také měla zahrnout provozovatele infrastruktur do navrhování, financování a provádění iniciativ a zároveň získat politickou podporu a integrovat zpětnou vazbu od veřejnosti. Posledním doporučením je zřízení koordinačního orgánu a specializovaného plánovacího systému (Roland Berger, 2017).

2.2 HODNOTÍCÍ INDEXY A RÁMCE

Pro hodnocení Smart Cities existuje mnoho indexů a rámců, které tato města hodnotí a řadí dle různých kritérií. V této kapitole je porovnáno pět indexů, která byly publikovány alespoň dvakrát. Existují také další indexy, jako je Cities of the Future Index od organizace EasyPark nebo SmartEcoCity Index od SmartEcoCity, ale nebudou blíže popsány, protože se jedná pouze o jednorázové zprávy.

Prvním indexem v Tabulce 3 je Cities in Motion Index (CIMI), který publikuje IESE Business School od roku 2014, když poslední zpráva z roku 2022 porovnává celkem 183 měst (první porovnávala 135 měst). Global Cities Index (GCI) a Global Cities Outlook (GCO) jsou publikovány společností Kearney v rámci Global Cities Report od roku 2008 a prozatím vyšlo

13 zpráv, které tak umožňují komplexně porovnat vývoj některých měst v této oblasti (v roce 2008 bylo porovnáno jen 60 měst oproti roku 2023, kdy se jednalo o 156 měst). Global Power City Index (GPCI) je publikován Mori Memorial Foundation od roku 2015. Zpráva Smart City Governments (SCG) hodnotí rozvoj 50 Smart Cities z pohledu městské administrativy a toho, jak zástupci měst podporují rozvoj Smart City (především různé formy podpory projektů). Poslední zpráva pochází z roku 2021. GPCI i SCG srovnávají jen největší světová města, většinou hlavní města. IMD Smart City Index (SCI) byl poprvé publikován v roce 2019, kdy hodnotil 102 měst oproti 141 v roce 2023, a to s důrazem na ekonomické a technologické aspekty Smart Cities s ohledem na indikátory lidského kapitálu jako je kvalita života atd.

Tabulka 3: Porovnání indexů a rámců pro hodnocení konceptu Smart City. Zdroj: vlastní.

Index / rámec	**Vydavatel**	**Počet vydaných zpráv**	**Aktuální (poslední vydaná) zpráva**	
			Počet měst	**Dimenze / kategorie hodnocení**
CIMI	IESE Business School	8 (2014–2022)	183	Lidský kapitál, sociální soudržnost, ekonomika, správa města, prostředí, doprava a transportace, urbanismus, mezinárodní profil, technologie.
GCI	Kearney	13 (2008–2023)	156	Podnikové aktivity, lidský kapitál, výměna informací, kulturní zkušenosti, politická angažovanost.
GPCI	Mori Memorial Foundation	9 (2015–2023)	48	Ekonomika, věda a výzkum, kulturní interakce, živobytí, prostředí, dostupnost.
SCG	Eden Strategy Institute	2 (2019–2021)	50	Vize, vůdcovství, rozpočet, finanční pobídky, podpůrné programy, připravenost občanů, zaměřenost na občany, inovační ekosystém, chytré politiky, výkon v oboru.
SCI	IMD Business School	4 (2019–2023)	141	Postoje, struktury města, využité technologie.

Každý z těchto indexů zahrnuje různé dimenze / kategorie, jako je kvalita života nebo chytré vzdělávání (viz poslední sloupec v Tabulce 3), a různé sady ukazatelů, které měří konkrétní akce nebo zlepšení v rámci příslušných dimenzích / kategoriích, když těchto indikátorů mohou

být i desítky a během let se mění. Některé z těchto indexů zahrnují také sub-indexy, které jsou reprezentovány dimenzemi, kategoriemi nebo oblastmi a mohou také sloužit k hodnocení Smart Cities. Všechny tyto strukturální úrovně, podle kterých lze dané město porovnávat jsou sdruženy do rámce, který slouží k výpočtu konkrétních hodnot a pořadí pro dané město. Vydávání jednotlivých zpráv se mezi porovnávanými indexy liší, nicméně zpravidla je to každý rok nebo jednou za dva roky. Každá zpráva zároveň obsahuje i metodiku, podle které bylo určeno pořadí daného města v daném roce. Zpráva zpravidla obsahuje i změny provedené v rámci a metodice, tzn. odstraněné nebo nové indikátory, zvýšení váhy (významu) dané dimenze / kategorie atd.

CIMI vytváří své hodnocení pomocí devíti dimenzí. První je lidská kapitál neboli schopnost udržet, a hlavně rozšiřovat talent, zlepšovat vzdělání, podporovat tvořivost a výzkum. Druhou dimenzí je sociální soudržnost a to, jak město podporuje socializaci a spolupráci mezi občany. Dalším je ekonomika, když zde se jedná o zamření na podporu ekonomického rozvoje daného města. Správa města je další dimenzí a měří účinnost, kvalitu a správné zaměření státních intervencí a podpor města. Mezi další dimenze pak spadá prostředí, doprava a transportace, urbanismus, mezinárodní profil, technologie (IESE Business School, 2022).

Kearney vytvořilo svůj hodnotící rámec GCI, s nímž v dané správě publikuje pořadí GCO, které představuje pohled do budoucnosti, jak města vytvářejí podmínky pro svůj budoucí status jako globální centra. Rámec GCI využívá 29 metrik, které spadají do 5 dimenzí. Mezi tyto dimenze patří podnikové aktivity, lidský kapitál, výměna informací, kulturní zkušenosti a politická angažovanost. Do podnikové aktivity spadá kapitálový tok, dynamika trhu, přítomnost významných společností. Lidský kapitál jsou úrovně vzdělání. Informační výměna je složena z přístupu k informacím skrze internet a další mediální zdroje. Do kulturní zkušenosti patří přístup do muzeí, kulturní a sportovní události. Politická angažovanost je hodnocena podle politických událostí, think tanků a ambasád (Kearney, 2023).

GPCI má metodiku založenou na šesti funkcích. První je ekonomika, do které spadá velikost trhu, tržní atraktivita, vitalita, lidský kapitál, byznys prostředí a jednoduchost provozu byznysu. Druhou je věda a výzkum, kam spadají akademické zdroje, inovace a prostředí pro vývoj. Třetím je kulturní interakce, ve které se nachází turismus, mezinárodní interakce, schopnost tvořit trendy, kulturní místa a návštěvnické oblasti. Čtvrtým je živobytí, do kterého patří pracovní prostředí, náklady na život, jednoduchost žití, pohoda a bezpečnost a ochrana. V oblasti bezpečnosti a ochrany jsou vymezené body pro počet vražd a ekonomický risk životní

pohromy. Pátou funkcí je prostředí, kde je udržitelnost, kvalita ovzduší a městské prostředí. Poslední funkcí je dostupnost, do které spadají mezinárodní sítě, letecká doprava, doprava ve městě a komfort dopravy (Mori Memorial Foundation, 2023).

SCG index je tvořen deseti dimenzemi. Mezi ně patří vize, vůdcovství, rozpočet, finanční pobídky, podpůrné programy, připravenost občanů, zaměřenost na občany, inovační ekosystém, chytré politiky a výkon v oboru. V metodice je uvedeno, že bezpečnostní prvky jsou vztažené v dimenzi chytré politiky, příkladem je zde ochrana Internet Protocol (IP) adresy (Eden Strategy Institute, 2021).

SCI je hodnotící rámec, který je tvořen IMD Business School for Management and Leadership. V tomto rámci dochází k rozdělení do dvou kategorií, jedná se o strukturu a technologie. Struktura odkazuje na existující infrastrukturu města a technologie odkazují na technologické opatření a dostupné služby. Jak struktura, tak technologie jsou ohodnocovány skrze pět klíčových oblastí – zdraví, bezpečnost, mobilita, aktivity, správa a příležitosti. Co se týče bezpečnosti a kyberbezpečnosti, tak tento index pouze hodnotí, jestli se lidé cítí bezpečně v rámci struktury a v rámci technologií, např. zda jsou kamerové systémy dostačují. Dalším hodnotícím prvkem jsou postoje, které jsou vztažené na aspekty soukromí, tzn. zda jsou obyvatelé ochotni poskytnout osobní data, využívat rozpoznávání obličeje a jak funguje dostupnost online informací a zda jim lze důvěřovat (IMD Business School, 2023).

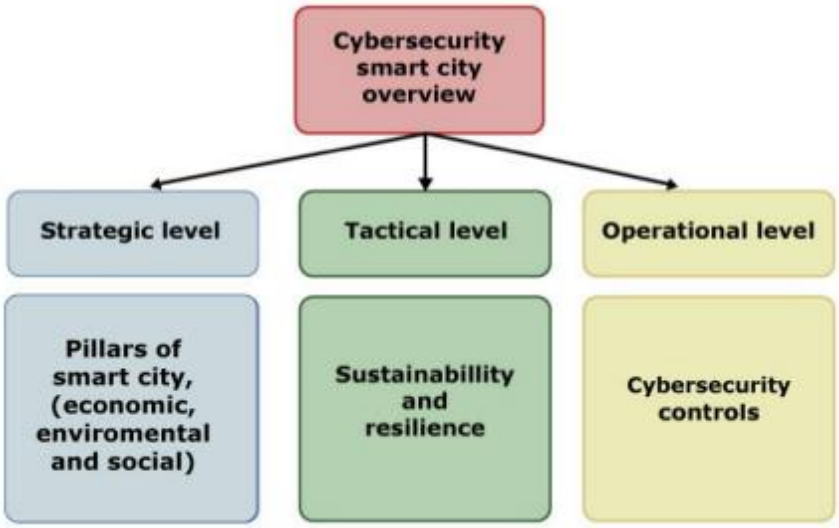
2.3 VÝZKUMNÉ PRÁCE

Na téma Smart City a kyberbezpečnost, resp. ochrana dat, v rámci strategií a projektů, existují různé vědecké práce, které se snaží tuto problematiku řešit, zkoumat, prezentovat studie nebo sumarizovat existující problémy a navrhovat řešení. V této kapitole práce jsou shrnuta různá doporučení pro kyberbezpečnost a ochranu dat z různých výzkumných prací a článků, ať už se bude jednat o modely, metodiky nebo různé postupy. Výběr nejvhodnějších zdrojů probíhal vyhledáváním klíčových slov (*smart city AND cybersecurity OR data protection*) v databázích Scopus, Web of Science a Google Scholar. Byly vybrány nejvíce relevantní zdroje, které jsou nejčastěji citovány.

Chen Ma ve své práci na téma Smart City a kyberbezpečnost popsal několik bezpečnostních řešení, která se dají využít. Prvním je bezpečnost kritické infrastruktury, do které spadá ochrana komunikační sítě, energetické přenosové sítě, čističek vody, semaforů, prodejních míst nebo zdravotních středisek. Tato místa nejsou přímo spojena s kyberútoky, ale slouží jako vstupní

brána pro malware. Bezpečností řešení se týkají zabezpečení sítě, zlepšení zabezpečení pomocí bezpečnostních programů, informační bezpečnosti, zlepšení bezpečnosti pomocí využití cloudu, vytvoření plánu obnovy po havárii, provozní bezpečnosti, zabezpečení IoT, trénovacích programů pro uživatele a zabezpečení aplikací. Dále tato práce rozebírá a doporučuje využití hlubokého učení, které se dá též aplikovat na kyberbezpečnost. V práci je dále uvedeno několik bodů, kterým by měla být věnována největší pozornost. Prvním je najmutí bezpečnostního experta. Mělo by dojít k anonymizaci uživatelských dat a získat povolení pro aplikace, které ukládají citlivá data. Nemělo by docházet ke zveřejňování citlivých informací a v případě úniků vše nahlásit relevantním autoritám. Města by dále měla investovat do nástrojů, které omezují přístup k informacím pro třetí strany nebo dodavatele a neustále skenovat zařízení, databáze a unikající informace. Dále je nutné používat složitá hesla s vícefaktorovým ověřováním, využívat více vrstev zabezpečení a používat VPN pro komunikaci. Dále pravidelně využívat aktualizace pro SW a operační systémy, nevyužívat veřejné Wi-Fi pro přístup k citlivým datům nebo zasílání informací (Ma, 2021).

Dalšími doporučeními jsou zabezpečení týkající se IoT, které je často využívané v rámci fungování města a smart aplikací. Andrade, společně s kolegy, sepsali výzkumnou práci s názvem *A Comprehensive Study of the IoT Cybersecurity in Smart Cities*. Pro zabezpečení IoT se doporučuje využívat autentizace, jelikož nejsou tolik využívány kryptografické algoritmy, je nedostatečná správa hesel a průměrné heslo v IoT přístrojích je často krátké. Dále je nutné využívat a mít zavedenou kontrolu přístupů, kvůli manipulaci s metadaty, špatné konfiguraci přístroje nebo obcházení kontroly přístupu. Měly by se kontrolovat také vstupy a výstupy v IoT, tímto lze zamezit např. Denial of Service (DoS) nebo Distributed Denial of Service (DDoS) útokům. Dále zabezpečit komunikaci a související kanály a k tomuto využívat i kryptografii, jelikož na ní není v komunikačních protokolech spoléháno. Pro vytvoření rámce, viz Obrázek 1, je nutné dbát rozdělení bezpečnosti do tří úrovní. Strategická úroveň odkazuje na tři pilíře, na kterých je Smart City postaveno, tedy ekonomika, prostředí a sociální dimenze. Taktická úroveň odkazuje na udržitelnost a odolnost celého řešení. Operační úroveň je poté zaměřena na implementace prvků jako jsou bezpečnostní kontroly, detekce nedostatků a slabých míst, výpočetní infrastruktura, efektivita reakcí na incidenty a přístupů k zařízením atd. (Andrade et al., 2020).



Obrázek 1: Úrovně řešení kyberbezpečnosti ve Smart City. Zdroj: Andrade et al. (2020).

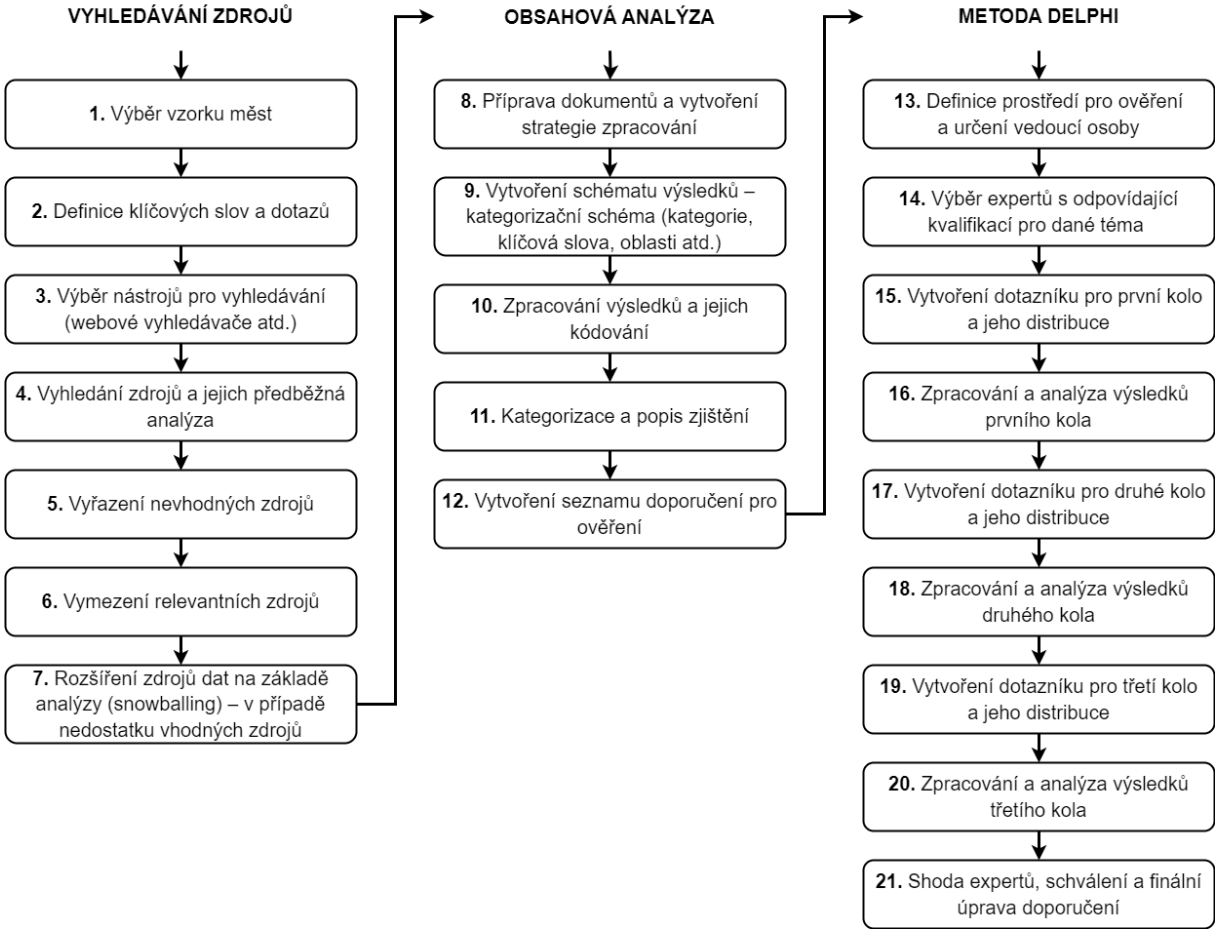
V další práci jsou rozebrány tři bezpečnostní dopady architektury Smart City. Komplexní přístup zahrnuje vícevrstvý bezpečnostní mechanismus. Tento mechanismus zajišťuje ochranu všech úrovní systémů, které se skládají z fyzické, komunikační a databázové komponenty. Je nutné také zabezpečit přístroje, které se využívají v rámci Smart City. Jejich zabezpečení by mělo probíhat na čtyřech úrovních. Těmi jsou firmware, přístroje, obvody a energie. Do firmwaru spadá zajištění izolace operačního systému a ověření integrity platformy. Pro úroveň přístroje jde o vymazání paměti a zabránění klonování přístroje. Úroveň obvodu znamená ochrana proti laserové injektáži nebo imunita vůči analýze kanálů založených na výkonu. Energetická úroveň jsou protiopatření proti vyčerpání energie nebo baterie (Habibzadeh et al., 2019).

3 ANALÝZA A VYHODNOCENÍ ZÍSKANÝCH DAT

Tato kapitola je zaměřena na nalezení a analýzu Smart City strategií. Jedná se o nalezení, zpravování a vyhodnocení dat ohledně strategií, projektů a různých plánů, které jsou spjaté se Smart City. Nejprve je představena metodika, pomocí které byla data získána, analyzována, vyhodnocena, a zároveň také ověřena za účelem získání doporučení pro danou problematiku. Následují kapitoly, kde jsou jednotlivé kroky metodiky blíže popsány.

3.1 METODIKA A POSTUP ŘEŠENÍ

Metodický postup směřující ke splnění cíle této diplomové práce, tzn. *analyzovat problematiku kyberbezpečnosti a ochrany dat ve strategiích a projektech Smart Cities ve vybraných světových městech a na základě těchto zjištění navrhnout doporučení pro tuto problematiku*, je zobrazen na Obrázku 2.



Obrázek 2: Metodika řešení cíle diplomové práce. Zdroj: vlastní.

Postup řešení lze rozdělit do tří částí (fází), kde každé z nich se skládá z různého počtu kroků. Prvním krokem je vymezení a výběr vzorku měst. Města jsou vybrána podle existujících Smart City indexů, které by měly reprezentovat to, že se dané město hlásí ke konceptu Smart City. Na základě porovnání indexů v kapitole 2.2 byl jako klíčový index zvolen CIMI, jehož poslední vydání je z roku 2022. Zároveň však také došlo k porovnání i s ostatními Smart City indexy zmíněnými v kapitole 2.2 a jejich, v danou chvíli, nejnovějšími verzemi. Na základě zjištění vyplývajících z tohoto porovnání bylo určeno, že města budou vybírána ze čtyř kontinentů a jejich počet je omezen na maximálně šest měst z jednoho kontinentu. Tato kritéria byla zvolena proto, aby došlo k analýze co největšího rozpětí existujících Smart City strategií a nebyla vybrána pouze města z jednoho nebo dvou kontinentů, u kterých lze předpokládat podobné přístupy ke strategiím a projektům Smart Cities, viz např. společná doporučení pro státy EU, což by mohlo ovlivnit komplexní analýzu možných existujících globálních řešení a přístupů.

Další kroky vyhledávání zdrojů zahrnují definici klíčových slov a dotazů, výběr webových vyhledávačů a dalších online informačních zdrojů (např. United Nations Digital Library, kde lze nalézt různé zprávy z dané oblasti), předběžnou analýzu nalezených zdrojů a jejich vhodnost pro potřeby diplomové práce, vyřazení nevhodných zdrojů, vytvoření seznamu relevantních zdrojů, a nakonec jeho doplnění o další možné zdroje, pokud je jejich počet získaný na základě předchozích kroků nedostačující. Za tímto účelem byl zvolen postup nazývaný snowballing, kdy na již nalezené zdroje se nabalují další související zdroje, např. když je v nalezeném zdroji zmínka o jiném zdroji, který ale nelze nalézt online nebo je přístupný jen po přihlášení. I takto nalezené zdroje jsou pro analýzu přínosné, protože mohou obsahovat důležité informace. Více informací k vyhledávání zdrojů lze nalézt v kapitole 3.3.

Obsahová analýza zdrojů je zaměřena na kroky, jejichž cílem je analýza nalezených dokumentů a hledání toho, zda se zmiňují o bezpečnosti, kyberbezpečnosti nebo ochraně dat. Dále jakým způsobem k tomu vybraná města přistupují, zda mají vytvořené vlastní plány a strategie nebo se pouze řídí zákony a tím, co vyžaduje stát ohledně soukromí a ochrany dat. Průběžné výsledky byly systematicky zpracovávány tak, aby byly jednak přehledné, a jednak kategorizovatelné pro další zpracování, tzn. tvorba vhodných schémat. Dalším krokem tedy bylo zpracování výsledků a jejich kódování, tzn. vytvoření tabulky, kde byla vždy uvedená daná strategie, její popis a další charakteristiky, uvedení hledaného klíčového slova nebo skupiny slov, kolikrát je zmíněno a v jakém kontextu, resp. k jaké komponentě nebo oblasti Smart City se vztahuje. Na

základě toho pak byla vytvořena doporučení, která sloužila jako vstup do fáze jejich ověření. Podrobně lze tyto kroky druhé fáze nalézt v kapitolách 3.4 a 3.5.

