

Ochrana vodohospodářské infrastruktury před možnou hrozbou teroristického útoku

Bc. Patrik Hartman

Diplomová práce
2022



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení

Akademický rok: 2021/2022

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: **Bc. Patrik Hartman**
Osobní číslo: **L20681**
Studijní program: **N1032A020002 Bezpečnost společnosti**
Specializace: **Rizikové inženýrství**
Forma studia: **Prezenční**
Téma práce: **Ochrana vodohospodářské infrastruktury před možnou hrozbou teroristického útoku**

Zásady pro vypracování

1. Zpracujte literární rešerši zkoumané oblasti z domácích a zahraničních zdrojů.
2. Popište současný stav řešené problematiky pro danou oblast.
3. Zpracujte analýzu a vyhodnocení stavu ochrany vodohospodářské infrastruktury.
4. Vypracujte plán pro zlepšení stavu ochrany vodohospodářské infrastruktury před teroristickou hrozbou.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KROČOVÁ, Šárka. *Bezpečnost provozu technické infrastruktury*. Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2017. SPBI Spektrum, 94. ISBN 978-80-7385-185-9.
2. TOMEK, Miroslav, Jan STROHMANDL a Jakub RAK. *Zásobování obyvatelstva pitnou vodou za mimořádných situací*. Praha: Academia, 2014. ISBN 978-80-7454-462-0.
3. RADVANSKY, Robert a Allan MCDougall. *Critical infrastructure: homeland security and emergency preparedness*. Boca Raton: CRC Press, 2010. 2nd ed. ISBN 978-14-2009-527-2.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **doc. Ing. Jaromír Novák, CSc.**
Ústav krizového řízení

Datum zadání diplomové práce: **1. prosince 2021**

Termín odevzdání diplomové práce: **6. května 2022**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 5. 8. 2022

Jméno a příjmení studenta: Bc. Patrik Hartman

.....
podpis studenta

ABSTRAKT

Diplomová práce se zabývá tématem ochrany vodohospodářské infrastruktury před možným teroristickým útokem. Je zvolena lokalita Jižní Morava, přesněji část území, kde působí Vodovody a Kanalizace Hodonín akciová společnost, a státní podnik Povodí Moravy. Diplomová práce je poté strukturována na základní teoretickou část, která je vyhrazena terminologii potřebné pro danou problematiku, pojednává o oblasti vodohospodářské infrastruktury, plynule navazuje kybernetická bezpečnost, kde následuje legislativa pro oblast vodního hospodářství a ochrany vydaná Evropskou unií nebo Českou republikou. Následují obsáhlejší části v podobě terorismu, a oblast určená pro technickou a mechanickou ochranu objektů. Poslední část teorie je vyhrazena cílům a metodice práce. Praktická část se zaměřuje na popis současného stavu v oblasti ochrany vodohospodářské infrastruktury v návaznosti na možný teroristický útok. Uvádí zde informace vztažené pro řešenou oblast a její části. Navazuje zpracování analýzy a slovního popisu zjištěného stavu z pohledu nedostatků. Aplikační část je již vyhrazena pouze pro plán v podobě rizikových oblastí a případných návrhů pro zlepšení současného stavu.

Klíčová slova: ochrana, vodohospodářství, bezpečnost, terorismus, voda.

ABSTRACT

The diploma thesis deals with the topic of the protection of water management infrastructure through a possible terrorist attack. The location of South Moravia is chosen, more precisely the part of the territory where the Vodovody a Kanalizace Hodonín joint-stock company and the state enterprise Povodí Moravy operate. The diploma thesis is then structured into a basic theoretical part, which is reserved for the terminology needed for the given issue, discusses the area of water management infrastructure, followed smoothly by cyber security, followed by legislation for the area of water management and protection issued by the European Union or the Czech Republic. This is followed by more extensive sections in the form of terrorism and an area designated for technical and mechanical protection of objects. The last part of the theory is reserved for the objectives and methodology of the work. The practical part focuses on the description of the current situation in the field of water management infrastructure protection following a possible terrorist attack. It provides information related to the addressed area and its parts. It follows the processing of the analysis and verbal description of the detected condition from the point of view of shortcomings. The application part is already reserved only for the plan in the form of risk areas and possible proposals for improving the current state.

Keywords: Protection, Water Management, Security, Terrorism, water.

Chci poděkovat mému vedoucímu panu doc. Ing. Jaromíru Novákovi, CSc., za odborný přístup, vedení a ohleduplnost v průběhu tvorby závěrečné diplomové práce.

Dále chci poděkovat své rodině a přátelům, za dlouhodobou podporu v období studia na vysoké škole.

„Vědět málo je nebezpečné, Vědět mnoho, také.“

Albert Einstein

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD	10
I TEORETICKÁ ČÁST	11
1 VŠEOBECNÁ TERMINOLOGIE	12
2 PŘEHLED ZÁKLADNÍCH POJMŮ V OBLASTI VODOHOSPODÁŘSVÍ	17
3 VODOHOSPODÁŘSKÁ INFRASTRUKTURA	22
3.1 HISTORIE VODOHOSPODÁŘSKÉ INFRASTRUKTURY.....	22
3.2 PITNÁ VODA	23
3.2.1 Definice, charakteristika a výroba pitné vody.....	23
3.2.2 Distribuce pitné vody	24
3.2.3 Vodovody nadmístního významu	24
3.2.4 Vodovody místního významu	25
3.3 OCHRANA VODOHOSPODÁŘSKÉ INFRASTRUKTURY	26
3.3.1 Ochrana vod	26
3.3.2 Ochrana vodních zdrojů	27
4 KYBERNETICKÁ BEZPEČNOST	28
4.1.1 Typy informací.....	28
4.1.2 Životní cyklus informace	29
4.1.3 Cílené útoky	29
5 LEGISLATIVA A PRÁVNÍ PŘEDPISY	32
5.1 DŮLEŽITÉ SMĚRNICE A PRÁVNÍ PŘEDPISY EU A ČR	32
6 TERORISMUS	37
6.1 PRÁVNÍ DOKUMENTY EVROPSKÉ UNIE A ČESKÉ REPUBLIKY V OBLASTI TERORISMU.....	37
6.2 TERORISMUS V ČESKÉ REPUBLICE.....	38
6.3 CHARAKTERISTIKA A TYPOLOGIE TERORISMU	39
6.4 TERORISTICKÉ HROZBY PRO VODOHOSPODÁŘSKOU INFRASTRUKTURU	41
6.5 OCHRANA PROTI TERORISMU.....	42
7 TECHNICKÁ A MECHANICKÁ OCHRANA OBJEKTŮ	43
7.1 INTEGROVANÝ BEZPEČNOSTNÍ SYSTÉM	43
7.2 ZABEZPEČOVACÍ SYSTÉMY	44
7.3 ZÁKLADNÍ DRUHY OCHRANY.....	45
7.3.1 Klasická ochrana	45
7.3