Poslední fází, která má pomoci ke splnění cíle této práce, je využití metody Delphi pro ověření a vytvoření konečného seznamu doporučení pro problematiku kyberbezpečnosti a ochrany dat ve Smart Cities. V prvním kroku této fáze je definováno prostředí pro ověření, tzn. modelové Smart City mající za cíl řešit problematiku kyberbezpečnosti a ochrany dat, a vybrána vedoucí osoba, která bude řídit proces průběhu této metody, zpracovávat a vyhodnocovat získaná data. Dalším krokem je výběr vhodných expertů s odpovídajícími znalostmi a kvalifikací pro dané téma. Následuje vytvoření dotazníku pro první kolo a jeho distribuce. S ohledem na zapojení expertů z různých zemí byly dotazníky distribuovány v elektronické podobě. Výsledky prvního kola jsou pak zpracovány a analyzovány, když vedoucí osoba rozhoduje o tom, jaké informace a doporučení budou upraveny podle připomínek expertů. Všechny provedené změny a výsledky jsou vždy k dispozici expertům pro další kola, aby na jejich základě potenciálně mohli upravit svoje hodnocení, dokud nedojde ke shodě mezi experty a schválení finálních doporučení. Do druhého kola tedy vstupuje upravený dotazník. Pokud se experti ve druhém kole neshodnou na seznamu doporučení, tak následují další kola. Proces metody Delphi končí, když se všichni experti shodnou a nenavrhují další úpravy. Zároveň je nutné zmínit, že význam jednotlivých doporučení se u expertů bude lišit, protože není cílem se shodnout na nějaké hodnotě, ale seznamu finálních doporučení. Podrobněji jsou jednotlivé kroky metody Delphi a výsledky popsány v kapitole 4.

3.2 VÝBĚR VZORKU

Města byla vybrána podle hodnotících indexů Smart City. Jako hlavní index byl vybrán CIMI 2022, podle jehož pořadí měst byla města pro vzorek postupně vybírána s ohledem na pravidlo maximálně šesti měst na jeden kontinent, tzn. Severní Amerika, Evropa, Asie a Oceánie. Tímto je zaručeno porovnání strategií Smart City z více států a zároveň dostatek vstupních dat pro analýzu těchto dokumentů. Dále byla tato města porovnána s ostatními indexy a byla vybírána města, která se objevují i v těchto ostatních indexech. Mezi ostatní indexy patří GCI 2023, GPCI 2023, SCG 2021 a SCI 2023. Takto bylo vybráno celkem 22 měst, viz Tabulka 4.

Pro Severní Ameriku, Evropu a Asii je vybráno šest měst na kontinent, kdy vybraná města jsou zastoupena alespoň ve čtyřech indexech. Jedinou výjimkou je Praha, která je zařazena pro porovnání ČR se zbytkem světa. Z důvodu menší dostupnosti dat pro Oceánii jsou odsud vybrána pouze čtyři města a jsou zde zařazena i města, která nejsou obsažena ve více indexech.

Čísla ve sloupcích tabulky níže znamenají pořadí města v žebříčku daného indexu v daném roce. Všechny indexy řadí města od nejlepšího, tzn. pořadí 1., 2., 3. atd. Zároveň je nutné zmínit, že každý index porovnává různý počet měst (viz Tabulka 3 v kapitole 2.2), a proto horší umístění nemusí nutně znamenat horší výsledky.

Tabulka 4: Výběr vzorku 22 měst odpovídajících konceptu Smart City. Zdroj: vlastní.

Index / Město	CIMI 2022	GCI 2023	GPCI 2023	SCG 2021	SCI 2023
Severní Amerika					
New York (NYC)	2.	1.	2.	6.	21.
Washington DC	6.	19.	36.	-	39.
Chicago	13.	11.	25.	42.	61.
San Francisco (SF)	16.	17.	27.	13.	68.
Toronto	21.	15.	23.	-	48.
Los Angeles (LA)	22.	8.	21.	40.	50.
Evropa					
Londýn	1.	2.	1.	3.	6.
Paříž	3.	3.	4.	-	46.
Berlín	5.	16.	10.	23.	33.
Amsterdam	8.	20.	6.	10.	15.
Kodaň	10.	41.	11.	35.	4.
Praha	43.	47.	-	-	14.
Asie					
Tokio	4.	4.	3.	22.	72.
Singapur	7.	7.	5.	1.	7.
Soul	12.	14.	7.	2.	16.
Hong Kong (HKG)	26.	10.	18.	41.	19.
Tchaj-pej	34.	59.	35.	19.	29.
Peking	37.	5.	17.	15.	12.
Oceánie					
Sydney	36.	18.	12.	18.	18.
Melbourne	38.	9.	9.	20.	31.
Canberra	40.	-	-	-	3.
Wellington	70.	-	-	33.	23.

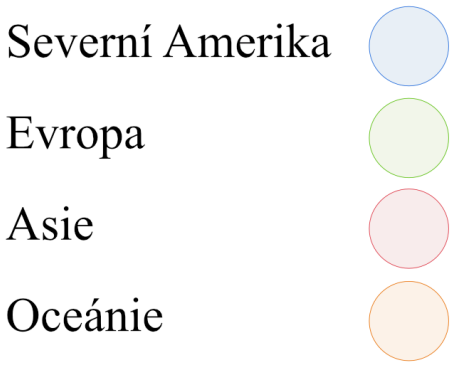
3.3 VYHLEDÁVÁNÍ ZDROJŮ DAT

Tato část práce se blíže zabývá postupem vyhledávání strategií, projektů, plánů, konceptů, dokumentů, webových stránek a dalších zdrojů dat pro vybraná Smart Cities. Pro vyhledávání bylo využito webových vyhledávačů Google a Bing, případně dalších informačních zdrojů. Pro jednotlivá města byly vyhledávány primárně zdrojové dokumenty a sekundárně webové stránky, které města vytvářejí jako webový rozcestník a informační podporu pro koncept Smart City.

Postup vyhledávání se skládal z vymezení klíčových slov. Bylo použito jméno města společně s pojmy Smart City, plan, strategy, documentation, concept. Příkladem je *New York AND Smart City AND plan OR strategy OR documentation OR concept*. Při vyhledávání byl nejdříve používán anglický jazyk. Pokud se nepodařilo nalézt žádné dokumenty nebo webové stránky v anglickém jazyce, tak došlo k přeložení do jazyka státu, ve kterém se město nachází.

Seznam nalezených dokumentů je zobrazen v Tabulce 5. S těmito dokumenty se dále pracuje při jejich analýze, která se zaměřuje na to, zda obsahují informace ohledně bezpečnosti dat nebo kyberbezpečnosti jako celku. Jelikož budou tyto informace zpracovány i pro šest komponent Smart City, tak i pro ně byly vyhledávány informace týkající se kyberbezpečnosti a ochrany dat. Seznam těchto zdrojů je obsažen v Příloze I.

U Tabulky 5 stejně jako i v tabulkách v následujících kapitolách, jsou města barevně odlišena pro lepší orientaci. Severní Amerika je zobrazena modrou barvou, Evropa zelenou barvou, Asie červenou barvou a Oceánie oranžovou barvu. Legenda pro tabulky je zobrazena na Obrázku 3.



Obrázek 3: Legenda barev pro tabulky s výstupy hodnocení Smart Cities. Zdroj. vlastní.

Tabulka 5: Přehled zdrojů nalezených pro vybraná Smart Cities. Zdroj: vlastní.

Město	Typ	Název	Rok vydání	Počet stran
NYC	Dokument	Building a smart + equitable city	2015	23
	Dokument	OneNYC 2050	2019	59
	Dokument	The New York City Internet of Things Strategy	2021	77
Washington DC	Dokument	Smart DC	2016	33
	Web	DC comprehensive plan	2024	-
Chicago	Dokument	IT Strategic Plan	2021	167
	Dokument	The city of Chicago technology plan	2013	94
	Web	Smart Grid for a Smart Chicago	2024	-
SF	Dokument	San Francisco digital services strategy	2015	65
	Dokument	City of San Francisco Meeting the Smart City Challenge Volume 1	2016	74
	Dokument	City of San Francisco Meeting the Smart City Challenge Volume 2	2016	335
Toronto	Web	Toronto official plan	2023	-
	Web	Connected Community / Smart City TO	2019	-
	Dokument	Digital infrastructure Strategic framework City of Toronto	2022	108
LA	Dokument	SmartLA 2028	2020	54
Londýn	Dokument	Smart London plan	2014	54
	Dokument	Smarter London Together	2018	60
	Web	London programmes and strategies	2024	-
Paříž	Dokument	Paris smart and sustainable	2020	60
	Web	Paris Services	2024	-
Berlín	Dokument	Gemeinsam digital: Berlin	2022	78
	Web	Smart City Berlin Publications	2024	-
Amsterdam	Dokument	Amsterdam Circular 2020-2025 Strategy	2020	30
	Web	Responsible Sensing Lab	2024	-
	Web	Amsterdam Smart City	2024	-

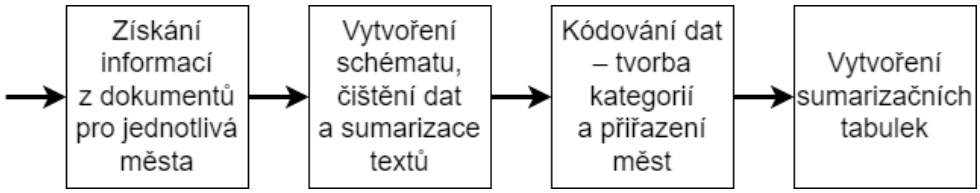
Město	Typ	Název	Rok vydání	Počet stran
Kodaň	Dokument	Smart city Infrastrukturanalyse	2016	64
	Web	Copenhagen Solution Lab	2024	-
	Dokument	ITS, data collection and the Personal Data Act	2014	2
Praha	Dokument	Koncepce Smart Prague do roku 2030	2017	88
	Web	Smart Prague	2024	-
	Dokument	Smart Prague Index ročenka 2022	2022	33
Tokio	Web. dok.	Future Tokyo version 2023	2023	172
	Dokument	Smart Tokyo implementation strategy	2020	69
	Web	Promoting Smart Tokyo	2024	-
	Web	Data Connect Project	2024	-
Singapur	Dokument	Security Industry Digital Plan	2023	6
	Web	A Secura Smart Nation	2024	-
	Web	IMDA Singapore	2024	-
Soul	Web. dok.	Sustainable Seoul Smart City	2017	54
	Web	Smart Seoul	2024	-
	Web	Seoul Digital Archive	2024	-
	Web	Smart City Seoul Policy	2024	-
HKG	Dokument	Hong Kong Smart City Blueprint 2.0	2020	36
	Web	Hong Kong Smart City Blueprint	2024	-
Tchaj-pej	Dokument	Smart Taipei, One City	2023	35
	Dokument	Smart Taipei: Government as a Platform City as a Living Lab	2023	209
	Web	Smart Taipei	2024	-
Peking	Dokument	Akční program města Peking pro rozvoj Smart Cities v období 14. pětiletého plánu	2020	27
	Dokument	Smarter Beijing 2019	2019	41
	Web	Beijing City lab	2024	-
Sydney	Dokument	Smart City Strategic Framework	2020	58
	Dokument	Sustainable Sydney 2030—2050	2022	106

Město	Typ	Název	Rok vydání	Počet stran
Melbourne	Dokument	Future Melbourne 2026	2016	28
	Web	Participate Melbourne	2024	-
Canberra	Dokument	ACT Digital Strategy	2020	31
	Dokument	Data Governance and Management Policy Framework	2020	45
	Dokument	Records Management Program: Policy and Procedure	2022	14
Wellington	Dokument	Wellington towards 2040: smart capital	2011	41
	Web	Abosolutely Positively Wellington City Council	2024	-
	Dokument	Wellington Resilience Strategy	2017	116

3.4 VYHODNOCENÍ VÝSLEDKŮ PRO SMART CITY STRATEGIE

Vyhodnocení nalezených zdrojů se skládá z jejich analýzy a kódování, tzn., zda obsahují sekce nebo alespoň odstavce či věty zabývající se bezpečností, kyberbezpečností, ochranou dat, práci s daty a podobné informace, ze kterých lze vyvodit relevantní závěry pro danou problematiku. Výsledky pro analyzované Smart City strategie jsou zobrazeny jako souhrny v Přílohách II, III, IV a V pro Severní Ameriku, pro Evropu, pro Asii a pro Oceánii.

Postup řešení obsahové analýzy dokumentů a webových stránek spočívá v jejich prozkoumání, prohledání a přečtení, a to s využitím obsahu dokumentů a jejich struktury, vyhledávání slov jako je kyberbezpečnost, ochrana, data, využití dat atd. (vše v jazyce daného zdroje). V rámci webových stránek jde o vyhledávání stejných klíčových slov, kontrolu sekcí (mapa stránek) týkajících se různých plánů, oblastí, projektů atd. Z tohoto tedy bylo vytvořeno kategorizační schéma výsledků. Součástí kódování pak bylo systematické evidování nalezených poznatků a vytváření poznámek v MS Excel, tzn., že vždy existuje sloupec s daným městem, zdrojem, dále číselným označením nalezené informace (slova nebo textu), aby vždy bylo jasné, kde byla daná informace nalezena. Tyto poznatky byly po analýze všech zdrojů znovu zkontrolovány a očištěny o nepotřebné a nerelevantní informace pro tuto diplomovou práci. Na základě toho pak byly vytvořeny kategorie, včetně měst, která do dané kategorie spadají. Nakonec byly vytvořeny sumarizační tabulky měst podle kontinentů. Celý postup je uveden na Obrázku 4.



Obrázek 4: Postup analýzy nalezených zdrojů pro strategie Smart Cities. Zdroj: vlastní.

V Přílohách II, III, IV a V jsou uvedené všechny tabulky pro nalezené prvky kyberbezpečnosti, ochrany dat a přístupu k datům. Takto získané výsledky byly kategorizovány a odpovídající města byla přiřazena do těchto kategorií, tzn., zda obsahují informace v rámci daných kategorií. Nalezené shrnutí je zobrazené v Tabulce 6.

Tabulka 6: Shrnutí přístupů k ochraně dat a kyberbezpečnosti pro Smart Cities. Zdroj: vlastní.

Kyberbezpečnost a ochrana dat	**Město**
1. Jsou implementována bezpečností řešení pro IoT a práci s takto získanými daty.	NYC, SF, LA
	Berlín, Amsterdam, Kodaň, Praha
	Peking, Soul, Tchaj-pej
	Wellington, Canberra
2. Vládní systémy pro občany, shromažďují kontakty, komunikace mezi vládou a občany. Online nástroje pro sběr a sdílení dat a jejich využití pro bezpečnostní prvky.	NYC, Washington
	Londýn, Paříž, Berlín, Praha
	Singapur, Soul, HKG, Tchaj-pej, Peking
	Sydney, Canberra, Wellington
3. Digitální sledovací systém zpracovává údaje z kamer, zvuky, sledovací technologie, monitorovací technologie.	NYC, Toronto, LA
	Paříž, Amsterdam, Kodaň, Praha
	Tokio, Singapur, Soul, Tchaj-pej, Peking
	Sydney, Canberra
4. Transparentnost, sběr pouze potřebných dat, zahrnutí aspektu soukromí, omezení shromažďování osobních údajů.	SF, Toronto
	Londýn, Paříž, Amsterdam, Kodaň

Kyberbezpečnost a ochrana dat	Město
	Tokio, Peking
	Melbourne, Canberra
5. Nastavení, vytvoření a implementovaní postupů a zásad pro ochranu osobních údajů.	Washington, Chicago, SF, Toronto, LA
	Londýn, Paříž, Berlín
	Singapur, Soul, Tchaj-pej
	Sydney, Melbourne, Canberra
6. Využití open dat a vytvoření odpovídajících standardů.	Washington, SF
	Londýn, Paříž, Berlín, Amsterdam, Kodaň, Praha
	Tokio, Singapur, Soul, HKG
	Sydney, Melbourne, Wellington
7. Vytvoření entity, která spravuje kyberbezpečnost a ochranu dat.	NYC, Chicago, SF
	Londýn
	Singapur, Soul, Tchaj-pej
	Melbourne
8. Projekty vyhodnocení připravenosti kybernetické bezpečnosti a monitorování rizikových přístupů.	Washington, SF, Toronto
	Singapur, Soul
	Sydney
9. Využití nových metod a technologií pro shromažďování, analyzování a publikování dat.	Chicago, SF, Toronto
	Londýn, Amsterdam, Kodaň, Praha
	Tokio
10. Vypracování strategií a projektů kybernetické bezpečnosti, včetně datové strategie.	Londýn, Berlín, Amsterdam, Kodaň
	Singapur, Soul, Tchaj-pej
	Sydney, Canberra
11. Umělá inteligence, big data, datové platformy.	Praha, Amsterdam
	Tokio, Singapur, Soul, HKG, Tchaj-pej

Kyberbezpečnost a ochrana dat	Město
12. Integrita dat.	SF, Toronto
	Singapur
	Sydney
13. Sdílené služby pro IT po městě, standardizace IT postupů, vývoj IT, využití open-source pro IT.	Chicago
	Berlín
	HKG, Tchaj-pej
	Canberra, Wellington
14. Kontrola přístupu osob.	SF, Toronto
	Kodaň
	Singapur
15. Vzdělání a školení zaměstnanců a občanů. Nábor IT odborníků.	SF
	Paříž
	Tokio, HKG
	Melbourne, Canberra
16. „Jedna síť“ – jednotný přístup vládních služeb. Spolupráce vládních a veřejných služeb napříč městem.	Londýn
	Peking, HKG
	Sydney
17. Privacy-By-design, Security-by-design přístup.	Toronto
	Sydney
18. Multi-party-computation (MPC) kryptografická metoda pro analýzu dat bez hrozby soukromí, ukládání dat v šifrované formě.	Amsterdam, Kodaň
19. Kontrola přenosu dat.	Kodaň
	Singapur
20. Klasifikace a třídění dat.	NYC
	Peking
21. Využití cloudové infrastruktury.	Chicago
	HKG, Peking
22. Testovací platformy.	Londýn, Amsterdam
23. Anonymizování dat.	NYC

Kyberbezpečnost a ochrana dat	Město
	Kodaň
24. Větší implementace opatření pro sofistikované kybernetické útoky.	Tokio
25. Aktualizace již platných opatření.	Toronto
	Singapur
26. Systém správy dokumentací zdravotnictví, zajištění ochrany a soukromí.	Tchaj-pej
27. Firewall, centrálně spravovaný firewall, automatická implementace kyberbezpečnosti.	Tchaj-pej
	Sydney
28. Neustálý vývoj systémů pro ochranu před kyberútoky.	Canberra

Souhrnná tabulka je rozdělena do 28 kategorií, ve kterých jsou přiřazená města podle toho, zda obsahují nějaké informace a zmínky ohledně dané kategorie. Tyto kategorie lze ještě rozřadit na kategorie, které jsou více aplikované (kategorie 1-7) a mnohem více měst je využívá napříč všemi kontinenty. Dále na méně časté kategorie, ve kterých je méně měst rozprostřených na 2 až 3 kontinenty, sem lze zařadit kategorie 8-16. Poté zde jsou kategorie, které jsou obsaženy pouze v minimu měst, na 1 až 2 kontinentech. Tyto poslední kategorie (17-28) jsou zde uvedeny proto, že v rámci bezpečnosti a ochrany dat také hrají důležitou roli.

První kategorií je implementování IoT, jejich bezpečnostních plánů a řešení a zda řeší dané strategie, jak nakládat s daty z IoT. Toto v sobě zahrnuje 11 měst ze všech 4 kontinentů. Druhou kategorií jsou vládní systémy a aplikace pro občany, které shromažďují kontakty a informace, umožňují komunikaci mezi vládou a občany. S tímto jsou také spjaté online nástroje pro sběr a sdílení dat a jejich využití pro bezpečnostní prvky. Tyto vládní služby, aplikace a online nástroje má ve svých plánech zahrnuto mnoho měst, také ze všech 4 zkoumaných kontinentů. Třetí kategorií je digitální sledovací systém, který zpracovává údaje z kamer, zvuky, sledovací technologie a monitorovací technologie. Čtvrtou kategorií je transparentnost, sběr pouze potřebných dat, zahrnutí aspektu soukromí a omezení shromažďování osobních údajů. Tato kategorie je také obsažena ve strategiích měst na všech 4 kontinentech.

Mezi další kategorie, které jsou hojně využívané a zastoupené ve více městech patří pátá kategorie nastavení, vytvoření a implementovaní postupů a zásad pro ochranu osobních údajů. Dále sem spadá šestá kategorie o využití open dat a vytvoření odpovídajících standardů.

Poslední velmi často využívanou kategorií je vytvoření entity, která spravuje kyberbezpečnost a ochranu dat.

Následují kategorie, které jsou již méně zastoupené anebo nebyly nalezeny u měst na všech kontinentech. Do této oblasti je zařazeno 8 kategorií. Mezi tyto kategorie tedy spadá vytvoření a využití projektů vyhodnocení připravenosti kybernetické bezpečnosti a monitorování rizikových přístupů. Další kategorií je využití nových metod a technologií pro shromažďování, analyzování a publikování dat. Další města pak vypracovávají strategie a projekty kybernetické bezpečnosti a datové strategie. Kategorie, do které spadá využití umělé inteligence, big dat nebo tvorba datových platforem, na kterých jsou daná data následně dostupná, včetně metod pro jejich analýzu, zpravidla s využitím umělé inteligence a strojového učení, obsahuje 7 měst, a to především v Asii. Důraz na integritu dat obsahují strategie čtyř měst. Sdílené služby pro IT po městě, standardizace IT postupů, vývoj IT, využití open-source pro IT je další kategorií. Čtrnáctou kategorií je kontrola přístupu osob k datům. Posledními kategoriemi, které lze nalézt u více Smart Cities, je zaměření na školení a vzdělávání zaměstnanců a občanů v oblasti kyberbezpečnosti a nábor IT odborníků. Druhou je „Jedna síť" – jednotný přístup vládních služeb a spolupráce vládních a veřejných služeb napříč městem.

Poslední část kategorií jsou kategorie, které jsou velmi málo využívané, resp. v daném vzorku měst byly nalezeny méně často, nebo je obsahují pouze jednotlivá města. Nicméně i přesto to mohou být důležité bezpečnostní prvky, které Smart Cities mohou aplikovat. Mezi takovéto kategorie spadá Privacy-By-design, Security-by-design přístup, které využívají města Toronto a Sydney. Další kategorií jsou kryptografické metody a šifrování dat, které jsou obsaženy v dokumentech Amsterdamu a Kodaně. Kontrolu přenosu dat využívají v Kodani a Singapuru. Klasifikace a třídění dat využívá NYC a Peking. Další kategorie je využití cloudové infrastruktury, které využívají v Chicagu, HKGu a Pekingu. Kategorie anonymizování dat využívají v NYC a Kodani. Testovací platformy lze nalézt v Londýně a Amsterdamu. Aktualizace již platných opatření je součástí plánů v Torontu a Singapuru. Systém správy dokumentací zdravotnictví, zajištění ochrany a soukromí má Tchaj-pej. Firewall, centrálně spravovaný firewall a automatická implementace kyberbezpečnosti byla nalezena pro Tchaj-pej a Sydney. Neustálý vývoj systémů pro ochranu před kyberútoky preferuje Canberra.

3.5 VYHODNOCENÍ VÝSLEDKŮ PRO SMART CITY KOMPONENTY

Tato kapitola obsahuje vyhodnocení strategií, plánů a různých projektů pro komponenty Smart City, které jsou zmíněné v kapitole 1.3.1. Mezi tyto komponenty patří Smart Economy neboli

konkurenceschopnost, inovace, podnikání, ekonomická image, ochranné známky, produktivita, mezinárodní začlenění a schopnost transformace. Prvek Smart People, jinak řečeno také sociální kapitál, je složen z kvalifikace, celoživotního učení, flexibility, tvořivosti, otevřenosti a veřejného života. Smart Governance pak obsahuje rozhodování, veřejné a sociální služby, transparentní řízení a politiku. Smart Mobilita je doprava a ICT, zahrnuje dostupnost, ICT infrastrukturu nebo dopravní systémy. Do Smart Environment patří znečištění, přírodní podmínky, ochranu prostředí a řízení zdrojů. Smart Living zahrnuje kulturu, zdravotnictví, kvalitu bydlení, vzdělávání a turistiku (Giffinger a Gudrun, 2010).

Ve zdrojových dokumentech a webech byly dále hledány informace ohledně dat, jejich využití, zabezpečení a kybernetické bezpečnosti, které jsou následně sumarizovány v Tabulce 7. Tato tabulka vychází z Příloh VI, VII, VIII, IX, X a XI, ve kterých jsou zobrazeny nalezené a zapsané informace ohledně komponent Smart City pro vybraná města.

Tabulka 7: Sumarizační tabulka pro komponenty Smart City. Zdroj: vlastní.

Kyberbezpečnost a ochrana dat	Komponenta	Město
1. Publikování dat, transparentnost, otevřenost dat, sdílení dat s veřejností, výzkumnými středisky, experty, IT podniky, partnery, a univerzitami.	Economy	NYC
		Paříž, Kodaň, Praha
		Tokio, Peking Soul, HKG
	People	SF, Toronto
		Paříž, Amsterdam
		Tokio, Peking
		Canberra
	Governance	Amsterdam, Kodaň
		Tokio, Soul, HKG, Peking
		Sydney, Canberra, Melbourne, Wellington
	Mobility	Chicago, LA
		Kodaň
		Singapur, HKG
		Sydney, Melbourne
	Environment	Londýn
		Soul, HKG
	Living	Chicago, SF

Kyberbezpečnost a ochrana dat	Komponenta	Město
2. Datové platformy, platformy pro analýzy, simulace s daty, platformy na ukládání a archivaci dat. Big data a open data přístupy.	Economy	Washington, SF, LA
		Praha
		Soul, Singapur
		Sydney, Melbourne, Wellington
	Governance	Tchaj-pej
	Mobility	Chicago, SF
		Londýn, Berlín, Amsterdam
		Tchaj-pej
	Environment	Washington, LA
		Paříž, Kodaň
		Singapur, HKG, Tchaj-pej
	Living	LA
		Paříž, Berlín
		Singapur
		Sydney
3. Data z digitálních technologií a IoT, jejich získávání, správa, analýza a další využití v Smart City.	Economy	LA
		Singapur
		Sydney
	People	Paříž
		Sydney
	Environment	NYC, Toronto
		Praha
		Singapur
		Melbourne, Canberra
	Living	NYC
		Londýn, Paříž
		Tokio, Singapur, Tchaj-pej, Peking
		Canberra
4. Vytvoření zásad, standardů, postupů, rámců, plánů nebo zákonů pro zacházení s daty, ochranou dat nebo kyberbezpečnost.	Economy	Washington, Chicago, Toronto
		Amsterdam
		Singapur
		Sydney, Wellington

Kyberbezpečnost a ochrana dat	Komponenta	Město
	People	Washington
		Berlín
	Governance	NYC, SF, Chicago, Washington, Toronto
		Londýn, Paříž, Berlín, Praha
		Tokio, Singapur, Peking
		Sydney
	Mobility	NYC
	Environment	Chicago
		Soul
5. Zřízení programů a agentur pro kybernetickou bezpečnost a odvětvové týmy.	Economy	NYC
		Paříž, Amsterdam
		Singapur, Soul, Peking
	Governance	NYC
		Soul
	Living	NYC
		Singapur
6. Využití technologické a technické infrastruktury, datových center pro zajištění ochrany dat a soukromí. Využití nových technologií a přístupů.	People	Washington, SF, Toronto
		Londýn, Kodaň, Praha
		Tokio, Singapur, Soul
		Sydney, Wellington
	Governance	Chicago, LA
		Kodaň, Praha
		Soul
		Wellington
	Living	Soul, HKG
7. Využití, přenos a uplatnění real-time dat a informací pro fungování městských prvků a částí s důrazem na jejich zabezpečení a ochranu.	Governance	Tokio
		Canberra
	Mobility	NYC, Washington
		Paříž, Amsterdam, Kodaň, Praha
		Singapur, Soul, HKG
		Canberra

Kyberbezpečnost a ochrana dat	Komponenta	Město
	Environment	Praha
		HKG, Peking
	Living	Soul
8. Poskytnutí datové gramotnosti, vzdělávání, školení, online nástroje pro občany a zaměstnance. Poskytování cílených znalostí a datových služeb v rámci ochrany dat a kyberbezpečnosti.	Economy	Soul, Singapur
	People	NYC
		Amsterdam, Kodaň
		Soul, Singapur, HKG, Tchaj-pej
	Governance	NYC
		Amsterdam, Kodaň
		Tokio, Soul, HKG, Peking
		Sydney, Melbourne, Canberra, Wellington
9. Anonymizace dat.	Mobility	NYC, Toronto
		Singapur
	Environment	Londýn, Kodaň
	People	Soul
10. Aktivní sběr informací o občanech – rasa, věk, pohlaví, vzdělání atd. S tímto souvisí projekty na větší kontrolu těchto dat a lepší správu takto získaných dat.	People	Washington
		Amsterdam, Kodaň
		Tokio, Peking
		Melbourne, Canberra
	Living	Washington
		Paříž, Kodaň, Praha
11. Pracovní pozice v oblasti ochrany dat a soukromí.	Governance	NYC
12. Automatizovaný kanál publikací, zohledňuje soukromí a bezpečnost.	Governance	Toronto
13. Ochrana dat, které využívají autonomní a propojená vozidla.	Mobility	Washington
		Peking

Tato sumarizační tabulka zobrazuje několik zevšeobecněných kategorií kyberbezpečnostních prvků a ochrany dat nebo soukromí. Toto je vzhledem k ochraně občanů, kteří Smart City prvky využívají a také vzhledem k ochraně samostatného projektu Smart City. Tabulka obsahuje 13 kategorií, ke kterým jsou přiřazeny komponenty spolu s městy, které tyto kategorie obsahují.

Lze říci, že prvních 9 kategorií je více všeobecných a lze je uplatnit ve všech komponentách Smart City, zatímco zbylé 4 kategorie jsou více specifické pro vybrané komponenty Smart City.

První kategorií je publikování dat, jejich transparentnost a otevřenost, sdílení s veřejností, výzkumnými středisky, experty, IT podniky, partnery a univerzitami. Oblasti Economy, People, Governance a Mobility nejvíce využívají této kategorie. V oblasti Smart Economy lze nalézt zmínky o městech jako je NYC, Paříž, Kodaň, Praha, Tokio, Peking, Soul nebo HKG. Města SF, Toronto, Paříž, Amsterdam, Tokio, Peking a Canberra jsou města z oblasti Smart People. Dále ze Smart Governance toto využívají města jako je Amsterdam, Kodaň, Tokio, Soul, HKG, Peking, Sydney, Canberra, Melbourne a Wellington. V oblasti Mobility lze nalézt města ze všech kontinentů, města jako je Chicago, LA, Kodaň, Singapur, HKG, Sydney a Melbourne. V oblasti Environemntu pouze nalezneme Londýn, Soul a Melbourne. Chicago a SF využívají toto u Smart Living.

Druhou kategorií je využití datové platformy, platformy pro analýzy, simulace s daty, platformy na ukládání a archivaci dat, big data a open data přístupy, které pracují s velkým množstvím všech různých typů dat a je tedy potřebné dbát jejich ochrany a zabezpečení. Oblasti pro tuto kategorii jsou Economy, Governance, Mobility, Environment a Living. V rámci Economy se jedná o města Washington, SF, LA, Praha, Soul, Singapur, Sydney, Melbourne a Wellington. Oblast Mobility nalezneme ve městech Chicago, SF, Londýn, Berlín, Amsterdam, Tchaj-pej. V rámci Smart Environemnt tuto kategorii zmiňují Washington, LA, Paříž, Kodaň, Singapur, HKG a Tchaj-pej. Jediná Tchaj-pej využívá toto v rámci Governance. Platformy také nalezneme u oblasti Smart Living, zde se jedná o města LA, Paříž, Berlín, Singapur a Sydney.

Třetí kategorií jsou data z digitálních technologií a IoT, jejich získávání, správa, analýza a další využití v Smart City. Kde tuto kategorii v rámci Economy zmiňuje LA, Singapur a Sydney. V rámci People se jedná o Paříž a Sydney. Dalšími oblastmi jsou Environment, kde se jedná o NYC, Toronto, Prahu, Singapur, Melbourne a Canberru, a dále oblast Living, kde je znovu NYC, Londýn, Paříž, Tokio, Singapur, Tchaj-pej, Peking a Canberru.

Čtvrtou kategorií je tvorba zásad, standardů, postupů, rámců, plánů nebo zákonů pro zacházení s daty, ochranou dat nebo kyberbezpečnost. Zde mluvíme o pěti oblastech a to Economy, People, Governance, Mobility a Environment. U Smart Economy jsou města Washington, Chicago, Toronto, Amsterdam, Singapur, Sydney a Wellington. Washington a Berlín toto využívá v rámci Smart People. V rámci Smart Governance je patrné, že zásady, postupy, standardy a další jsou využívány nejvíce. Zde se jedná o města jako je NYC, SF, Chicago,

Washington, Toronto, Londýn, Paříž, Berlín, Praha, Tokio, Singapur, Peking a Sydney. V rámci Mobility zde je pouze NYC. Dále města Chicago a Soul mají vytvořené zásady, standardy a další pro oblast Smart Environment.

Pátou kategorií je zřízené programů a agentur pro kybernetickou bezpečnost a odvětvové týmy. Zde se jedná pouze o Economy, která lze tuto kategorii nalézt nejčastěji, Governance a Living. V rámci všech tří lze nalézt NYC. Dále se v Economy jedná o Paříž, Amsterdam, Singapur, Soul a Peking. Soul nalezneme v rámci Governance a Singapur v rámci Living. Šestou kategorií je využití technologické a technické infrastruktury, datových center pro zajištění ochrany dat a soukromí. Využití nových technologií a přístupů. Zde je vidět veliký zájem měst v rámci oblasti People, kde nalezneme města Washington, SF, Toronto, Londýn, Kodaň, Praha, Tokio, Singapur, Soul, Sydney a Wellington. Další oblastí je Governance, zde se jedná o města Chicago, LA, Kodaň, Praha, Soul a Wellington. Města Soul a HKG toto využívají v rámci oblasti Smart Living.

Sedmou kategorií je využití, přenos a uplatnění real-time data a informací pro fungování městských prvků a částí s důrazem na jejich zabezpečení a ochranu. Tuto kategorii nalezneme ve čtyřech oblastech Smart City. Těmito oblastmi jsou Governance s městy Tokio a Canberra, Environment s městy Praha, HKG, Peking, oblast Smart Living a město Soul. Nejvíce nalezneme využití real-time dat a jejich správu v oblasti Mobility. Zde se jedná o města NYC, Washington, Paříž, Amsterdam, Kodaň, Praha, Singapur, Soul, HKG a Canberra.

Osmou kategorií je poskytnutí datové gramotnosti, vzdělávání, školení, využití online nástrojů pro občany a zaměstnance městské infrastruktury. Dále sem patří nabídka cílených znalostí a datových služeb v rámci ochrany dat a kyberbezpečnosti. Toto poskytují, v rámci Smart Economy, města Soul a Singapur. V rámci People lze toto nalézt ve městech NYC, Amsterdam, Kodaň, Soul, Singapur, HKG a Tchaj-pej. Nejvíce se tedy vzdělávání o ochraně dat a kyberbezpečnosti využívá v rámci Smart Governance komponenty měst NYC, Amsterdam, Kodaň, Tokio, Soul, HKG, Peking, Sydney, Melbourne, Canberra a Wellington. Poslední devátou více všeobecnou kategorií je anonymizace dat. Tu lze nalézt v oblasti Mobility ve městech NYC, Toronto a Singapur. Ve Smart Environment toto aplikují města Londýn a Kodaň. Město Soul toto aplikuje v oblasti Smart People.

Následující kategorie jsou spíše více zaměřené na jednotlivé komponenty a oblasti Smart City. Desátou kategorií je tedy aktivní sběr informací o občanech. S tímto souvisí projekty na větší kontrolu těchto dat a lepší správu takto získaných dat. Zde se jedná pouze o komponenty Smart

People a Smart Living. Města v oblasti Smart People jsou Washington, Amsterdam, Kodaň, Tokio, Peking, Melbourne a Canberra. V oblasti Living jsou to města Washington, Paříž, Kodaň a Praha. Jedenáctou kategorií je tvorba pracovních pozicí v oblasti ochrany dat a soukromí. Toto zmiňuje pouze město NYC v oblasti Smart Governance. Dvanáctou kategorií je vytvoření automatizovaného kanálu publikací, který zohledňuje soukromí a bezpečnost. Zde se znovu jedná o oblast Smart Governance a město Toronto. Poslední vytvořenou kategorií je ochrana dat, kterou využívají autonomní a propojená vozidla. V tomto případě je jasné, že se jedná o specifickou kategorii pro komponentu Smart Mobility, kterou lze nalézt pro města Washington a Peking.

Z této souhrnné tabulky lze říci, že komponenty, které nejvíce dbají a využívají ochrany dat a kyberbezpečnosti jsou Smart Economy a Smart Governance, jelikož lze nalézt největší počet těchto komponent pro více kategorií, a existuje i nejvíce měst v těchto komponentách. Také je zde patrné že v rámci komponenty Smart Economy je kladen velký důraz měst na vytvoření datových platforem, platforem pro analýzy, simulace, ukládání a archivaci dat, big dat a open dat společně s vytvořením zásad, standardů, rámců a zákonů na ochranu dat a kyberbezpečnost. V rámci Smart Governance se znova nejvíce vyskytuje tvorba zásad, standardů, rámců a zákonů na ochranu dat a kyberbezpečnost. Dále se hodně měst věnuje problematice datové gramotnosti, vzdělávání, školení, a souvisejícím online nástrojům pro občany a zaměstnance, kde lze tyto služby poskytovat, např. ve formě e-learningu. Poskytování cílených znalostí a datových služeb v rámci ochrany dat a kyberbezpečnosti je další ze směrů v této kategorii.

Mezi velmi málo zastoupené komponenty patří Smart Living a Smart Environment. Zde je vidět že na tyto komponenty není kladen takový důraz pro zabezpečení dat a kyberbezpečnost. V rámci prvních 9 všeobecných kategorií je patrné, že v komponentech Smart Economy jsou nejvíce aktivními městy Soul a Singapur, které využívají 4 z 9 kategorií. Co se týče kontinentu, tak zde je vidět celkově 11 záznamů využití pro Asii v různých městech a v různých kategoriích ochrany dat a kyberbezpečnosti. Severní Amerika má 9 záznamů, Evropa 6 a Oceánie pouze 4.

V komponentě Smart People využívá nejvíce bezpečnostních prvků Soul a Sydney, které využívají 3 z 9 kategorií. Nejaktivnějšími kontinenty jsou zde Evropa a Asie s 10 různými výskyty v rámci Smart People. Je také vidět že velmi aktivní je Oceánie, která má 8 výskytů, což je v rámci jejich 4 porovnávaných měst vysoké číslo. Severní Amerika má pak pouze 7 záznamů. Zabezpečení a kyberbezpečnost ve Smart Governance využívají 3 z 9 kategorií města Tokio, Soul, Singapur, Sydney a Wellington. Z tohoto je tedy patrné, že nejaktivnějším

kontinentem v rámci Governance je Asie s 13 výskyty v těchto 9 kategoriích. Velmi aktivní je i Oceánie s 9 výskyty. Jak Severní Amerika, tak Evropa mají 8 záznamů.

Co se týká Smart Mobility, tak nejvíce zabezpečení pro tuto komponentu využívá NYC, které má 3 z 9 kategorií. Celkově je zde více patrný úpadek bezpečnostních prvků oproti prvním třem smart komponentám. Nejvíce aktivní kontinent je Severní Amerika s 9 záznamy v rámci Smart Mobility, v Evropě 8 záznamů, v Asii 6 záznamů a Oceánie s 3 záznamy. Komponenta Smart Environment je znovu nejvíce využívaná v rámci Asie, kde je 9 záznamů oproti 7 evropským, 5 americkým a 2 záznamům z Oceánie. Nejvíce proaktivním městem je zde HKG, který využívá 3 z 9 kategorií. Smart Living je komponenta, kterou nejvíce využívá město Singapur, které využívá 3 z 9 kategorií. Nejvíce výskytů se zaměřením na ochranu dat a kyberbezpečnost této komponenty lze nalézt v Asii s 8 záznamy, Evropa má pouze 4 záznamy, Severní Amerika 5 záznamů a Oceánie 2 záznamy.

4 NÁVRH DOPORUČENÍ PRO DANOU PROBLEMATIKU

Poslední kapitola této práce je zaměřená na ověření výsledků představených v přechozí kapitole 3 a jejich formulaci do podoby doporučení pro kyberbezpečnost a ochranu dat ve Smart Cities, na kterých se shodli vybraní experti. Jedná se tedy o vytvoření doporučení a návrhů pro ochranu dat a kyberbezpečnost, které by se měly využívat a je možné je brát jako základní stavební kámen, na kterých by měly Smart City projekty stavět a rozvíjet ochranu a kyberbezpečnost pro svoje specifické problémy. Pro ověření doporučení je využita metoda Delphi, která je založena na hledání shody mezi experty ohledně předloženého seznamu doporučení, který byl vytvořen na základě zjištění v předchozí kapitole 3. V této práci musela pro získání shody proběhnout tři kola metody Delphi.

4.1 OVĚŘENÍ POMOC METODY DELPHI

Při provádění Delphi metody v této diplomové práci je stanoven autor práce jako jedinec, který provádí tuto metodu, tedy je řídící osoba pro metodu Delphi. Vybírá seznam vhodných expertů pro téma kyberbezpečnosti a ochrany dat tak, aby experti měli kvalifikaci v této oblasti. Dále formuluje pokyny pro experty, nastavuje a kontroluje termíny, vytváří dotazníky pro jednotlivá kola, rozesílá je, zpracovává a analyzuje výsledky a rozhoduje o tom, které změny budou do seznamu doporučení zapracovány. Nakonec vytváří finální verzi doporučení, která je ve shodě s experty v metodě Delphi.

4.1.1 Metoda Delphi

Metoda Delphi je založena na porovnání a konfrontaci různých nápadů a názorů nebo vytvoření vhodných informací pro rozhodovací procesy. Základem této metody je strukturovaný proces sběru a zhušťování nebo shrnutí velkého množství dat od skupiny odborníků (expertů). Tohoto je dosahováno sérií dotazníků, které jsou proložené řízenou zpětnou vazbou. Lze říci, že se jedná o řízenou komunikaci mezi skupinou expertů a usnadňuje tvorbu skupinového úsudku (Crisp et al., 1997). Wissema tuto metodu označuje jako techniku průzkumu s proměnnou pro technologické odpovědi. Metoda vznikla pro možnost komunikace a diskuse mezi odborníky bez sociálně interaktivního chování, což je běžné při skupinové diskusi, ale zabraňuje to tvorbě názorů (Wissema, 1982).

Metodu Delphi lze rozdělit do deseti hlavních kroků, které lze ale případně dále rozvíjet a navazovat na ně dalšími rozšířeními. Příkladem může být rozšíření o další dotazníková kola.

Prvním krokem je stanovení týmu (řídící osoby), který bude danou metodu Delphi provádět. Druhým krokem je výběr expertů v dané oblasti Delphi metody. Následuje třetí krok, kterým je vytvoření prvního kola dotazníku. Dále je potřeba zkontrolovat dotazník, zda jsou otázky správně položené. Pátým krokem je předložení dotazníku expertům pro jeho vyplnění. Šestým krokem je provedení analýzy odpovědí prvního kola dotazníku. Sedmým krokem je vytvoření dotazníku pro druhé kolo. Osmým krokem je předání druhého kola dotazníku expertům. Deváté kolo je znovu analýza odpovědí druhého kola. Posledním krokem je příprava závěrů ze všech provedených kol (Crisp et al., 1997).

Silné stránky této metody jsou: vyhnout se přímým konfrontacím mezi experty, spojení znalostí a shody/neshody, nejsou potřebná osobní setkání, umožňuje anonymitu a tím pádem větší kreativitu a snižuje rizika skupinové dynamiky, získáním odpovědí od expertů dochází k obohacení vlastních znalostí, odborníci přispívají k pochopení a řešení důležitých problémů, ověřitelnost, srozumitelnost a celistvost, poskytuje celistvý náhled jelikož dochází k využití jak kvalitativní, tak kvantitativních metod, šetří peníze a čas (Fink-Hafner et al., 2019). Slabé stránky jsou: nedostatek pokynů a dohodnutých standardů, jak implementovat a analyzovat výsledky, všeobecně uznávané definice konsensu, výběr účastníků, možnost odstoupení účastníků, možná finanční odměna za účast v této metodice může mít vliv na výsledky, jakožto je anonymita silná stránka, tak i svým způsobem je slabou stránkou, obtížnost zobecnění výsledků, může dojít k nerovnoměrnému rozložení odborných znalostí mezi účastníky (Fink-Hafner et al., 2019).

4.1.2 Experti a jejich popis

Potřebným krokem při využití metody Delphi je výběr expertů. Odbornost vybraných expertů by měla korespondovat s tématem, na které předkládají své názory a hodnotí vybrané kategorie a doporučení v rámci ochrany dat a kyberbezpečnosti ve Smart City projektech. Celkem bylo osloveno sedm expertů, když všichni po seznámení s požadavky a postupem realizace metody Delphi souhlasili s účastí. Všichni experti jsou z Evropy, když dva jsou z ČR, další jsou ze sousedních zemí, a jeden expert je ze Švýcarska. Průměrná délka praxe v oboru je 15 let s tím, že rozsah je od 3 let až do 25 let.

Seznam zapojených expertů je zobrazen v Tabulce 8, která obsahuje informace o zemi, ze které experti pochází, popis pracovní pozice, délku praxe a profesní odbornost, která popisuje náplň jejich práce a odborné znalosti. Většina expertů má znalosti z oblasti informatiky, informačních a bezpečnostních systémů, HW a SW řešení, a veřejného sektoru (Smart Cities).

Tabulka 8: Seznam a charakteristika expertů v metodě Delphi. Zdroj: vlastní.

Č.	Země	Pracovní pozice	Délka praxe	Profesní odbornost
1.	ČR	Odborný asistent, datový analytik, e-government konzultant	15 let	Expert má dlouholeté zkušenosti v oblastech e-governmentu, big a open linked dat, bezpečnosti dat, datové analytiky a analýzy dopadů moderních technologií ve veřejném sektoru.
2.	Německo	Německý vládní zaměstnanec (pod státem)	12 let	PhD v oboru informatika, 4 roky zaměstnán na univerzitě jako výzkumný pracovník – výzkum informačních systémů, 8 let praxe jako systémový analytik a designér ve veřejném sektoru.
3.	Rakousko	Profesor, projektový manažer	25 let	Informatika, Informační systémy, Datové modelování a témata projektového řízení se zaměřením na datové modelování a řízení. Odborník má bohaté zkušenosti s řízením projektů veřejného sektoru.
4.	Polsko	Výzkumník	5 let	Výzkumník v oblasti informatiky, informačních systémů a e-governmentu se zaměřením na Smart Cities/villages/regions.
5.	Slovensko	IT konzultant a datový specialista	20+ let	Expert má více než 20 let zkušeností v oblasti informačních systémů, webových aplikací a dalších HW a SW řešení se zaměřením na datové požadavky, výměnu dat a hodnocení bezpečnosti. Podílel se na projektech soukromého i veřejného sektoru.
6.	Švýcarsko	PhD student	3 roky	Smart City a e-government.
7.	ČR	Odborný asistent	25 let	ICT systémy, počítačové sítě.

4.1.3 První kolo metody Delphi

První kolo začíná vytvořením první verze dotazníku. Dotazník je složen ze dvou částí. První část popisuje, na jaké téma je dotazník zaměřen, a jak dotazník vyplnit, tzn., že nejdříve dojde k ohodnocení významu jednotlivých doporučení a poté musí experti zhodnotit úplnost seznamu doporučení. Tato část také obsahuje upozornění na dvě otevřené otázky, a to jednu zaměřenou na to, zda je nutné ze seznamu doporučení něco odstranit, a druhou týkající se návrhu nových doporučení, které v seznamu podle experta chybí.

Hlavní část dotazníku se skládá z vytvořených kategorií a jednotlivých doporučení v rámci kyberbezpečnosti a ochrany dat. Pro toto kolo jsou doporučení strukturována do 6 kategorií a 33 podkategorií neboli prvků těchto kategorií. Ty byly vytvořeny z existujících doporučení v rámci Smart City indexů a rámců a zejména dokumentů analyzovaných v kapitole 3. Došlo tedy k jejich sumarizaci a využití metody Delphi pro jejich ověření a přesnější specifikaci. Ohodnocení všech doporučení je realizováno pomocí čtyřstupňové Likertovy škály – *High*, *Moderate*, *Low*, *None* neboli *Vysoká, Střední, Nízká, Žádná*. Tuto škálu lze bodově rozdělit od 0 do 3, tedy *High* je 3, *Moderate* je 2, *Low* je 1 a *None* je 0. Experti na konci dotazníku rovněž vyplňují, jak moc souhlasí s vytvořenými doporučeními, a to škálou pro hodnocení 0 až 5, tedy *Strongly agree* je 5, *Agree* je 4, *Slightly agree* je 3, *Slightly disagree* je 2, *Disagree* je 1, a *Strongly disagree* je 0. Mají i možnost se slovně vyjádřit k danému tématu prostřednictvím dvou otázek. První zjišťuje, zda by odstranili nějakou kategorii nebo konkrétní doporučení. Druhá se zaměřuje na to, zda jim v seznamu doporučení něco schází.

Druhým krokem v prvním kole bylo rozeslání vytvořeného dotazníku všem expertům. Experti měli na jeho vyplnění 14 dní. Všech sedm dotazníků se vrátilo zpět a všechny byly správně vyplněné. Mohly být tedy dále zpracovány a analyzovány. Výsledky prvního kola ukazují, že se experti shodují na tom, že nejméně důležitou kategorií je využití dat pro ochranu. Tato kategorie má průměrné hodnocení 2, což odpovídá hodnocení střední důležitost. Všechny ostatní kategorie mají průměrné hodnocení vyšší jak 2,3. Nejlépe hodnocenou kategorií jsou lidské zdroje, které jsou průměrně ohodnocené 3, neboli vysoce důležité.

Co se týká doporučení v rámci vytvořených kategorií, tak nejméně důležitým podle průměrů hodnocení všech expertů je *„Minimalizace stahování dat do koncových zařízení“*, které získalo průměrné hodnocení 1,86. Dalšími doporučeními s nízkým hodnocením jsou *„Bezpečnostní požadavky na SW a jeho vývojový cyklus“*, *„Použití nástrojů pro detekci aktivity“*, *„Částečné skrytí celých dat po odfiltrování omezení dopadů“*, *„Analýza dat a hluboké učení týkající se potřeb projektů Smart City*“. Všechny tyto prvky mají průměrné hodnocení 2. Nejvyšší důležitost kladou experti na *„Implementace přísných zákonů a zásad na ochranu soukromí na ochranu citlivých dat“*, *„Vzdělávání a školení uživatelů o kyberbezpečnosti a ochraně dat“*. Tyto dvě doporučení mají průměrné hodnocení 3, tedy jsou vysoce důležité.

Průměrné hodnocení úplnosti seznamu doporučení v prvním kole je 4,14 (maximum je 5), tedy experti s vytvořenými kategoriemi a doporučení souhlasí. Výsledky hodnocení z prvního kola lze nalézt v Příloze XII.

4.1.4 Druhé kolo metody Delphi

Pro druhé kolo byl vytvořen upravený dotazník, který reflektoval hodnocení a připomínky expertů z prvního kola. V první části dotazníku byla přesněji specifikována opatření a prostředí modelového Smart City, pro které jsou tato opatření navržena, aby mohli experti lépe ohodnotit dané doporučení v navrženém kontextu.

V hlavní části dotazníku byly provedeny následující změny. Pro kategorii *„HW a SW řešení“* došlo k úpravě doporučení zaměřeného na bezpečnost SW, jelikož města zpravidla nevyvíjí vlastní SW, ale spíše podporují a financují projekty zaměřené na občany, které pak vedou k vytvoření nějaké aplikace nebo systému. Proto došlo k úpravě tohoto doporučení a vzniklo doporučení „*Mít vytvořené bezpečnostní požadavky na SW, blacklisting a deny-by-exception pro neautorizovaný SW*“. Také bylo upřesněno doporučení zaměřené na biometrické systémy na *„Využití biometrických systémů pro přístup do vymezených částí budov, například administrativa, serverovny a další“*. Dalším upřesněním je doporučení *„Využití nástrojů detekce aktivit v kyberprostoru, např. IDS nebo Security Information and Event Management (SIEM), …“*. Dále došlo k vytvoření nového doporučení v kategorii *„Organizačních řešení“*, které zohledňuje to, že města mají přístupné informace a doporučení ohledně kyberbezpečnosti a ochrany dat na webu tak, aby je občané a další uživatelé mohli najít. Dále bylo vytvořeno nové doporučení pro zhodnocení toho, jak je město připravené implementovat nová kybernetická opatření a ochranu dat, které se nazývá *„Analýza připravenosti a současného stavu města vzhledem k financím a lidským zdrojům potřebným pro implementaci nových kybernetických opatření a ochraně dat“*.

V kategorii *„Zásady ochrany dat“* došlo k vytvoření nového doporučení, které se zabývá vytvořením zásad pro správu dat po skončení jejich životného cyklu. To se nazývá *„Vytvoření zásad a politik pro odstranění dat po skončení jejich životního cyklu“*. Dále došlo k odstranění doporučení *„Minimalizace stahování dat do koncových zařízení“*, jelikož mělo nejmenší průměrné hodnocení od expertů. V této kategorii bylo na doporučení expertů vytvořeno ještě jedno nové doporučení zabývající se využitím rámců a standardů Národního institutu standardů a technologie (NIST) a Mezinárodní organizace pro normalizaci (International Organization for Standardization, ISO). Po více připomínkách expertů došlo k přesunu tří prvků z kategorie *„Organizační řešení“* do kategorie *„Zásady ochrany dat“*.

V kategorii *„Ochrany dat během přenosu a ukládání“* došlo k nahrazení doporučení *„Částečné skrytí celých dat po odfiltrování omezení dopadů“* za doporučení *„Využití data loss prevention*

(DLP)“, jelikož původní doporučení patřilo k těm, které měly nízké průměrné hodnocení. DLP v sobě částečně zahrnuje i předchozí doporučení, který nahrazuje. V kategorii *„Lidských zdrojů“* došlo k úpravě a rozdělení doporučení řešícího *„Vzdělávání a školení uživatelů o kyberbezpečnosti a ochraně dat“*. Došlo tak ke vzniku dvou nových doporučení, jelikož vzdělávání se bude lišit vzhledem k tomu, zda se jedná o zaměstnance města, kteří s daty pracují nebo se bude jednat o občany města, kteří sdílí data prostřednictvím nějakých služeb nebo aplikací. Vznikla tedy dvě doporučení: „*Vzdělávání a školení zaměstnanců města ohledně kyberbezpečnosti a ochraně dat“* a *„Vzdělávání a školení občanů a dalších subjektů ohledně kyberbezpečnosti a ochraně dat“*. Nakonec bylo blíže specifikováno doporučení *„Vytvoření dedikované kybernetické entity – týmu, velikost týmu dle velikosti města“*.

V rámci kategorie *„Využití dat pro ochranu“* došlo k upřesnění kategorie, tedy *„Využití existujících dat pro další ochranu“*. V této kategorii došlo k bližší specifikaci doporučení ohledně datové analýzy, hlubokého a strojového učení na *„Datová analýza, hluboké a strojové učení ohledně potřeb bezpečnosti Smart City, například detekce anomálií v síťovém provozu, detekce malwaru nebo monitorování zabezpečení IoT, …“*. Dále podle návrhů expertů došlo k vytvoření nových doporučení pro tuto kategorii, a to: *„Využití generativní AI, například užití chatbotů, kteří využívají data pro řešení bezpečnostních situací“* a *„Reakce na incidenty, tedy využití starých existujících dat o bezpečnostních incidentech, výběr možných oblastí útoku, zpřesnění reakce na incidenty atd“*.

Jelikož cílem práce je vytvoření doporučení, která zajišťují ochranu dat, kyberbezpečnost nebo bezpečnost, nebyl brán v potaz jeden bod experta, který poukazoval, že u aplikace kamer nebo přístupu pomocí automatické registrace návštěvníků mohou nastat etické otázky ohledně takto získávaných dat. Další připomínkou, která nebyla brána v potaz, je reformulace všech tvrzení, aby bylo zřejmé, pro jakou fázi je dané doporučení vhodné. Tzn., zda se jedná pouze o návrh, zda je to návrh s konkrétními požadavky, doporučení je již implementováno, ale musí být vylepšeno nebo již existuje HW, SW a infrastruktura, která se následně pro implementaci doporučení využije apod. Jelikož se jedná o všeobecná doporučení pro všechny Smart City projekty, ať již existující nebo teprve vznikající, nelze z tohoto důvodu přesně vymezit, kdy se daná doporučení mají aplikovat a v jakých požadavcích.

Takto upravený dotazník byl opět rozeslán všem expertům, kteří měli jeden týden na jeho vyplnění a poslání zpět. Jelikož na základě zpracování výsledků z tohoto druhého kola experti navrhovali už pouze změny týkající se znění jednotlivých doporučení, ale už dále neplánovali

upravovat svoje hodnocení, tak jsou hodnoty významů jednotlivých kategorií a doporučení prezentovány v následující kapitole.

4.1.5 Třetí kolo metody Delphi

Pro třetí kolo dotazníku již tedy došlo pouze k úpravě znění doporučení podle připomínek expertů z druhého kola. Došlo tedy k bližší specifikaci v rámci kategorie *„HW a SW řešení“*, kde ke každému doporučení bylo doplněno, zda se jedná o HW, SW anebo HW/SW řešení, tedy zda obsahuje pouze HW, pouze SW anebo je to kombinace obojího. Dále byla blíže specifikována doporučení v kategoriích *„Zásady ochrany dat*“, *„Lidský zdroje“*, *„Využití dat pro ochranu“*. Následně byl nově upravený dotazník rozeslán expertům, kteří byli požádáni o vyjádření konečného souhlasu a shodu na seznamu doporučení pro danou problematiku. Na třetí kolo byl vyhrazen opět týden, ale většina expertů se vyjádřila obratem. Všichni experti se shodli na konečném seznamu doporučení i jejich významu a nevznesli již žádné další nové připomínky, které by bylo nutné zapracovat.

Po získání vyplněných dotazníků tedy došlo ke konečnému zpracování výsledků, které jsou zobrazeny v Tabulce 9. U každého doporučení, resp. kategorie, jsou uvedeny odpovědi expertů na škále významu doporučení (*High* je 3, *Moderate* je 2, *Low* je 1 a *None* je 0) a průměrné hodnocení a směrodatná odchylka těchto odpovědí. Poslední řádek tabulky má pak škálu 0 až 5, aby experti mohli přesněji vyjádřit svůj celkový souhlas se seznamem doporučení.

Tabulka 9: Výsledky z třetího kola metody Delphi. Zdroj: vlastní.

SEZNAM DOPORUČENÍ	**Průměr**	**Směrodatná odchylka**	**Odpovědi expertů**						
			n. 1	**n. 2**	**n. 3**	**n. 4**	**n. 5**	**n. 6**	**n. 7**
HW A SW ŘEŠENÍ	**2,86**	**0,35**	3	3	3	2	3	3	3
[HW, SW] Nastavení dohledu a analýzy na místě – použití kamer s podporou analýzy, AI nebo rozpoznávání pohybu…	**2,57**	**0,49**	3	3	3	2	2	3	2
[HW, SW] Přístup do zařízení nebo částí budov pomocí automatických systémů registrace návštěvníků	**2,57**	**0,49**	3	2	3	2	3	3	2
[HW, SW] Použití nástrojů pro detekci aktivity v kyberprostoru, např. IDS, SIEM, …	**2,14**	**0,35**	3	2	2	2	2	2	2
[HW, SW] Vícefaktorová autentizace	**2,86**	**0,35**	3	3	3	2	3	3	3

	[SW] Nástroje ochrany e-mailů – vestavěné skenování e-mailů, phishing a ochrana zabezpečení internetu	**3,00**	**0,00**	3	3	3	3	3	3	3
	[SW] Mít bezpečnostní požadavky na SW, blacklist nebo deny-by-exception pro neautorizovaný SW atd.	**2,86**	**0,35**	2	3	3	3	3	3	3
	[HW, SW] Použití biometrických systémů pro přístup do definovaných částí budov, např. administrativa, serverovny apod.	**2,43**	**0,49**	2	2	2	2	3	3	3
ORGANIZAČNÍ ŘEŠENÍ		**2,57**	**0,49**	3	3	3	2	2	3	2
	Centralizované poskytování datové infrastruktury	**2,14**	**0,35**	3	2	2	2	2	2	2
	Zabezpečená komunikační síť na úrovni bezpečnostních složek krizového řízení	**2,29**	**0,45**	3	2	2	2	2	2	3
	Provádět pravidelné hodnocení rizik zabezpečení dat	**2,71**	**0,45**	3	3	3	2	3	3	2
	Kybernetická bezpečnost na vrcholu priorit (finanční zdroje, lidé, infrastruktura)	**2,71**	**0,45**	3	3	3	3	2	3	2
	Využití Privacy Impact Assessment při zavádění nových technologií	**2,29**	**0,45**	2	2	3	2	2	3	2
	Mít plán aktualizací aplikací, provádět je včas	**2,43**	**0,73**	3	3	3	2	2	3	1
	Nastavení požadavků na cloud a poskytovatele služeb	**2,14**	**0,35**	2	3	2	2	2	2	2
	Analýza připravenosti a současného stavu města z hlediska financí a lidských zdrojů na zavádění nových kybernetických opatření a ochrany dat	**2,86**	**0,35**	3	3	3	3	3	3	2
	Mít volně dostupné informace a doporučení o ochraně dat a kybernetické bezpečnosti, tedy příkladem na webu města (vytváření kategorií pro subjekty dle potřeby)	**2,29**	**0,45**	3	2	3	2	2	2	2
ZÁSADY OCHRANY DAT		**2,71**	**0,45**	3	3	3	2	3	3	2
	Implementace přísných zákonů a zásad ochrany osobních údajů na ochranu citlivých dat	**3,00**	**0,00**	3	3	3	3	3	3	3
	Vývoj harmonizovaného rámce pro kybernetickou bezpečnost	**2,71**	**0,45**	3	3	3	2	3	3	2
	Mít připravený plán po proniknutí a plán reakce	**2,57**	**0,49**	3	3	3	2	2	3	2
	Minimalizovat místa útoku, tj. různé body, kterými může aktér ohrozit bezpečnost dat	**2,57**	**0,49**	3	3	2	2	3	3	2
	Shromažďovat a ukládat data pouze tam, kde je to nutné	**2,57**	**0,49**	3	3	2	2	3	2	3
	Mít přístup k údajům pouze pro nezbytnou a povolenou akci	**2,57**	**0,49**	3	3	2	2	2	3	3
	Vytváření záloh systémů a dat	**2,86**	**0,35**	3	3	3	2	3	3	3
	Využití přístupu privacy-by-design	**2,57**	**0,49**	3	2	3	3	2	3	2

	Použití architektury zero trust (nulové důvěry)	**2,29**	**0,45**	2	2	2	3	2	3	2
	Vytváření zásad pro mazání dat po skončení jejich životního cyklu	**2,14**	**0,35**	2	2	2	2	2	2	3
	Implementace rámců NIST/ISO a/nebo standardů do nových nebo stávajících strategií	**2,86**	**0,35**	3	3	3	3	3	3	2
	Pravidelně provádět autorizované (povolené státem) penetrační testy	**2,43**	**0,73**	2	3	3	2	3	3	1
ZABEZPEČENÍ DAT PŘI UKLÁDÁNÍ A PŘENOSU		**2,43**	**0,49**	3	2	2	2	2	3	3
	Nepoužitelnost dat po exfiltraci (hašování, šifrování na úrovni pole, tokenizace…)	**2,14**	**0,35**	2	2	2	2	2	3	2
	Použití ochrany před ztrátou/únikem dat (DLP)	**2,43**	**0,49**	3	2	2	2	2	3	3
	Implementovat ochranu během přenosů (šifrování, hesla, používání ověřených kanálů…)	**2,86**	**0,35**	3	3	3	2	3	3	3
	Implementovat ověřování integrity dat	**2,29**	**0,45**	2	2	2	2	2	3	3
LIDSKÉ ZDROJE		**3,00**	**0,00**	3	3	3	3	3	3	3
	Vzdělávání a školení zaměstnanců města v oblasti kybernetické bezpečnosti a ochrany dat, např. prezentace, kurzy, …	**3,00**	**0,00**	3	3	3	3	3	3	3
	Vzdělávání a školení občanů a dalších subjektů v oblasti kybernetické bezpečnosti a ochrany dat, např. webové stránky města s informacemi, …	**2,57**	**0,49**	3	2	3	2	3	3	2
	Vytvoření dedikovaného kybernetického subjektu – týmu (podle velikosti města a potřeb)	**3,00**	**0,00**	3	3	3	3	3	3	3
	Využívat a prohlubovat stávající spolupráci s jinými organizacemi, průmyslem, agenturami a dalšími subjekty	**2,43**	**0,49**	2	2	3	2	3	3	2
VYUŽITÍ EXISTUJÍCÍCH DAT PRO DALŠÍ OCHRANU		**2,14**	**0,35**	2	2	2	2	2	3	2
	Analýza dat, hluboké a strojové učení týkající se potřeb zabezpečení Smart City, např. detekce anomálií v síťovém provozu, detekce malwaru nebo monitorování zabezpečení internetu věcí, …	**2,29**	**0,45**	2	3	2	2	2	3	2
	Využití generativní AI, např. pomocí chatbotů, kteří využívají data k řešení situací souvisejících se zabezpečením	**2,43**	**0,49**	2	2	3	3	2	3	2
	Reakce na incidenty, tedy využití starých existujících dat o bezpečnostních incidentech, výběr možných oblastí útoku, zpřesnění reakce na incidenty atd.	**2,29**	**0,45**	2	2	2	2	2	3	3
Do jaké míry souhlasíte se seznamem doporučení, tedy kategoriemi (úrovněmi) i položkami každé kategorie?		**4,71**	**0,45**	4	5	5	5	5	5	4

Z těchto výsledků je patrné, že nejnižší průměrné hodnocení, které se vyskytuje mezi vytvořenými doporučeními, je pouze 2,14 pro kategorii „V*yužití existujících dat pro další ochranu"*. Pro doporučení lze také nalézt nejnižší průměrné hodnocení 2,14. To se týká: „*[HW, SW] Použití nástrojů pro detekci aktivity v kyberprostoru, např. IDS, SIEM, …"*; *„Centralizované poskytování datové infrastruktury"*; *„Nastavení požadavků na cloud a poskytovatele služeb"*; *„Vytváření zásad pro mazání dat po skončení jejich životního cyklu"*; *„Nepoužitelnost dat po exfiltraci (hašování, šifrování na úrovni pole, tokenizace…)"*. Nejvyšší průměrné hodnocení získala kategorie *„Lidské zdroje"*, která dosáhla maximálního možného průměru, tedy 3,0. V rámci samostatných doporučení se jedná o *„[SW] Nástroje ochrany e-mailů – vestavěné skenování e-mailů, phishing a ochrana zabezpečení internetu; Implementace přísných zákonů a zásad ochrany osobních údajů na ochranu citlivých dat; Vzdělávání a školení zaměstnanců města v oblasti kybernetické bezpečnosti a ochrany dat, např. prezentace, kurzy, …; Vytvoření dedikovaného kybernetického subjektu – týmu (podle velikosti města a potřeb)"*, které mají maximální hodnocení 3,0.

V rámci třetího kola se většina expertů shodla, že se seznamem doporučení *„Silně souhlasí"* (Strongly agree), což uvedlo pět expertů. Zbylí dva experti se vyjádřili, že s vytvořenými doporučeními *„Souhlasí"* (Agree). Průměr souhlasu se seznamem je 4,71. Toto třetí kolo je tedy finální, a proto vytvořená doporučení, na kterých se experti shodli, jsou brána jako konečná doporučení pro problematiku kyberbezpečnosti a ochrany dat ve strategiích a projektech Smart Cities.

4.2 KONEČNÝ SEZNAM DOPORUČENÍ

Konečný seznam doporučení pro kyberbezpečnost a ochranu dat ve Smart Cities je zobrazen v Tabulce 10. Došlo tedy k vytvoření šesti kategorií – *„HW a SW řešení, organizační řešení, zásady ochrany dat, zabezpečení dat při ukládání a přenosu, lidské zdroje a využití existujících dat pro další ochranu"*. V těchto kategoriích došlo k vytvoření 39 doporučení. Kategorie „*HW a SW řešení"* obsahuje 7 doporučení, „*Organizační řešení"* obsahuje 9 doporučení, „*Zásady ochrany dat"* obsahuje 12 doporučení, *„Zabezpečení dat při ukládání a přenosu"* obsahuje 4 doporučení, *„Lidské zdroje"* obsahují 4 doporučení a poslední kategorie *„Využití existujících dat pro další ochranu"* obsahuje 3 doporučení.

Tabulka 10: Konečný seznam doporučení pro kyberbezpečnost a ochranu dat ve Smart Cities. Zdroj: vlastní.

DOPORUČENÍ	
I.	**HW A SW ŘEŠENÍ**
1.	[HW, SW] Nastavení dohledu a analýzy na místě – použití kamer s podporou analýzy, AI nebo rozpoznávání pohybu…
2.	[HW, SW] Přístup do zařízení nebo částí budov pomocí automatických systémů registrace návštěvníků
3.	[HW, SW] Použití nástrojů pro detekci aktivity v kyberprostoru, např. IDS, SIEM, …
4.	[HW, SW] Vícefaktorová autentizace
5.	[SW] Nástroje ochrany e-mailů – vestavěné skenování e-mailů, phishing a ochrana zabezpečení internetu
6.	[SW] Mít bezpečnostní požadavky na SW, blacklist nebo deny-by-exception pro neautorizovaný SW atd.
7.	[HW, SW] Použití biometrických systémů pro přístup do definovaných částí budov, např. administrativa, serverovny apod.
II.	**ORGANIZAČNÍ ŘEŠENÍ**
8.	Centralizované poskytování datové infrastruktury
9.	Zabezpečená komunikační síť na úrovni bezpečnostních složek krizového řízení
10.	Provádět pravidelné hodnocení rizik zabezpečení dat
11.	Kybernetická bezpečnost na vrcholu priorit (finanční zdroje, lidé, infrastruktura)
12.	Využití Privacy Impact Assessment při zavádění nových technologií
13.	Mít plán aktualizací aplikací, provádět je včas
14.	Nastavení požadavků na cloud a poskytovatele služeb
15.	Analýza připravenosti a současného stavu města z hlediska financí a lidských zdrojů na zavádění nových kybernetických opatření a ochrany dat
16.	Mít volně dostupné informace a doporučení o ochraně dat a kybernetické bezpečnosti, tedy příkladem na webu města (vytváření kategorií pro subjekty dle potřeby)
III.	**ZÁSADY OCHRANY DAT**
17.	Implementace přísných zákonů a zásad ochrany osobních údajů na ochranu citlivých dat
18.	Vývoj harmonizovaného rámce pro kybernetickou bezpečnost
19.	Mít připravený plán po proniknutí a plán reakce
20.	Minimalizovat místa útoku, tj. různé body, kterými může aktér ohrozit bezpečnost dat
21.	Shromažďovat a ukládat data pouze tam, kde je to nutné
22.	Mít přístup k údajům pouze pro nezbytnou a povolenou akci
23.	Vytváření záloh systémů a dat

24.	Využití přístupu privacy-by-design
25.	Použití architektury zero trust (nulové důvěry)
26.	Vytváření zásad pro mazání dat po skončení jejich životního cyklu
27.	Implementace rámců NIST/ISO a/nebo standardů do nových nebo stávajících politik
28.	Pravidelně provádět autorizované (povolené státem) penetrační testy
IV.	**ZABEZPEČENÍ DAT PŘI UKLÁDÁNÍ A PŘENOSU**
29.	Nepoužitelnost dat po exfiltraci (hašování, šifrování na úrovni pole, tokenizace…)
30.	Použití ochrany před ztrátou/únikem dat (DLP)
31.	Implementovat ochranu během přenosů (šifrování, hesla, používání ověřených kanálů…)
32.	Implementovat ověřování integrity dat
V.	**LIDSKÉ ZDROJE**
33.	Vzdělávání a školení zaměstnanců města v oblasti kybernetické bezpečnosti a ochrany dat, např. prezentace, kurzy, …
34.	Vzdělávání a školení občanů a dalších subjektů v oblasti kybernetické bezpečnosti a ochrany dat, např. webové stránky města s informacemi, …
35.	Vytvoření dedikovaného kybernetického subjektu – týmu (podle velikosti města a potřeb)
36.	Využívat a prohlubovat stávající spolupráci s jinými organizacemi, průmyslem, agenturami a dalšími subjekty
VI.	**VYUŽITÍ EXISTUJÍCÍCH DAT PRO DALŠÍ OCHRANU**
37.	Analýza dat, hluboké a strojové učení týkající se potřeb zabezpečení Smart City, např. detekce anomálií v síťovém provozu, detekce malwaru nebo monitorování zabezpečení internetu věcí, …
38.	Využití generativní AI, např. pomocí chatbotů, kteří využívají data k řešení situací souvisejících se zabezpečením
39.	Reakce na incidenty, tedy využití starých existujících dat o bezpečnostních incidentech, výběr možných oblastí útoku, zpřesnění reakce na incidenty atd.

Vyhodnocením výše uvedeného konečného seznamu lze městům, jež přijaly nebo se chystají řešit projekty založené na konceptu Smart City, doporučit zvážení těchto kategorií ve svých strategiích a projektech. První kategorií je *„HW a SW řešení“*, která je zaměřena především na HW, SW nebo propojení obou přístupů pro problematiku kyberbezpečnosti a ochrany dat. Tato doporučení jsou hlavně zaměřena na přístupy do budov, jejich částí, přístupy do místností, jako jsou serverovny apod., kde dochází nějakým způsobem k práci s daty. Dále jsou doporučení zaměřena na prevenci a detekci aktivit v rámci kyberprostoru a správu emailů. V rámci detekce aktivit v kyberprostoru může dojít k využívání IDS nebo SIEM. IDS je technologie nebo aplikace, která proaktivně kontroluje, monitoruje a analyzuje síť před škodlivými hrozbami.

SIEM je bezpečnostní řešení, které pomáhá detekovat hrozby, analyzovat a reagovat na hrozby. Do tohoto řešení může spadat centrální logování, korelace událostí, detekce anomálií a další.

„Organizační řešení“ jsou taková doporučení, která si nastavuje město jako organizace. Jedná se o vytvoření zabezpečených, centralizovaných infrastruktur různého typu. Provádění analýz a nastavení priorit v rámci ochrany dat a kyberbezpečnosti. Vytvoření požadavků například pro cloudové řešení nebo na volnou dostupnost informací ohledně kyberbezpečnosti. *„Zásady ochrany dat“* jsou doporučení, která jsou zaměřená na zavedení zásad, politik nebo zákonů tak, aby napomáhaly a zaváděly ochranu dat a kyberbezpečnost. Je také nutné mít vytvořené plány reakce po incidentu, zálohovat systémy a data, využívat přístupy k tvorbě jako je privacy-by-design nebo zero trust architektura. Dále je nutné řešit, jakým způsobem nakládat s daty, pokud ta již nejsou potřebná a využívaná, a také pravidelně testovat zabezpečení všech kanálů kudy data procházejí, stejně jako datových úložišť.

„Zabezpečení dat při ukládání a distribuci“. V této kategorii se jedná o doporučení zaměřená na správu a ochranu dat při práci s nimi, tedy hlavně na ukládání dat a následně jejich přenos. Dochází k využití šifrovacích metod, hesel, hašování a dalšího. Dále je zde doporučení pro využití DLP, což je řešení nebo přístup, který identifikuje a pomáhá zabránit nebezpečnému sdílení, přenosu nebo používání citlivých dat pomocí různých technik. Může využívat šifrování, filtraci dat nebo monitoring a další. *„Lidské zdroje“* je kategorie zaměřující se na práci s lidmi, resp. uživateli dat jako často nejslabším článkem celého procesu zabezpečení a ochrany dat, vytváření týmů a spoluprací, a jejich vzdělání v oblasti ochrany dat a kyberbezpečnosti s důrazem na jejich roli, tzn. zaměstnanec města, úředník, občan, podnik nebo jiná organizace atd. *„Využití existujících dat pro další ochranu“* obsahuje doporučení, která se zaměřují na využití již existujících informací a dat a jejich aplikaci a využití pro další prohloubení ochrany dat a kyberbezpečnosti. Příkladem mohou být různé datové analýzy v reálném čase, hloubkové a strojové učení, využití generativní AI a chatbotů nebo reakce na incidenty dle již existujících historických dat.

ZÁVĚR

Cílem této práce byla analýza kyberbezpečnosti a ochrany dat ve strategiích a projektech Smart Cities ve vybraných světových městech, která pomocí definovaných metodických kroků vedla k vytvoření doporučení pro ochranu dat a kyberbezpečnost při tvorbě Smart City projektů.

Cíl práce byl splněn. V prvních kapitolách této práce bylo definováno prostředí, ve kterém je tato práce zpracovávána, tzn. definice základních pojmů jako je kyberprostor, kybernetická bezpečnost a Smart City. V rámci kyberbezpečnosti pak došlo k vymezení pojmů bezpečnost a kyberbezpečnost. Byly uvedeny principy kyberbezpečnosti a současné hrozby, které se vyskytují v rámci kyberbezpečnosti. U Smart City byly uvedeny definice tohoto termínu, dále byly vymezeny základní komponenty Smart City a došlo k uvedení příkladu technologií, které se v Smart City využívají. V další kapitole byla popsána stávající situace v této oblasti založená na identifikaci a porovnání přístupů a kritérií. Došlo tedy k popisu dnešní doby, a její potřeby v rámci měst využívat kybernetické bezpečnosti a ochrany dat, a k uvedení příkladů způsobů ochrany. Dále došlo k popisu a rozboru existujících dokumentů, které se zaobírají strategiemi a projekty Smart City. Zde došlo k sumarizaci několika dokumentů na úrovni mezinárodního, nadnárodního, národního a soukromého sektoru. Také došlo k vytvoření přehledu a popisu rámců a indexů, které hodnotí města v rámci rozvoje a implementace konceptu Smart City. V neposlední řadě jsou brány v potaz i výzkumné práce, které se zaobírají ochranou dat a kyberbezpečností ve strategiích a projektech Smart City. Došlo tedy k vyhledání několika prací a sumarizaci jejich doporučení a přístupu k tomuto tématu.

Hlavní část práce se věnovala analýze a vyhodnocení získaných dat. Nejdříve byl zvolen metodický postup řešení, který byl tvořen jednotlivými kroky, pomocí kterých byly analýza a vyhodnocení dat provedeny. Tento postup je klíčový pro ověřitelnost získaných zjištění. Poté následovaly konkrétní kroky vyhledávání zdrojů, obsahové analýzy a metody Delphi, která byla zvolena pro ověření získaných dat. Vlastnímu ověření je pak věnována kapitola 4, ve které je nejdříve představena metoda Delphi a následně popsány kroky její realizace, včetně výsledků. Ověřený seznam doporučení pro danou problematiku je pak diskutován v kapitole 4.2.

Ačkoliv byl cíl práce splněn a seznam 39 doporučení rozdělených do 6 kategorií představuje ucelený pohled na možnosti nejenom měst hlásících se ke konceptu Smart City, které chtějí řešit problematiku kyberbezpečnosti a ochranu dat ve svých strategiích a projektech, tak i tato zjištění a doporučení mají svoje omezení, především v oblasti aplikovatelnosti v praxi. Prvním

omezením je, že seznam doporučení byl ověřen pro modelové Smart City, které svým popisem a vymezením reprezentuje spíše Smart Cities, která lze nalézt na vyšších příčkách indexů/rámců pro hodnocení konceptu Smart City, tzn., že mají zpravidla k dispozici dostatečné lidské, finanční a výpočetní zdroje, a zároveň existující infrastrukturu ve formě sítí, silnic atd., které mohou využít pro implementaci navržených doporučení. Pro některá města tak nemusí být některá doporučení relevantní, ať už z důvodů chybějících zdrojů nebo infrastruktury. Druhým omezením je pak výběr expertů, když více zapojených expertů by mohlo vyprodukovat další doporučení, která by mohla být pro tuto problematiku využitelná. Nicméně větší počet expertů nebyl s ohledem na omezené zdroje k dispozici, resp. větší počet expertů by mohl způsobit problémy při realizaci metody Delphi, především co se týká doby trvání a dodržování termínů. Posledním omezením je pak aktuálnost tohoto tématu, když Smart Cities neustále vydávají nové strategie a řešení nové projekty, ze kterých by šlo získat nové informace. Toto omezení bylo v této práci vyřešeno volbou vzorku měst a zároveň tím, že experti mohli navrhovat i vlastní doporučení, která odpovídají aktuálním trendům, což je např. generativní AI a využití chatbotů pro řešení bezpečnostních situací, kde si občané mohou nechat poradit.

Závěrem lze tedy tvrdit, že tato práce poskytuje důležité přínosy pro praxi ve formě ověřených doporučení pro řešení problematiky kyberbezpečnosti a ochrany dat ve strategiích a projektech Smart Cities. Zároveň nabízí přínosy i pro teorii, a to ve formě sumarizace existujících přístupů ke tvorbě a hodnocení strategií a projektů, především s ohledem na existující rámce, indexy, jejich strukturu a základní komponenty Smart City.

POUŽITÉ ZDROJE

ALAMER, Maryam; ALMAIAH, Mohammed Amin. Cybersecurity in Smart City: A systematic mapping study. In: *2021 international conference on information technology (ICIT)*. IEEE, 2021. p. 719-724.

ANDRADE, Roberto Omar; YOO, Sang Guun; TELLO-OQUENDO, Luis; ORTIZ-GARCES, Ivan. A comprehensive study of the IoT cybersecurity in smart cities. *IEEE Access*, 2020, 8: 228922-228941.

BACON, Madelyn. *What is security?* TechTarget [online]. [cit. 2023-10-07]. 2021. Dostupné z: https://www.techtarget.com/searchsecurity/definition/security

BRISSON, Marie-Noelle; DOGGENDORF, Dan; SAVOIE, Michael J. Cybersecurity of building technology: smart cities and smart buildings require smart protection. *CRE Real Estate Issues*, 2019, 43.1: 1-9.

BUNDESMINISTERIUM DES INNERN UND FÜR HEIMAT. *Smart City Charta: Digitale Transformation in den Kommunen nachhaltig gestalten* [online]. 2017. [cit. 2024-02-04]. Dostupné z: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/building-housing/city-housing/smart-city-charter-short.pdf

CAMBRIDGE DICTIONARY. *Security*. Cambridge Dictionary [online]. Cambridge University Press & Assessment, 2023. [cit. 2023-10-07]. Dostupné z: https://dictionary.cambridge.org/dictionary/english/security

CISA. *Cybersecurity Best Practices for Smart Cities.* [online]. 2023. [cit. 2024-02-04]. Dostupné z: https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf

CLARK, David D. *Characterizing Cyberspace: Past, Present and Future*. MIT [online]. 2010. [cit. 2023-12-30]. Dostupné z: https://dspace.mit.edu/bitstream/handle/1721.1/141692/Clark%20%282010%29%20Characterizing%20cyberspace.pdf

COHEN, Julie E. Cyberspace as/and Space. *Columbia Law Review*, 2007, 107.1: 210-256.

CRISP, Jackie; PELLETIER, Dianne; DUFFIELD, Christine; ADAMS, Anne; NAGY, Sue. The delphi method?. *Nursing Research*, 1997, 46.2: 116-118.

EC-COUNCIL. *Understanding the Incident Response Life Cycle*. EC-COUNCIL [online]. 2022. [cit. 2023-11-22]. Dostupné z: https://www.eccouncil.org/cybersecurity-exchange/incident-handling/what-is-incident-response-life-cycle/

GIFFINGER, Rudolf; GUDRUN, Haindlmaier. Smart cities ranking: an effective instrument for the positioning of the cities. *ACE: Architecture, City and Environment*, 2010, 4.12: 7-26.

GLADSTONE, Nikki; FLATT, Jo; FADER, Julie; HELLSTERN, Meghan. *How to be Smart(er) in Mid-Sized Cities in Ontario* [online]. 2018. [cit. 2023-11-19]. Dostupné z: https://futurecitiescanada.ca/portal/wp-content/uploads/sites/2/2021/11/evergreen-howtobesmarterinmidsizedcities-february2018.pdf

EDEN STRATEGY INSTITUTE. *Top 50 Smart City Governments* [online]. 2021. [cit. 2024-02-06]. Dostupné z: https://static1.squarespace.com/static/5b3c517fec4eb767a04e73ff/t/6063814af4d39b693379597d/1617133979623/Eden_Top+50+Smart+City+Governments+2020-21_DIGITAL.pdf

EUROPEAN COMMISION. *The making of a smart city: policy recommendations*. SCIS/SCM Policy paper. [online]. 2017. [cit. 2024-02-04]. Dostupné z: https://smart-cities-marketplace.ec.europa.eu/sites/default/files/2021-04/the_making_of_a_smart_city_-_policy_recommendations.pdf

EVROPSKÝ PARLAMENT. *Kybernetická bezpečnost: Hlavní a nově se objevující hrozby.* Evropský parlament [online]. 2022. [cit. 2023-11-14]. Dostupné z: https://www.europarl.europa.eu/topics/cs/article/20220120STO21428/kyberneticka-bezpecnost-hlavni-a-nove-se-objevujici-hrozby

FALCONER, Gordon; MITCHELL, Shane. Smart city framework: A Systematic Process for Enabling Smart+Connected Communities [online]. 2012. [cit. 2023-11-22]. Dostupné z: https://www.cisco.com/c/dam/en_us/about/ac79/docs/ps/motm/Smart-City-Framework.pdf

FARRIER, Ellie. *What is social engineering?* Norton [online]. 2023. [cit. 2023-11-23]. Dostupné z: https://us.norton.com/blog/emerging-threats/what-is-social-engineering

FINK-HAFNER, Danica; DAGEN, Tamara; DOUŠAK, May; NOVAK, Meta; HAFNER-FINK, Mitja. Delphi method: strengths and weaknesses. *Advances in Methodology and Statistics*, 2019, 16.2: 1-19.

FRUHLINGER, Josh. *The CIA triad: Definition, components and examples*. CSO [online]. [cit. 2023-11-11]. 2020. Dostupné z: https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html

GOHAR, Ali; NENCIONI, Gianfranco. The role of 5G technologies in a smart city: The case for intelligent transportation system. *Sustainability*, 2021, 13.9: 5188.

GOV.UK. *Secure connected places (smart cities) guidance collection*. Gov.UK [online]. 2023. [cit. 2024-02-04]. Dostupné z: https://www.gov.uk/government/publications/secure-connected-places-smart-cities-guidance-collection

HABIBZADEH, Hadi; NUSSBAUM, Brian H.; ANJOMSHOA, Fazel; KANTARCI, Burak a SOYATA, Tolga. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, 2019, 50: 101660.

HASHEM, Ibrahim Abaker Targio, et al. The role of big data in smart city. *International Journal of Information Management,* 2016, 36.5: 748-758.

IBM. *What is Cybersecurity?* IBM [online]. 2023 [cit. 2023-10-07]. Dostupné z: https://www.ibm.com/topics/cybersecurity

IESE BUSINESS SCHOOL. *IESE Cities in Motion Index 2022* [online]. 2022. [cit. 2024-02-06]. Dostupné z: https://www.iese.edu/media/research/pdfs/ST-0633-E.pdf

IMD BUSINESS SCHOOL. *IMD Smart City Index Report 2023* [online]. 2023. [cit. 2024-02-06]. Dostupné z: https://www.imd.org/wp-content/uploads/2023/04/smartcityindex-2023-v7.pdf

ISMAIL, Adiel; BAGULA, Bigomokero Antoine; TUYISHIMIRE, Emmanuel. Internet-of-things in motion: A uav coalition model for remote sensing in smart cities. *Sensors*, 2018, 18.7: 2184.

JOHNSON, Ashley. *Balancing Privacy and Innovation in Smart Cities and Communities*. Information Technology & Innovation Foundation [online]. 2023. [cit. 2024-02-06]. Dostupné z: https://www2.itif.org/2023-smart-cities-privacy.pdf

KASPERSKY. *What is cybersecurity?* Kaspersky [online]. [cit. 2023-10-07]. AO Kaspersky Lab, 2023. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

KEARNEY. *The distributed geography of opportunity: The 2023 Global Cities Report* [online]. 2023. [cit. 2024-02-07]. Dostupné z: https://www.kearney.com/documents/291362523/299003325/The+distributed+geography+of+opportunity-the+2023+Global+Cities+Report.pdf

KEMMERER, Richard A. Cybersecurity. In: *25th International Conference on Software Engineering, 2003. Proceedings*. IEEE, 2003. p. 705-715.

KHATOUN, Rida; ZEADALLY, Sherali. Cybersecurity and privacy solutions in smart cities. *IEEE Communications Magazine*, 2017, 55.3: 51-59.

KIM, Tai-hoon; RAMOS, Carlos; MOHAMMED, Sabah. Smart city and IoT. *Future Generation Computer Systems*, 2017, 76: 159-162.

KOLOUCH, Jan; BAŠTA, Pavel. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

LAW, Kincho H.; LYNCH, Jerome P. Smart city: Technologies and challenges. *IT Professional*, 2019, 21.6: 46-51.

LINKOV, Václav; ZÁMEČNÍK, Petr; HAVLÍČKOVÁ, Darina; PAI, Chih-Wei. Human factors in the cybersecurity of autonomous vehicles: Trends in current research. *Frontiers in Psychology*, 2019, 10:995.

MA, Chen. Smart city and cyber-security; technologies used, leading challenges and future recommendations. *Energy Reports*, 2021, 7: 7999-8012.

MCGRAW, Gary; MORRISETT, Greg. Attacking malicious code: A report to the infosec research council. *IEEE Software*, 2000, 17.5: 33-41.

MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy*. Praha: Leges, 2018. Teoretik. ISBN 978-80-7502-275-2.

MERRIAMWEBSTER. *Cybersecurity.* MerriamWebster Dictionary [online]. [cit. 2023-09-11]. 2023. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity

MIJWIL, Maad; DOSHI, Ruchi; HIRAN, Kamal Kant; AL-MISTAREHI, Abdel-Hameed; GÖK, Murat. Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects. *Mesopotamian Journal of Cybersecurity*, 2022, 2022: 1-4.

MINISTERSTVA INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SR. Metoda k tvorbe inteligentných projektov [online]. 2023. [cit. 2024-02-04]. Dostupné z: https://www.smartcity.gov.sk/wp-content/uploads/2023/08/Metodika-k-tvorbe-smart-projektov_compressed.pdf

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR. *Metodika Smart Cities: Metodika pro přípravu a realizaci konceptu Smart Cities na úrovni měst, obcí a regionů* [online]. 2018. [cit. 2024-02-04]. Dostupné z: https://mmr.gov.cz/getmedia/f76636e0-88ad-40f9-8e27-cbb774ea7caf/metodika_smart_cities.pdf.aspx?ext=.pdf

MOHAMED, Nader; AL-JAROODI, Jameela; JAWHAR, Imad; IDRIES, Ahmed a MOHAMMED, Farhan. Unmanned aerial vehicles applications in future smart cities. *Technological Forecasting and Social Change*, 2020, 153:119293.

MOHANTY, Saraju P.; CHOPPALI, Uma; KOUGIANOS, Elias. Everything you wanted to know about smart cities: The Internet of things is the backbone. *IEEE Consumer Electronics Magazine*, 2016, 5.3: 60-70.

MORI MEMORIAL FOUNDATION. *Global Power City Index 2023* [online]. 2023. [cit. 2024-02-07]. Dostupné z: https://mori-m-foundation.or.jp/pdf/GPCI2023_summary.pdf

O'GORMAN, Gavin; MCDONALD, Geoff. *Ransomware: A Growing Menace.* Norton (Symantec) [online]. 2012. [cit. 2023-11-22]. Dostupné z: https://radar.assets.avrotros.nl/editorial/Documenten/symantec.pdf

O'KANE, Philip; SEZER, Sakir; CARLIN, Domhnall. Evolution of ransomware. *Iet Networks*, 2018, 7.5: 321-327.

PENDER-BEY, Georgie. *The parkerian hexad*. Information Security Program at Lewis University [online]. 2019. [cit. 2023-12-30]. Dostupné z: https://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf

ROLAND BERGER. *Smart city, smart strategy*. Munich: Roland Berger GMBH, 2017.

ROUSE, Margaret. *What is Cyberspace.* Techopedia [online]. 2023. [cit. 2023-11-11]. Dostupné z: https://www.techopedia.com/definition/2493/cyberspace

SAEED, Imtithal A.; SELAMAT, Ali; ABUAGOUB, Ali MA. A survey on malware and malware detection systems. *International Journal of Computer Applications*, 2013, 67.16: 25-31.

SAMONAS, Spyridon; COSS, David. The CIA strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 2014, 10.3: 21-45.

SARKER, Iqbal H.; KAYES, A. S. M.; BADSHA, Shahriar; ALQAHTANI, Hamed; WATTERS, Paul et al. Cybersecurity data science: an overview from machine learning perspective. *Journal of Big Data*, 2020, 7:41.

SASHINSKAYA, Maria. *Smart Cities in Europe Open Data in a Smart Mobility Context*. CreateSpace Independent Publishing Platform, 2015. ISBN 978-1522924890.

SHU, Kai; BHATTACHARJEE, Amrita; ALATAWI, Faisal; NAZER, Tahora H.; DING, Kaize et al. Combating disinformation in a social media age. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 2020, 10.6: e1385.

SLAVÍK, Jakub. *Smart city v praxi: jak pomocí moderních technologií vytvářet město příjemné k životu a přátelské k podnikání*. Praha: Profi Press, 2017. ISBN 978-80-86726-80-9.

SOUČEK, Vladimír, Eva STAŇOVÁ a Martin LINHART. *Vnitřní bezpečnost a veřejný pořádek Krizové řízení* [online]. [cit. 2023-10-07]. Praha: MVČR, 2005. Dostupné z: https://www.mvcr.cz/soubor/bezpecnost-pdf.aspx

TOWNSEND, Anthony. *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*. W. W. Norton & Company, 2013. ISBN 9780393241532.

UNITED NATIONS. *Around 2.5 billion more people will be living in cities by 2050, projects new UN report.* United Nations [online]. 2023. [cit. 2023-12-31]. Dostupné z: https://www.un.org/en/desa/around-25-billion-more-people-will-be-living-cities-2050-projects-new-un-report

VENABLES, Adrian. Modelling Cyberspace to Determine Cybersecurity Training Requirements. *Frontiers in Education*, 2021, 6:768037.

VERHULSDONCK, Gustav; WEIBLE, Jennifer L.; HELSER, Susan; HAJDUK, Nancy. Smart cities, playable cities, and cybersecurity: a systematic review. *International Journal of Human–Computer Interaction*, 2023, 39.2: 378-390.

VODÁK, Josef; ŠULYOVÁ, Dominika; KUBINA, Milan. Advanced technologies and their use in smart city management. *Sustainability*, 2021, 13.10: 5746.

WISSEMA, Johan G. Trends in technology forecasting. *R&D Management*, 1982, 12.1: 27-36.

WORLD ECONOMIC FORUM. *Governing smart cities: Policy benchmarks for ethical and responsible smart city development*. Geneva: World Economic Forum, 2021.

WU, Yung Chang; SUN, Rui; WU, Yenchun Jim. Smart city development in Taiwan: From the perspective of the information security policy. *Sustainability*, 2020, 12.7: 2916.

YIN, ChuanTao; XIONG, Zhang; CHEN, Hui; WANG, JingYuan; COOPER, Daven et al. A literature survey on smart cities. *Science China Information Sciences*, 2015, 58.10: 1-18.

SEZNAM PŘÍLOH

Příloha I: Zdroje pro šest komponent Smart City strategií. Zdroj: vlastní

Město	Název dokumentu nebo webu					
	Smart Economy	**Smart People**	**Smart Governance**	**Smart Mobility**	**Smart Environment**	**Smart Living**
NYC	IoT Strategy Plan NYC EDC	IoT Strategy Plan	IoT Strategy Plan	IoT Strategy Plan	IoT Strategy Plan	IoT Strategy Plan
Washington DC	Ch. 7 Economic Development	Volume 3 Implementation Element	Ch. 11 Community Services and Facilities	Ch. 4 Transportation	Ch. 6 Environmental Protection	Ch. 5 Housing
Chicago	IT Strategic Plan	IT Strategic Plan	IT Strategic Plan	Strategic Plan for Transportation	Chicago Nature and Wildlife Plan	Chicago energy benchamrking 2020
SF	ICT Plan 2022-2026	City of San Francisco	City of San Francisco	City of San Francisco	SF environment department	City of San Francisco
Toronto	Toronto Official Plan – Chapter 2	HousingTO 2020-2030	Toronto Open Data Masterplan	Toronto Official Plan – Chapter 2	Toronto Official Plan – Chapter 3	HousingTO 2020-2030
LA	SmartLA 2028	SmartLA 2028	SmartLA 2028	The Mobility Plan 2035	Sustainable city pLan	Strategic plan 2024-2025
Londýn	Smart London Plan	Smart London Plan	Smart London Plan	Smart London Plan	Smart London Plan	Smart London Plan
Paříž	Paris Smart and Sustainable	Paris Smart and Sustainable	Paris Smart and Sustainable	Paris Smart and Sustainable	Paris Tomorrow	Paris Smart and Sustainable
Berlín	Gemeinsam Digital: Berlin	Gemeinsam Digital: Berlin	Gemeinsam Digital: Berlin	Stadtentwicklungsplan Mobilität und Verkehr Berlin 2030	Values Compass for Berlin as a digital city	Gemeinsam Digital: Berlin

Amsterdam	Circular Economy Programme 2020-2021	Projekt AMdEX	Circular Economy Programme 2020-2021	Mobility Data	Circular Economy Programme 2020-2021	Projekt PAUL
Kodaň	Flow data solutions	Smart City Infrastructure Analysis	Flow data solutions	Copenhagen Parking	CPH 2025 Climate Plan	CPH 2025 Climate Plan
Praha	Koncepce Smart Prague do roku 2030	Koncepce Smart Prague do roku 2030	Koncepce Smart Prague do roku 2030	Koncepce Smart Prague do roku 2030	Koncepce Smart Prague do roku 2030	Koncepce Smart Prague do roku 2030
Tokio	Tokyo Sustainability Action 2023	Tokyo Sustainability Action 2023	ST implementation strategy	ST implementation strategy	ST implementation strategy	ST implementation strategy
Singapur	Digital economy framework for action	Smart Urban Initiatives	Digital economy framework for action	Smart Transport Initiatives	Smart Urban Initiatives	Smart Urban Initiatives
Soul	Smart Seoul Policies	Smart Seoul Policies	Smart Seoul Policies	Smart Seoul Policies	Smart Seoul Policies	Smart Seoul Policies
HKG	Hong Kong Smart City Blueprint 2.0 HK Smart Economy	HK Smart People	Hong Kong Smart City Blueprint 2.0	Hong Kong Smart City Blueprint 2.0	Hong Kong Smart City Blueprint 2.0	Hong Kong Smart City Blueprint 2.0
Tchaj-pej	Smart Taipei	Smart Taipei, One City	Smart Taipei, One City	Smart Taipei, One City	Smart Taipei, One City	Smart Taipei, One City
Peking	Beijing Investment Development Report	Smarter Beijing 2019	Beijing Investment Development Report	Smarter Beijing 2019	Smarter Beijing 2019	Smarter Beijing 2019
Sydney	Smart City Strategic Framework	Smart City Strategic Framework	Smart City Strategic Framework	Smart City Strategic Framework	Smart City Strategic Framework	Smart City Strategic Framework

Melbourne	Melbourne's Thriving Economic Future 2031	Health And Wellbeing Action Plan 2021–2025 Gender Equality Action Plan 2022–25	Future Melbourne 2026	Transport Strategy 2030	Emerging Technology Testbed	Design And Construction Standards
Canberra	ACT Digital Strategy	ACT Digital Strategy	ACT Digital Strategy	Act Transport Recovery Plan	ACT Digital Strategy	ACT Digital Strategy
Wellington	Wellington Towards 2040: Smart Capital	Capacity Assessment Wellington City Council	-	A zero waste future for Wellington	Accessible Wellington	-

Příloha II: Vyhodnocení Smart City strategií pro města v Severní Americe. Zdroj: vlastní.

Město	Kyberbezpečnost a ochrana dat – Severní Amerika
NYC	Systém sběru dat o veřejné bezpečnosti, monitorování akustických výstřelů po městě, největší městská veřejná bezpečnost v USA. Domain Awareness System – digitální sledovací systém shromažďuje a zpracovává údaje o videozáznamech policie NYC, čtečky registrovaných značek, radiační a chemické senzory, 911 hlášení a datové kanály městských systémů. NYC 311 systém je služba pro komunikaci mezi vládou a občany, shromažďuje přes 232 milionů kontaktů od roku 2003. Tři úrovně IoT dat vzhledem k soukromí: 1) je neschopná (nesmí) identifikovat daného jedince, 2) je nutné znát kontext, aby byla možná identifikace a 3) rozezná a určí jedince vždy a jedná se vždy o citlivé informace. Department of Citywide Administrative Services má implementované bezpečnostní politiky a procedury pro přístup k programům, vzhledem k citlivosti dat o lokaci vozidel. Anonymizování těchto dat. Pro ochranu před kybernetickými útoky vznikl New York City Cyber Command. Provádí hloubkové analýzy kybernetické bezpečnosti zařízení a systémů. Ve městě jsou nastaveny procesy pro kontrolování a testování kybernetické bezpečnosti v rámci nasazení IoT.
Washington DC	Hlavní prvky Smart City jsou zdroje dat (generátory) a uživatelé dat, když datové systémy jsou úzce integrovány se sítěmi v celém městě. Pro ně jsou nastaveny postupy pro ochranu osobních údajů. Standardy v politice otevřených dat, které ústí v transparentnost a zabezpečení dat. Využívání otevřených dat v reálném čase pro analýzy dat a plánování. Projekt na vyhodnocení připravenosti kybernetické bezpečnosti fyzických systémů, které zahrnuje zranitelnosti a hrozby pro fyzické systémy. Vyvinout online nástroj pro sběr a sdílení dat o veřejném životě s vhodnou ochranou soukromí. Využití informací z osobních mobilů a z infrastruktury Smart City k pochopení toho, jak má fungovat veřejná správa a využít toho pro lepší bezpečnost. Spolupráce s federálními agenturami na vývoji a návrhových opatření, které vyhovují bezpečnostním potřebám veřejného prostoru.
Chicago	Existuje IT strategický plán s akčním plánem na městskou IT infrastrukturu, který obsahuje složku bezpečnost. Implementace hybridní multi-cloudové infrastruktury. Tým digitálních služeb a příručky, které obsahují zabezpečení. Spadá sem digitální identita, autentifikační technologie, soukromí dat a jejich ochran, integrita dat,

Město	Kyberbezpečnost a ochrana dat – Severní Amerika
	Application Programming Interface, automatické testování nebo postupy systémového inženýrství. Model sdílených služeb pro IT napříč městskými odděleními a agenturami. Sloučení oddělení a standardizace IT postupů napříč obchodními jednotkami povede k lepší kyberbezpečnosti. Využití nových technologií, shromažďování, analyzování a publikování dat a využití těchto nástrojů a informací.
SF	Neustále analyzování dat napříč městem. Tým digitálních služeb spolupracuje s DataSF na vývoji sady datových služeb a zabezpečené architektury pro vývoj datových standardů, modelů, hodnocení, monitorování a školení a služby ověřování dat a kvality dat. Vývoj zásad a monitorování rizikových přístupů k datům. Definování principů, požadavků a postupů pro fáze životního cyklu dat: • Plánování a generování: sběr pouze potřebných dat a snaha sběru přímo ze zdroje, transparentnost, zahrnout rizika soukromí; • Správa: zkontrolovat přesnost dat, zajistit že jsou data chráněná; • Přístup a využití: přístup pouze oprávněným osobám, každý subjekt má přístup ke svým datům; • Archivovat a likvidovat: udržení dat pouze po potřebnou dobu, zajistit ochranu po dobu uchování dat. Zajištění, že rámec zabezpečení informací bude v souladu se zásadami bezpečnosti informací státu i města. Začlenit různé rámce zabezpečení informací, včetně zásad NIST nebo ISO, a základních cílů důvěrnosti, integrity a dostupnosti. Rámec pro zajištění nových metod sběru dat, aby nevytvářely zbytečné ohrožení možnosti jednotlivců pohybovat se po městě, bez centrálního sledování. Pro data generovaná městem došlo k přijetí celoměstského licenčního standardu: Open Data Commons Public Domain Dedication License. Centrum otevřených dat nebude obsahovat žádné osobní údaje. Datové centrum bude uchovávat pouze souhrnná data z určitých senzorů, aby se zlepšilo soukromí a zabezpečení. Escrypt poskytuje implementaci bezpečnostního přístupu k systémům i datům. Bosch poskytuje poradenské služeb pro aplikace IoT Cloud a V2x Cybersecurity.
Toronto	Omezení shromažďování osobních údajů. Zavedení záruk, které prosazují práva na soukromí, a ochrání digitální infrastrukturu před zneužitím, hackery, krádeží nebo narušením. Přístup „by-design“ (ochrana soukromí, zabezpečení a přístup podle návrhu), aby vytvořené výhody nebyly zastíněny riziky ochrany soukromí a zabezpečení: Privacy-by-Design: zajištění soukromí a začlenění postupů ochrany osobních údajů od koncepce až po realizaci se musí stát výchozím způsobem fungování; Security-

Město	Kyberbezpečnost a ochrana dat – Severní Amerika
	by-Design: správně implementované bezpečnostní procesy a technologie mohou umožnit a chránit aktivity a majetek lidí i podniků. Transparentnost shromažďování osobních údajů. Zajištěné v dokumentu „Oznámení o shromažďování“, které vychází ze zákona o shromažďování informací. Aktualizace zásad a postupů ochrany údajů a kybernetické bezpečnosti: • Navrhování, vyvíjení, pořizování, implementování a vyhodnocování digitální infrastruktury v souladu s kybernetickou bezpečností; • Začlenění ověřovacích procesů do digitální infrastruktury s cílem omezit podvody a počítačovou kriminalitu; • Průběžně odhalovat, vyhodnocovat, spravovat a zmírňovat rizika kybernetické bezpečnosti vyplývající z digitální infrastruktury; • Chránit integritu a bezpečnost všech dat; • Zabudování vhodných auditů, protokolování, monitorování a řízení přístupu; • Vytvoření bezpečné konfigurace digitální infrastruktury; • Šifrování jakýchkoliv dat města, která obsahují osobní údaje; • Posílit kulturu povědomí o kybernetické bezpečnosti. Digitální identita je základní složkou kybernetické bezpečnosti. Město používá tradiční sledovací technologie pro účely zabezpečení a bezpečnosti.
LA	Koordinace inteligentní infrastruktury napříč státním a soukromým sektorem, využívání IoT senzorů. Potřeba sdíleného používání senzorů a kamer. Smart City projekt vždy musí vyřešit obavy týkající se kybernetické bezpečnosti (např. zabezpečení zařízení IoT) a potenciálního neetického využívání infrastruktury Smart City na úkor obyvatel (např. neoprávněné sledování). Revidovat informační bezpečnostní politiky zahrnutí IoT a sdílení infrastrukturních dat. Adaptovat IoT politiky pro sdílené využití senzorů.

Příloha III: Vyhodnocení Smart City strategií pro města v Evropě. Zdroj: vlastní.

Město	Kyberbezpečnost a ochrana dat – Evropa
Londýn	London Datastore je platforma pro veřejná data. Pokud jsou soukromé datové sady přeneseny do Datastore, dojde k zajištění ochrany soukromí a transparentnímu použití dat. Došlo k vypracování a přijmutí souboru standardů. Vytvoření platformy pro testování, získávání, zachycování a ukládání veřejných a soukromých dat z milionů senzorových zařízení. Vyvinutí nového přístupu pro využití silných stránek Londýna jako technologického centra kybernetické bezpečnosti.

Město	Kyberbezpečnost a ochrana dat – Evropa
	Projekt Smart City obsahuje čtyři mise. Druhou misí je uzavření nabídky pro City Data. V tomto bodě dojde ke spuštění London Office of Data Analytics a programu pro zvýšení sdílení dat; strategie kybernetické bezpečnosti s cílem koordinovat reakce na kybernetické hrozby pro podniky, veřejné služby a občany; posílení práva na data a odpovědnost a to, jak využívat veřejná data; podpoře otevřeného ekosystému pro zvýšení transparentnosti. Mayor's Office for Policing and Crime a skupina London Resilience Group vypracuje strategie kybernetické bezpečnosti. Město a jeho veřejné služby musí citlivěji reagovat a spolupracovat pro zajištění lepší kyberbezpečnosti. Londýnské digitální bezpečnostní centrum, které má pomoci při poskytování poradenství a ochrany před kybernetickou kriminalitou.
Paříž	Navyšuje se objem produkovaných dat občany města (kamery, měřiče, detektory pohybu, …), pasivní sběr dat pomocí chytrých telefonů, vozidel a dalších zařízení. Podpora otevřených inovací s partnery města prostřednictvím výměn dat, která jsou zabezpečeny a důvěrné v souladu s doporučeními od Commission nationale de l'informatique et des libertés. Zaměstnanci města musí být také vyškoleni, aby zajistili, že budou moci pomáhat uživatelům při používání digitálních služeb a všemu s tím spojenému. Město musí chránit občany před novými riziky spojenými s digitálními technologiemi – např. bezpečnost dat, ochrana soukromí – regulací, informováním.
Berlín	Stanovení rámcových podmínek pro implementaci specializovaných strategií, jako je digitální začlenění, strategie otevřených dat a kybernetické bezpečnosti. Pro zajištění kybernetické bezpečnosti se technologie musí stát odolnější. Veřejné IT systémy jsou vytvářeny na modulární a open-source bázi a lze je používat samostatně. Základem Smart Berlína je bezpečný a spolehlivý provoz služeb. Kritické infrastruktury musí být navrženy tak, aby byly bezpečné. Aktuální bezpečnostní požadavky v IT a požadavky berlínské ICT architektury jsou implementovány prostřednictvím strategií kybernetické bezpečnosti a zabezpečení dat. Vývoj IT dle standardů: interoperability, modularity, open source a otevřených dat, zabezpečení dat, kybernetické bezpečnosti a orientace na uživatele.

Město	Kyberbezpečnost a ochrana dat – Evropa
Amsterdam	Identifikaci incidentů pomocí kamerových systémů s měřením zvuku. Vše ale bez sběru a ukládání osobních informací. Projekt Responsible Sensing Lab, který testuje a provádí výzkumy, jak začlenit chytré technologie do veřejného prostoru. Patří sem např. tyto projekty spojené s bezpečností, kyberbezpečností a ochranou dat: • Vývoj dashboardu pro zkoumání algoritmů, jak fungují, co potřebují apod.; • Senzory místo kamer pro monitorování pohybů osob, což zajišťuje větší důraz na soukromí jedinců; • Pro větší soukromí, které s přibývajícími kamerami ubývá, využívá město projekt Shuttercam nebo BL0.OM; • Využití MPC, jedná se o kryptografickou metodu pro analýzu dat bez toho, aby měla hrozby pro soukromí.
Kodaň	Využívané technologie: mobilní technologie, optické kabely, Wi-Fi a IoT, které se používají společně se sensory pro sběr a využití dat ve městě. Zpracování datové strategie je potřebné pro vytvoření rámce pro manipulaci s daty, vytvoření Data Hub a definování zásad pro správu dat. Sběr dopravních údajů bude probíhat s plným zohledněním Zákona o osobních údajích, dojde k anonymizování provozních údajů. Data sbírána skrze Wi-Fi, Bluetooth a senzory jsou uložena v šifrované formě. Sběr dat skrze mobilní aplikace je proveden až po odsouhlasení. Pouze relevantní zaměstnanci mají přístup k nezpracovaným datům. Kompletní transparentnost ohledně využití nasbíraných dat.
Praha	Smart Prague 2030 zahrnuje popis využití mobilních technologií, sociálních médií, Big Dat, otevřených dat, IoT, umělé inteligence, robotizace atd. Důraz je kladen na Big Data, otevřená data a umělou inteligenci. Online detekce rizikových jevů ve veřejném prostoru, Wi-Fi a stacionární senzory na lavičkách. Využití senzorů pro řízení dopravy, senzorů v budovách pro vytvoření inteligentních budov. Využití umělé inteligence pro kamerové systémy. Vytvoření bezpečného prostoru pomocí okamžité automatické detekce rizikových jevů. Vytvoření datové platformy pro zobrazení a analýzu dat z projektů Smart City. Ukládání a zpřístupnění všech možných dat ze Smart City projektů. Poskytování otevřených dat soukromému i veřejnému sektoru, za účelem vývoje aplikací. Provádět datovou analýzu pro Smart City projekty. Datová platforma Golemio, která přejímá data z široké škály zdrojů. Data z projektů Smart Prahy jsou zpracovávány touto datovou platformou.

Příloha IV: Vyhodnocení Smart City strategií pro města v Asii. Zdroj: vlastní.

Město	Kyberbezpečnost a ochrana dat – Asie
Tokio	Městské služby využívají data a pokročilé technologie k realizaci „Smart Tokyo“, např. skrze implementaci městských operačních systémů. Otevřenost dat za účelem spolupráce s jinými městskými systémy. Vytvoření datové platformy pro různé typy spolupráce. Dochází ke shromažďování soukromých a veřejných dat. Spolupráce s vládou, soukromými společnostmi atd. a využití nejvyšší úrovně bezpečnostních technologií a řízení. Mobilní internet Tokyo Data Highway a využití umělé inteligence pro vytvoření systémů pro sdílení a využití dat a monitorování bezpečnosti dat. Využití 5G nebo 8K videa pro bezpečnost, systém video analýzy využívající pokročilé technologie. Podpora rozvoje lidských zdrojů jako jsou školení k reakci na bezpečnostní hrozby v kyberprostoru a metaverzním prostoru. Posílení kybernetických bezpečnostních opatření pro Tokijskou vládu, zastupitele a úředníky. Implementování více opatření proti sofistikovaným kyberútokům.
Singapur	Dohled a analýza na místě: kamery, bezpečnostní roboti, integrovaná správa zabezpečení, predikce a detekce rizik/hrozeb. Umělá inteligence pomáhá zlepšit bezpečnostní dohled, detekovat a předvídat potenciální hrozbu/riziko. Existují zásady bezpečného návrhu systémů a aplikací k ochraně vládních systémů kybernetické bezpečnosti. Třístupňový přístup zabezpečení: 1) bezpečnostní politiky ICT, bezpečné technologické architektury a časté bezpečnostní testy; 2) specializovaný tým kybernetické bezpečnosti, monitorování městských systémy 24/7, nezbytné zadržování incidentů, forenzní vyšetřování a obnova, pro reakci na události kybernetické bezpečnosti; 3) spolupráce s komunitou na zátěžovém testování odolnosti systémů. Zákony a zásady na ochranu osobních údajů. Dva právní rámce upravují správu dat ve veřejném a soukromém sektoru. Správa dat třetími stranami veřejných agentur, musí být vysoké standardy ochrany údajů. Jsou vytvářeny každoroční dokumenty aktualizující zabezpečení. Informační strategie zabezpečení obsahuje informace o ochraně dat a zabránění kompromitaci dat, detekci a reakci na incidenty, zvýšení kompetencí, odpovědnosti za ochranu údajů na všech úrovních a zajištění udržitelnosti a odolnosti.

Město	Kyberbezpečnost a ochrana dat – Asie
Soul	Smart Seoul Data of Things infrastruktura Smart City, senzory IoT po celém Soulu pro analýzu dat městských jevů, příprava městské politiky na základě využití relevantních dat. Shromažďování a používání dat o městské bezpečnosti. Vytvoření platformy pro kontrolu zabezpečení a kyberbezpečnosti založené na umělé inteligenci. Zřízení a provoz centra podpory pseudonymizace pro využití dat. Posílení monitorovacího systému proti úniku a zneužití osobních informací. Systém nepřetržité reakce na bezpečnostní a kybernetická rizika prostřednictvím posílení funkcí kontroly a činností na ochranu soukromí. Bezpečnostní řídicí systém založený na umělé inteligenci, vhodný pro prostředí kybernetické bezpečnosti. Seoul Cyber Safety Center – Údržba systému kontroly a reakce kybernetické bezpečnosti v reálném čase pro 72 institucí. Trénink simulace reakce na kybernetický útok a kontrola bezpečnostních zranitelností webových stránek apod. Stanovení zásad bezpečnosti informací, provoz národní kybernetické bezpečnosti.
HKG	Poskytnout studentům středních škol školení v oblasti IT. Nábor IT profesionálů, zejména v oborech datové vědy, umělé inteligence, robotiky a kybernetická bezpečnosti. Vládní cloudová infrastruktura pro poskytování digitálních služeb ve městě. Posílení schopností vlády v oblasti kybernetické bezpečnosti, řešit nová bezpečnostní rizika, usnadnit spolupráci mezi zúčastněnými stranami. Využití nových Big Data analytických platforem pro real-time data, jejich analýzy, přenos a sdílení. Využití veřejných cloudových služeb pro úřady a oddělení ve městě.
Tchaj-pej	Strategický rámec Smart City obsahuje oblast zaměřenou na kyberbezpečnost a IT infrastrukturu. Systém správy digitálních dokumentů Ministerstva zdravotnictví, zajištění jejich bezpečnosti a soukromí. Systému Orbit CMS pro lepší správu webů města, pro výhody jednotného řízení rozhraní, bezpečnosti informací, ovládání, sdílení dat a zálohování dat. Automatické nasazení brány firewall a instalace centrálně spravované autorizace ke stávajícímu firewallu. Inteligentní zabezpečení města slouží k udržování veřejné bezpečnosti, ochraně bezpečnosti provozu, službě lidem, zlepšení reakce na katastrofy. Využití platformy služeb AI Smart Patrol.

Město	Kyberbezpečnost a ochrana dat – Asie
	Přenos zvuku a videa v reálném čase. Rekonstrukce místa činu pomocí ručních a nositelných zařízení, vše se nahrává do zařízení a zálohuje do cloudu. Zavedení identifikace vyžívající umělou inteligenci do kamer a senzorů, upozornění na bezpečnostní hrozby. Technologie sběru dat pro veřejnost založená na umělé inteligenci. Aplikace pro správu zabezpečení IoT, chytrá bezpečnostní řešení pro kampusy a další veřejné prostory, zřízení monitorovacích center atd.
Peking	Posílení kapacity pro správu dat. Zdokonalení systému řízení dat, posílení kapacity platforem pro Big Data. Podpora jednotného sběru a sdílení potřebných sociálních dat. Podpora výstavby zdravotnického, vzdělávacího a průmyslového cloudu. Vývoj hybridního cloudu. Vybudovat služby bezpečnostního provozu cloud computingu a vytvoření komplexního systému zabezpečení s obranou a detekcí ex ante. Služby „jedna síť“ – jednotný vstup, kód, akceptace a zpětná vazba vládních služeb. Posílit bezpečnost nové infrastruktury, bezpečného a spolehlivého prostředí informační infrastruktury. Posílení ochrany bezpečnosti informačního prostoru, monitorování sítě a včasného varování, propojení sítě, koordinace a dispečinku. Posílení bezpečnosti IoT zařízení a zjišťování jejich bezpečnostního stavu. Zavedení systému klasifikace a třídění dat. Technická a řídící opatření pro různé úrovně zabezpečení dat a zlepšení systému monitorování. Sdílení zdrojů veřejných informací, využití kamer pro rozpoznávání obličejů, monitoring a sběr dat, automatizovaný dohled nad domácnostmi a komunitním vybavením.

Příloha V: Vyhodnocení Smart City strategií pro města v Oceánii. Zdroj: vlastní.

Město	Kyberbezpečnost a ochrana dat – Oceánie
Sydney	Inovátor na trhu s informacemi, zavádí bezpečnostních a soukromích protokolů, pro ochranu digitálních práv. Sydney zavedlo politiku otevřených dat. Město využívá „security by-design“ přístup k otevřeným datům. Politiky a správní rámce v oblasti otevřených dat pro lepší zabezpečení a publikování. Bezpečnostní opatření a protokoly v digitální infrastruktuře, aby byla chráněna dlouhodobá integrita dat. Využití dat k mapování zranitelnosti a rizik, vývoj cílených plánů odolnosti a intervencí.

Město	Kyberbezpečnost a ochrana dat – Oceánie
	Odpovědnost jednat jako etický správce při podávání žádosti účinné kontroly zabezpečení a soukromí. Sdílení dat se subjekty v Sydney, pohotovostními službami, vládními agenturami, veřejnou službou a stranami odpovědnými za kritickou infrastrukturu. Zaměření na řízení kybernetických rizik, pokročilé monitorování a skenování hrozeb. To je zásadní pro zajištění účinné reakce na narušení kybernetické bezpečnosti, minimalizaci škod a zajištění rychlé obnovy.
Melbourne	Rozhodovací a konzultační procesy budou otevřené a transparentní. Otevřená vládní data jsou ve formátech, které umožňují inovativní využití. Data budou bezpečně spravována pro ochranu soukromí firem a jednotlivců. Shromážděná data budou zabezpečena za účelem ochrany. Zákon Victoria's Privacy and Data Protection Act a zásady ochrany osobních údajů řídí, jak nakládat s osobními údaji. Dodržování ochrany osobních údajů je součástí programu pro zaškolení zaměstnanců. Vyhrazený tým pro ochranu osobních údajů.
Canberra	Neustálý vývoj systémů kvůli ochraně před kyberútoky. Mnohostranný přístup k zajištění bezpečnosti: zastavení přístupu ovládacími prvky jako je firewall a monitorování detekce, silná autentizace a monitoring procesů, monitorování a pravidelné aktualizace systémů, ochrana uživatelů, rychlé nalezení a zvládnutí problémů, vzdělávání uživatelů o bezpečnosti a spolupráce a sdílení informací o hrozbách. Kybernetická strategie při zachování a posílení zásad ochrany osobních údajů. Plán konsolidace a správy dat z kamer a senzorů a jejich využití k ochraně obyvatel.
Wellington	Rozvoj ICT infrastruktury. V rámci informací, dat a dostupnosti dojde k použití více open source přístupů. Vytvoření online informačního hubu, který budu především založen na datech z otevřených zdrojů a bude využívat data ze senzorů v reálném čase.

Příloha VI: Data a kyberbezpečnost v rámci projektů pro ekonomii. Zdroj: vlastní.

Město	Data a kyberbezpečnost v rámci Smart Economy
NYC	Publikování a sdílení ekonomických dat pro informování obchodních rozhodnutí. Měsíční zprávy o datech, abychom mohli měřit sílu ekonomiky města – od statistik práce přes trendy v odvětvích až po obsazenost nemovitostí.
Washington DC	Senzory, integrace a datová analýza. Big Data analytika, management a zásady, hlavně v oblastech citlivých dat, příklady: finanční prediktivní analytika a analýza úvěrových dat. Udržovat a pravidelně aktualizovat statistické údaje, dělení dat dle rasy. Maximalizujte využití technologií a údajů o trhu práce pro zaměstnání, trénink a vzdělání.
Chicago	Vytvoření plánu nástupnictví ke zmírnění rizik spojených s odchodem do důchodu – využití dat hodnocení dovedností z hodnocení současného stavu k identifikaci potenciálních kandidátů na obsazení prioritních rolí.
SF	Pomocí platforem městské infrastruktury – sítě, cloudu a dat – využití nových investicí a zjednodušit náklady na údržbu. Datové týmy DataSF se zabývají celoměstským úsilím zachytit plný potenciál dat, obchodní analytika a rozhodování v ekonomice.
Tor.	Dokumentace a sdílení osvědčených postupů a účast v programu sběru údajů o nákladní dopravě.
LA	Zavedení celoměstské 5G sítě pro možnost připojení k internetu a využití dostupných dat. Iniciativa Data Angels – nadšenci do civilních technologických dat.
Lon.	Použití digitální technologie, dat a datových sil přinese efektivitu, včetně úspor nákladů v různých oblastech služeb.
Paříž	Pomoc zúčastněným stranám strukturovat jejich obchodní modely prostřednictvím městských otevřených inovačních programů „DataCity“. Vypuštění finančních a sociálních dat, obsahuje přes 201 datových sad.
Berlín	Umožnit komunitně orientované využívání veřejných údajů různými aktéry, jako jsou podniky, akademická obec a občanská společnost.
Amsterdam	Strategie Amsterdam Circular Economy, která je založena na datech a vstupech z „Doughnut workshop“, které zahrnují obyvatele a organizace Data shromážděna k odhadu řádové velikosti materiálových toků. Ověření a obohacení dat ve spolupráci s průmyslovými asociacemi, sítěmi a jednotlivými společnostmi.

Město	Data a kyberbezpečnost v rámci Smart Economy
Kodaň	Flow data solutions report shrnuje tržní dialog o řešeních tokových dat. Kontakt s 30 firmami, které podali návrhy na inovativní řešení v rámci toku dat po městě, v kategoriích: tele data; Wi-Fi senzor; senzor počítačového vidění; aplikace pro průzkum dopravy.
Praha	Big Data v turismu řízení toku turistů a návštěvníků: funkční automatický sběr agregovaných dat (geografická, sociálních sítě, kreditní karty, senzory a kamery); řízení turistického ruchu na základě dat. Zveřejňování dat pro vývoj aplikací.
Tokio	Tokijské centrum na podporu oběhové ekonomiky pro funkce jako je šíření informací, výměnné salony, konzultace a párování a komunitní podpora podnikání. Vytvoření společné spouštěcí databáze a poskytnutí doma i v zahraničí.
Singapur	Zajistit, aby konektivita, platformy, data a další infrastruktura dobře podporovaly růst digitální ekonomiky. Využití Big Dat, cloud computingu, robotiky nebo strojového učení. Větší efektivita a účinnost pro podniky ať už jde o využití senzorů a dat k lepšímu řízení provozu nebo sledování bezpečnostních hrozeb. Pravidla pro přeshraniční ochranu soukromí a Uznávání soukromí pro zpracovatele zajišťují, aby certifikované organizace měly zásady ochrany dat.
Soul	Seoul Startup Hub – platforma na základní data více než 5 000 startupů, 183 investorů a akcelerátorů. Obsahuje více než 5 000 podnikových dat. Vyhledání podniků se sídlem v Soulu slibujících investice a vytvoření databáze.
HKG	Systém pro správu informací a dat z Cash Payout Scheme. Sledování provádění proinovační politiky státních zakázek. Spolupracování se Shenzhenem pro IT podniky, univerzity a výzkumná a vývojová centra z Hongkongu, zámoří a pevniny.
Tchaj-pej	Taipei City Multi-field Kiosk je veřejná služba, které také sbírá městská data. Obchodní sledování prostřednictvím analýzy velkých dat a zobrazení například v Taipei City Mall, Qingguang Market, Front Station Metro Mall a další.
Peking	Institucionální rámcový systém „1+3+N“, který hraje demonstrativní roli v několika oblastech, jako je Smart City, výměna dat a inteligentní síť. Beijing International Data Exchange zavedla a zlepšila obchodní formu a platformu založenou na právech duševního vlastnictví a spuštění 1 364 datových produktů. Systém sdílení dat a obchodní koordinace založený na informačních technologiích.

Město	Data a kyberbezpečnost v rámci Smart Economy
Sydney	Platformy pro integraci a analýzu business dat. Standardy v digitální infrastruktuře, které usnadňují tok dat a přístup stakeholderů k datům. Informační ekonomika buduje důvěryhodné prostředí na podporu sdílení dat. Využití IoT senzorových sítí pro sběr dat, která pomáhají podnikům. Data a digitální technologie mohou pomoci řídit toky materiálů a majetku po městě.
Melbourne	City Intelligence Hub otevřená datová platforma, digitalizuje operace prostřednictvím digitálních dvojčat a modeluje přijetí Průmyslu 4.0. Vylepšení knihoven, otevřená datová platforma, otevřená inovační agenda, rozvoj dovedností a vzdělávací programy.
Can berr	Schopnost ukládat a analyzovat obrovské množství dat vede k rostoucí schopnosti vytvářet nové poznatky a obchodní příležitosti.
Wellington	Odvětví služeb založených na znalostech, která dodávají produkty – obvykle ve formě velkého množství elektronických dat – pomocí infrastruktury ICT, jsou součástí „ekonomiky bez tíže“. Stanovení sazeb dle zákona a dat z databáze ratingových informací.

Příloha VII: Data a kyberbezpečnost v rámci projektů pro lidi. Zdroj: vlastní.

Město	Data a kyberbezpečnost v rámci Smart People
NYC	Zvýšit datovou gramotnost a školení o používání portálu NYC Open Data. Poskytovatelé digitální gramotnosti po celém městě také nabízejí školení a podporu v oblasti ochrany soukromí a dat online.
Washington DC	Využití sběru dat ohledně žití dle rasy osoby a vytvoření zásad v kontextu rasové spravedlnosti. Sledování společenských, ekonomických, komunitních a realitních trendů a dat, které mohou vyžadovat akce týkající úpravy zásad.
Chicago	Zpětná vazba a data pro upřednostnění digitálních služeb. Komunikační nástroje, průzkumy k identifikaci priorit pro digitální služby z pohledu obyvatel.
SF	Inkluzivní a na datech založený program na posílení postavení komunity. Závazek zpřístupnit, objevit a použít otevřená, strojově čitelná data veřejností k podpoře inovací a zapojení obyvatel.

Město	Data a kyberbezpečnost v rámci Smart People
Toronto	Spolupráce s poskytovateli služeb pro seniory a provincií na řešení nedostatků v datech, což zlepší koordinaci služeb pro seniory. Vývoj systému koordinovaného přístupu, který využívá data k upřednostňování lidí s nejvyšší potřebou.
LA	Objektivní analýza a rozhodování založené na datech pro plánování měst pro lepší čtvrti a žití.
Londýn	Přijetí nových přístupů prostřednictvím spojení lidí, technologií a dat. Sběr dat o lidech, když se registrují do komunit, využití demografických dat a oblasti jejich zájmu.
Paříž	Instalace GPS čipů na vozy pro svoz odpadu, aby bylo možné sdílet shromážděná data v reálném čase pro lepší plánování a možnost upozornění občanů na svoz odpadu.
Ber.	Posílení práva digitálních občanů a dodržování předpisy o ochraně osobních údajů.
Amsterdam	Projekt AMdEX s cílem poskytnout lidem větší kontrolu nad jejich daty prostřednictvím zabezpečené, důvěryhodné a neutrální infrastruktury, která umožňuje sdílení dat za specifických podmínek: • Poskytnout větší kontrolu nad osobními daty; • Učinit sdílení dat atraktivnějším.
Kodaň	Sběr dat, kde studenti škol budou přímo využívat digitální technologii. Díky možnosti využití Big Dat společnostmi, vznikají nové pracovní pozice.
Praha	Detekce rizikových jevů, naučení vzorců chování lidí pomocí umělé inteligence, která zkoumá data z kamerových systémů.
Tokio	Vizualizace, sdílení a analýza dat ze škol. Odstraňte obavy ohledně komunikace a dat v případě katastrofy. Použití Big Dat k prevenci demence. Chytré hodinky starším lidem a následné sbírání dat pro vývoj aplikací na podporu zdraví starších občanů.
Singapur	Datové analýzy a další technologie budou použity k lepšímu pochopení a zapojení obyvatel. Využití robotiky pro pečování o lidi, využití datové analytiky pro zlepšení jejich funkčnosti.

Město	Data a kyberbezpečnost v rámci Smart People
Soul	Spravování zdraví pomocí chytrých zařízení, získávání zdravotní konzultace a odborné péče na základě zdravotních dat uložených v chytrých zařízeních. G-Valley zahrnuje nově vybudovanou laboratoř lékařských dat; asistované využití lékařských dat a analýzy založené na umělé inteligenci.
HKG	Snaha o udržení a přilákání profesionálu v oblastech data science, umělé inteligence nebo kyberbezpečnosti. Vybudování znalostní společnosti na podporu budoucího rozvoje IT.
Tchaj-pej	CooC-cloud technologie umělé inteligence pro shromáždění interaktivních dat pro analýzu, výpočty, diagnostiku stavu učení studentů v reálném čase. Platforma služeb a dat pro sportoviště o sportovcích. Textový zákaznický servis má také horkou linku pro dotazy a je vylepšen znalostní databázi.
Peking	Kultivovat trh datových prvků Digital Human, jedná se o 3D virtuální verze a modely lidí. Chytrý terminál péče o seniory na jedno kliknutí, který přiřadí sanitku dle GPS lokace a databáze seniorů. Sběr dat ze sítě: Weibo nálada, vyhodnocení scénických spotů, spotřebitelské recenze, dopravní zácpy, OD trasy atd.
Sydney	Technologie a data na podporu a posílení komunit v jejich každodenním životě. Použití dat k identifikaci segmentů komunity. Využití IoT senzorových sítí pro sběr dat, pro efektivnější management davu nebo snížení čekací doby. Data řídící monitorování, predikce a dopady šoků a stresu.
Melbourne	Sběr a analýza dat ohledně bezpečnosti a pohody občanů. Základní data ohledně stížností, kriminality a grafitů nebo odpadků. Získávání dat o rozmanitosti pro budoucí audity na pracovišti, data týkající se kulturní identity, postižení, jazyků, sexuální orientaci, místa narození a náboženství.
Canberra	Data k identifikaci lidí s různorodými a komplexními potřebami, aby bylo zajištěno, že dostanou včasné a bezproblémové služby. Spolupracujte s lidmi v komunitě, porozumění rozsahu a síle postojů k soukromí a sdílení dat. Zůstat s nimi v kontaktu pro vyvážené rozhodování o využití dat. Jednodušší způsoby přístupu k datům a jejich interpretaci pro komunity.
Well.	-

Příloha VIII: Data a kyberbezpečnost v rámci projektů pro vládu. Zdroj: vlastní.

Město	Data a kyberbezpečnost v rámci Smart Governance
NYC	Lokální zákony o vytvoření Chief Privacy Officer, celoměstský výbor pro ochranu soukromí a ochranný rámec, open Data zákon. Úřad starosty pro informace o soukromí, který ochraňuje identifikující data občanů a maximalizuje sdílení dat mezi agenturami.
Washington DC	Datové vrstvy veřejných zařízení veřejně dostupné. Využití analytických nástrojů a dat. Open Data portál. Sběr dat ohledně veřejných škol, knihoven, odezva zdravotnické služby, kanalizace nebo kapacita veřejné dopravy. Aktualizace a rozšiřování databáze správy nemovitostí.
Chicago	Návrh a implementace datové a analytické strategii. Posílení technologické infrastruktury, integrace a bezpečnosti. Přístup cloudové migrace.
SF	Průběžný sběr dat, informací a analýz účinnosti. Vysoce vyspělá politika a zákon o otevřených datech. Sběr dat kombinací vodivých smyček, magnetických senzorů, radaru, videokamer a stropních spínačů.
Tor.	Datová centra, open data portál. Automatizovaný kanál publikací, který bude zohledňovat soukromí a zabezpečení.
LA	Investice do infrastruktury, digitálních služeb a datových nástrojů. Zapojení komunity a poskytnutí kritické ochrany zabezpečení soukromí a dat. Smart City Data Tools & Practices, které umožňují efektivní sdílení informací.
Londýn	Volný přístup k Londýnským datům. Identifikace dat, které jsou nutné pro růst Londýna.
Paříž	Analýza Big Dat, datová centra a open data portál. Využití dat shromážděných ze senzorů instalovaných na Place de la Nation.
Berlín	Využití dat jako informačního základu pro politiku rozvoje měst. Otevřeně přístupné, interoperabilní databáze. Berlínská otevřená data strategie. Posílit práva digitálních občanů a dodržovat předpisy o ochraně osobních údajů.
Amsterdam	Politiky a zásady tvořeny v právním a systému, vytvoření databáze a sběr dat. Na základě dat stanovit priority oběhové politiky. Zdroje dat a metodika jsou veřejně dostupné. Město poskytuje cílené znalosti a datové služby.

Město	Data a kyberbezpečnost v rámci Smart Governance
Kodaň	Data o tocích se využijí při rozvoji a plánování. Sdílení veřejných dat a Smart City Data Hub. Anonymizované data v souladu s Dánskou a EU legislativou, včetně GDPR skrze bezpečný přenos dat, nebo přímá manipulace s daty na zařízení.
Praha	Využití Big dat a otevřených dat. Využití IoT a tedy generování a přísun dat do datových center. Centralizované zajištění datové infrastruktury.
Tokio	Vytvoření Tokyo Data Highway a využití Big Dat a AI pro vytvoření systému sdílení a využití dat. Otevřenost dat za účelem spolupráce s jinými městskými operačními systémy. Vytvoření 3D modelu města, které využívá a zpracovává real-time data. Zvážení AI pro monitorování práce potvrzování dat.
Singapur	Vytvoření zásad, předpisů a norem pro zajištění prostředí pro datovou inovaci. Investice do AI, data science a IoT. Zákon o ochraně osobních údajů a dat.
Soul	Big Data Campus je platforma pro podporu dat a infrastruktury pro analýzu Big Dat. Senzory IoT pro analýzu různých dat městských jevů. Zavedení IoT městského systému pro správu dat pro sběr a používání dat IoT senzorů o životním prostředí, bezpečnosti atd.
HKG	Webový portál otevřených dat, open data zásady. Platforma pro analýzu Big Dat, přenos dat v reálném čase a sdílení. Platforma iAM Smart, která využívá e-služby založené na datové analýze a AI. Otevřená data ve veřejném i soukromém sektoru.
Tchaj-pej	Správa řízená daty. Taipei Urban Intelligence Center odvozuje poznatky z rozsáhlých městských dat a umožňuje chytřejší a lepší správu města.
Peking	Národní Big Data centrum. Podpora otevřeného přístupu k datům. Průzkumy přeshraničního toku dat a zřízení inovačního centra pro přeshraniční bezpečnost dat. Průběžné zkoumání pravidel ochrany datových práv.
Sydney	Chytrá transformace města pomocí sdílení dat, znalostí a poznatků. Open data. Vytvořený rámec, který umožní sdílení znalostí, dat, zdrojů a zkušeností. Rámec v souladu s ISO 37106:2018.

Město	Data a kyberbezpečnost v rámci Smart Governance
Melbourne	Otevřená vládní data s více něž 100 různými datovými sadami. Data budou bezpečně spravována pro ochranu soukromí firem a jednotlivců. Vytvoření Melbourne Testbed.
Canberra	Shromažďování a chránění transparentních dat. Využití dat zefektivní funkce vlády. Zlepšovat sdílení informací a dat v rámci vlády. Soukromí, bezpečnost, transparentnost a etika při datových a digitálních činnostech, opírajících se o přísná pravidla správy. Open a real-time data, být transparentní.
Wellington	Zpřístupnění a shromáždění dat, aby je občané, výzkumní pracovníci, investoři a návštěvníci mohli používat k vlastním rozhodnutím a plánům. Data z otevřeného zdroje. Data ze senzorů v reálném čase.

Příloha IX: Data a kyberbezpečnost v rámci projektů pro mobilitu. Zdroj: vlastní.

Město	Kyberbezpečnost v rámci Smart Mobility
NYC	Využití IoT zařízení a dat pro analyzování dopravních vzorců, počítání cyklistů a sledování vozidel vlastněných městem. Sledování vozidel pro agentury a autobusové společnosti. Sběr dat ohledně pozice, využití, opravy, havárie, rychlosti, využití pásů a volnoběhu. Anonymizování dat pro bezpečnost. Citlivost dat zaručuje soubor interních bezpečnostních zásad a postupů.
Washington DC	Dynamické parkovací hodiny, připojené signály a digitální senzory. Využití dat o vzorcích cestování pro zlepšení tranzitních služeb. Využití autonomních vozidel, jejich zabezpečení v rámci kyberbezpečnosti.
Chicago	Nové přístupy budou vycházet z potřeb a budou řízeny daty. Využití dat a technologií ke zlepšení ulic a infrastruktury. Zpřístupnit data a být transparentní. Databáze stavu chodníku a zlepšení programu údržby chodníků.
SF	Kritéria založená na datech, podněcují rozšíření sdílené mobility. Model dopravní platformy bude měřit dopady s využitím zavedených a dostupnějších zdrojů dat.

Město	Kyberbezpečnost v rámci Smart Mobility
Toronto	Nové technologie pro vylepšenou správu dat dopravní sítě, sběru, analýze a monitorování.
LA	Data k upřednostnění dopravních rozhodnutí, která usilují o rovnost v oblasti bezpečnosti, veřejného zdraví, přístupu, sociálních výhod a ekonomických výhod. Koridory byly vybrány na základě analýzy založené na datech.
Londýn	Využití technologií, kamer a dat pro detekci incidentů, upozornění na kolony a snížení nebezpeční v transportu. Transportní aplikace vytvořené z open dat. Redukce lehké nákladní dopravy pomocí open dat, technologií a business modelů.
Paříž	Autolib data jsou zprostředkována otevřeně. Zpřístupnění real-time dat o veřejné dopravě. Monitorování provozu pomocí nástrojů a zdrojů dat, kamer, GPS a operátorů.
Berlín	Vývoj datové platformy pro mobilitu. Informace v reálném čase jsou veřejně dostupné – zastávky, nádraží atd. Použití automaticky generovaných otevřených dat.
Amster.	Projekt Mobility Portal shromažďuje data od poskytovatelů v reálnem čase. Veřejné data ve strukturované podobě. Identifikace „Data 15“ neboli 15 nejdůležitějších typů dat pro digitalizaci, včetně parkování, logistiky nebo cyklistiky.
Kodaň	Shromažďování dat z parkování, dopravních situací a incidentů. Pomocí dat, algoritmů a strojového učení předpovídat volná parkovací místa. Tyto data jsou volně dostupná pro providery a developery parkovacích služeb.
Praha	Využití inteligentní mobility, která je založena na datech: chytré semafory, založené na datech ze senzorů a real-time řízení; sběr a využití dat v parkování, možnost vidět volná místa; informování pasažérů a zrychlení dopravy.
Tokio	Projekt podpory sociální implementace Mobility as a Service s cílem podpořit vytváření nových služeb, které využívají Big Data a sběr dat.
Singapur	Vylepšení veřejné dopravy pomocí dat. Otevřená transportní data, datová analytika. Úřad pro pozemní dopravu shromažďuje data, která využívá pro vylepšení transportace. Příkladem jsou anonymizovaná data z karet jízdného, identifikace hotspotů dojíždějících nebo využití analýzy real-time a historických dat pro řízení dopravy.

Město	Kyberbezpečnost v rámci Smart Mobility
Soul	Využití dat a v městské hromadné dopravě, autobusové dopravě apod. Parkovací politika s pomocí dat v reálném čase, sběru dat, GIS, Big Dat a umělé inteligence. Využití Big Dat pro vyřešení nerovnováhy využití kol po městě.
HKG	Real-time informačního příjezdový systém, provozovatelé musí otevřít data. Vyvinout systém analýzy dat o provozu. Využití datové analytiky.
Tchaj-pej	Smart parking meters, technologie rozeznávání značek, detekci vjezdu a výjezdu vozidel a jejich SPZ pro zjištění parkovacích údajů. Sběr dat o dopravě. Používá IoT a jízdenky k vytvoření datového modelu toku cestujících.
Peking	Datový soubor o autonomním řízení se synergickými vozidly. Městská vozidla se mění na městské snímací platformy – shromažďování informací, jako je městské tepelné zobrazování, znečištění ovzduší atd.
Sydney	Analýza dat pro informování o optimální rozdělení prostoru ulic a rozvoji infrastruktury pro chodce.
Melbourne	Analýza dat ukazuje zvýšený podíl cyklistů, vede k investicím do cyklistické infrastruktury. Zachycování a sdílení dat o pohybu, jezdě na kole a použití veřejné dopravy. Pozemní senzory podporují parkování a shromažďování údajů o obsazenosti.
Canb.	Neustále statistiky dat generovanými autobusů, lehkých železz, silnic atd. Cashless ticketing – informace v reálném čase a umožní společnosti Transport Canberra činit rozhodnutí o návrhu sítě na základě dat.
Wellington	Databáze o množství, umístění a typu parkovacích míst. Databáze pokrývá všechny typy parkovacích míst. Mapovací aplikace Access Map obsahuje informace o přechodech, chodnících a nájezdech.

Příloha X: Data a kyberbezpečnost v rámci projektů pro prostředí. Zdroj: vlastní.

Město	Kyberbezpečnost v rámci Smart Environment
NYC	IoT pro sledování dat ohledně kvality vzduchu, teploty a další data o počasí. Sběr dat z vozidel ohledně kvality vzduchu, teploty a vlhkosti.

Město	Kyberbezpečnost v rámci Smart Environment
Washington DC	Databáze pro mapování nových vysazených stromů, pomocí GIS. Zdokonalení získávání a udržování dat o živočiších a rostlinách. Hlavně o vzácných a chráněných druzích. Sběr dat o ovzduší a publikování mezi lidi.
Chicago	Monitorování oblastí a provádění průzkumů. Vytvoření osvědčených postupů pro projekty obnovy měst a generování vědeckých dat. Vytvoření online systému pro sdílení dat bez výzkumníky.
SF	Každoroční shrnutí ročních energetických srovnávacích testů ohledně budov.
Toronto	Data o různých složkách systému přírodního dědictví, napomáhá k jeho rozvoji. Navržené osvětlení pomocí dat, aby zajišťovalo ochranu a zároveň ho nebylo mnoho.
LA	Shromažďování dat k identifikaci nejúčinnějších programů ohledně kvality vody. Analýza dat o energii pro vytvoření energetické účinnosti.
Londýn	Využívání dat a technologií k vývoji nových trhů pro londýnský odpad. Otevřená data o výkonu, spotřebě a životním prostředí – energie, voda, odpady, znečištění.
Paříž	Snižování energie v budovách a shromažďování energetických dat. Centrum pro sběr odpadu a sanitaci, které využívá analýzy dat, monitorování apod.
Ber.	Využití nových technologií, dat a umělé inteligence pro udržení a zlepšení prostředí – snížení emisí, spotřeby zdrojů, elektřiny, tepla, potravin apod.
Amster.	Shromážděná data poskytují pohled na množství materiálů pohybujících se městem a dopad na životní prostředí. MicroLAN měření kvality vody nebo Public Eye shromažďující davová data.
Kodaň	Optimalizace využití vozidel na základě GPS dat a sdílení zařízení. Online nástroj specifikuje emise pomocí klíčových, dynamických zdrojů dat, takže obce nemusí shromažďovat data k vizualizaci svých emisí skleníkových plynů.
Praha	Využití senzorů a dat ve veřejných budovách za účelem sledování stavu budovy, znečištění a hospodaření s energiemi. Využití chytrého osvětlení, které využívá real-time data ze senzorů a koriguje osvětlení.

Město	Kyberbezpečnost v rámci Smart Environment
Tokio	Sledování a sbírání dat o hladině vody a prevenci povodní. Snížení uhlíku podporou aktivního úsilí zveřejňováním a využíváním efektivnějších statistických dat.
Singapur	Smart Nation Sensor Platform je celostátní platforma, která využívá senzory ke sběru základních dat. Bezdrátová síť senzorů pro sběr dat o vodě téměř v reálném čase. Senzory a SW v osvětlení pro sběr dat o vzorcích lidského pohybu.
Soul	Aktualizace Smart Safety City Seoul a vytvoření Smart Seoul Safety Network pomocí dat z kamer. Vytvoření Wi-Fi sítě pomocí analýzy Big Dat o výskytu obyvatel.
HKG	Platformu pro analýzu Big Dat v rámci Hospital Authority´s Data Collaboration Lab. Vytvoření chytrého osvětlené, které je schopné sbírat real-time data.
Tchaj-pej	Databáze počasí a vodní hladiny – déšť, řeky, kanály a počasí. Taipei Feitsui Reservoir Administration integrovala interní i externí databáze a přijala analýzu velkých dat a technologie umělých neuronových sítí.
Peking	Chytré osvětlení, které má audio a video monitoring a také obsahují senzory pro počasí a prostředí. Monitorování a sběr dat, provádění analýz a využití real-time dat anebo Big Dat pro: anomálie dat mikrostanic, data silničního prachum znečištění prostředí atd. Smart Heiding park obsahuje možnost skenování obličeje za účelem zobrazení dat.
Sydney	Data-řízený monitoring, predikce a řízení podmínek města. Data v reálném čase o ukazatelích městského zdraví, včetně emisí, vody a ovzduší.
Melbourne	Data a poznatky ke zkoumání veřejného prostranství, uspokojení potřeby a zlepšit zkušenosti občanů. „Smart park“ – vyjádření prostředí a jeho využití prostřednictvím dat a technologií. HeatSens je „chytrý“ digitální nástroj pro sběr dat, sledování změn a určování potenciálních tepelných nebezpečí.
Canb.	Zlepšit zdraví vodních cest ACT integrací dat z více zdrojů a senzorů, včetně srážek, průtoku toků a kvality vody.

Město	Kyberbezpečnost v rámci Smart Environment
Wellington	Nařízení o pevných odpadech tvoří příležitost k shromažďování dat. Poplatek za likvidaci odpadu s cílem zlepšit datové systémy, prozkoumat pobřežní recyklační závody a financovat projekty. Rada bude spolupracovat s průmyslem, partnery, provozovateli a komunitou, aby shromáždila přesná data pro měření odpadů ve městě.

Příloha XI: Data a kyberbezpečnost v rámci projektů pro žití. Zdroj: vlastní.

Město	Kyberbezpečnost v rámci Smart Living
NYC	Chytré osvětlení reaguje na kolemjdoucí a sbírá data, zda prošla osoba okolo skrze princip „privacy-by-design“ a pasivní infračervené senzory. IoT data pro správu systémů budov a podporu účinnosti energie.
Washington DC	Data o bezpečnosti, zaměstnání, příjmu, vzdělání a apod. pomáhají řízení investic pro výstavby. Management dat pro existující byty a vývojová místa. Data pro zvážení příjmů a rasových charakteristik čtvrtí. Sběr a udržování dat o prázdných bytech a budovách.
Chicago	Monitorování účinnosti budov a prosazování standardů. Zprávy o energetice budov, vyhláška ospravedlňuje sdílené těchto dat o budovách. Veřejné sdělování dat ohledně využití vody v budovách. Kvalita dat je zaručena potřebou každé 3 roky potvrzovat pravdivost a validitu dat.
SF	Otevřený datový portál i pro více nezpracovaná data z prvků infrastruktury v reálném čase.
Tor.	Vybudování integrovaného systému poskytování služeb a zavedení protokolů pro sdílení dat v rámci sektoru bydlení a bezdomovectví.
LA	Analýza dat pro platformu Homelessness využívající zabezpečené datové sady hostované v cloudu poskytovaným odděleními města.
Lon.	Využití dat ze senzorů v městské infrastruktuře pro nové inovace.
Paříž	Instalace senzorů a nových systémů přenosu dat uvnitř budov. Urbanismus řízený daty k upřednostňování voleb a objasňování rozhodnutí. Vybavení budov pro získávání dat a analýzu chování při používání
Ber.	Snaha o snížení CO2, kvůli tomu se využívá monitoring, sběr a využití dat.

Město	Kyberbezpečnost v rámci Smart Living
Amster.	Projekt PAUL ohledně fyzické aktivity občanů města a jejich zdraví. Vytvoření aplikace, její použití pro shromažďování dat o fyzické aktivitě a poloze uživatelů. Využití data mining technik.
Kod.	Vybudování potřebné expertizy, sběr dat o novostavbách města a systematické sledování toho, zda budovy splňují požadavky města ve výběrových řízeních.
Pra.	Měření kvality ovzduší a sběr přesných a aktuálních informací a dat o stavu pomocí stacionárních i mobilních senzorů.
Tokio	Vytvořit model městského rozvoje založený na datech. Rozvoj města pomocí autonomní mobility, 5G sítě a využití Big Dat.
Singapur	Počítačová simulace a analýza dat k plánování a navrhování technologií města. Chytré technologie se používají ke shromažďování a analýze dat o nemovitostech za účelem optimalizace cyklů údržby a předcházení problémům.
Soul	Posílení monitorování v reálném čase o zdraví, bezpečnosti, zranitelnosti osob, jako jsou starší občané. Real-time monitorování starších občanů. Zřízení energetického informačního centra pro integrovanou správu rozptýlených a segmentovaných energetických dat.
HKG	Vývin společné infrastruktury prostorových dat a zřízení geoprostorové laboratoře v rámci zdravotnictví.
Tchaj-pej	Technologie IoT, sběr dat regionálního určování polohy, rizikových oblastí, automatické hlášení nehod a vitálními funkcemi na staveništích. Platforma sběru a analýzy dat pro zlepšení kvality a efektivity provozu a služeb údržby. Stanovení datových zařízení a vybavení budov. Smart meter AI big data analytics – analýza dat energie budov.
Peking	Nová data a nové technologie jako prostředky s cílem nulové spotřeby energie, udržitelnosti a soběstačnosti. Sbírat data o hmotném prostoru. Sbírat data o obyvatelích pomocí senzorů, mobilních aplikací a snímků dálkového průzkumu pro vývoj budov, příkladem jsou vertikální farmy.

Město	Kyberbezpečnost v rámci Smart Living
Sydney	Data k mapování zranitelností, rizik a vzájemných závislostí v celé místní oblasti. Analýza dat o městských podmínkách před a po katastrofě pro lepší obnovu. Schopnosti strojového učení mohou analyzovat data shromážděná ze senzorových sítí za účelem monitorování kvality městských podmínek a automatizace rozhodování.
Melb.	Využití dat pro tvorbu podmínek prostředí, GIS data pro požadavky na praktické vyplnění prostoru. Closed-circuit television a datové služby jsou obvykle ve vedení města.
Canberra	IoT data v celoměstských modelech, pro fungování a plánování změn a zlepšení odolnosti a udržitelnosti. Uložení a archivace všech geoprostorových dat na platformě, která podporuje interní analýzu a kritické rozhodování. 3D digitální data pro infrastrukturu, budovy a nemovitosti.
Well.	-

Příloha XII: Výsledky prvního kola dotazníku metody Delphi s vyznačenými nejlepšími a nejhoršími doporučeními. Zdroj: vlastní.

RECOMMENDATIONS	Avg.	Standard Deviation	Expert responses						
			n. 1	n. 2	n. 3	n. 4	n. 5	n. 6	n. 7
HW AND SW MEASURES	**2,83**	**0,37**	**3**	**3**	**3**	**2**	**3**	**3**	**N/A**
On-site surveillance and analytics – use of cameras with support for analysis, AI, facial or movements recognition …	**2,43**	**0,49**	2	3	3	2	2	3	2
Access to the facility using automatic visitor registration	**2,14**	**0,35**	2	2	2	2	2	3	2
Use of activity detection tools	**2,00**	**0,00**	2	2	2	2	2	2	2
Multi-factor authentication	**2,86**	**0,35**	3	3	3	2	3	3	3
Email protection tools – built-in email scanning, phishing, and internet security protection	**2,86**	**0,35**	3	3	3	2	3	3	3
Security requirements for SW and his development cycle	**2,00**	**0,76**	1	2	2	1	3	2	3
Use of biometric systems	**2,57**	**0,49**	2	2	3	2	3	3	3
ORGANIZATIONAL MEASURES	**2,83**	**0,37**	**3**	**3**	**3**	**2**	**3**	**3**	**N/A**
Centralized provision of data infrastructure	**2,14**	**0,35**	3	2	2	2	2	2	2
A secure communication network at the level of security components of crisis management	**2,57**	**0,49**	3	2	2	2	3	3	3
Implementation of strict privacy laws and policies to protect sensitive data	**3,00**	**0,00**	3	3	3	3	3	3	3
Conduct regular data security risk assessments	**2,71**	**0,45**	3	3	3	2	3	3	2
Cyber security at the top of priorities (financial resources, people, infrastructure)	**2,29**	**0,45**	3	2	2	2	2	3	2
Use Privacy Impact Assessment when introducing new technologies	**2,71**	**0,45**	3	2	3	3	3	3	2
Have a schedule for app updates, do them in a timely manner	**2,43**	**0,73**	3	3	3	2	2	3	1
Setting requirements for cloud and service providers	**2,29**	**0,45**	3	3	2	2	2	2	2
Development of a harmonized framework for cyber security	**2,57**	**0,49**	2	3	3	2	3	3	2

	Have a post-breach and response plan in place	**2,43**	**0,49**	2	3	3	2	2	3	2
DATA PROTECTION POLICIES		**2,67**	**0,47**	**3**	**3**	**3**	**2**	**2**	**3**	**N/A**
	Minimize the attack surface, i.e. the various points through which an actor can compromise data security	**2,29**	**0,45**	2	2	3	2	2	3	2
	Collect and store data only where necessary	**2,29**	**0,45**	3	2	2	2	2	2	3
	Minimize data downloads to end devices	**1,86**	**0,35**	2	1	2	2	2	2	2
	Have access to data only for the necessary and permitted action	**2,43**	**0,49**	3	2	2	2	2	3	3
	Creating backups of systems and data	**2,86**	**0,35**	3	3	3	2	3	3	3
	A privacy-by-design approach	**2,71**	**0,45**	3	3	3	3	2	3	2
	Zero trust architecture	**2,29**	**0,45**	2	2	2	3	2	3	2
	Regularly run penetration tests	**2,43**	**0,73**	2	3	3	2	3	3	1
DATA SECURITY DURING STORAGE AND DISTRIBUTION		**2,33**	**0,47**	**3**	**2**	**2**	**2**	**2**	**3**	**N/A**
	Unusability of data after exfiltration (hashing, field level encryption, tokenization …)	**2,14**	**0,35**	2	2	2	2	2	3	2
	Partial hiding of the entire data, after exfiltration limitation of consequences	**2,00**	**0,00**	2	2	2	2	2	2	2
	Protection during distribution (encryption, passwords, use of verified channels …)	**2,71**	**0,45**	3	2	3	2	3	3	3
	Data integrity verification	**2,29**	**0,45**	2	2	2	2	2	3	3
HUMAN RESOURCES		**3,00**	**0,00**	**3**	**3**	**3**	**3**	**3**	**3**	**N/A**
	Educating and training users about cybersecurity and data protection	**3,00**	**0,00**	3	3	3	3	3	3	3
	Creation of a dedicated cyber entity	**2,57**	**0,49**	3	2	3	2	2	3	3
	Leverage collaboration with other organizations, industry, agencies and more	**2,29**	**0,45**	2	2	3	2	2	3	2
USE OF DATA FOR PROTECTION		**2,00**	**0,58**	**2**	**2**	**1**	**2**	**2**	**3**	**N/A**
	Data analysis and deep learning regarding the needs of Smart City projects	**2,00**	**0,53**	2	2	1	2	2	3	2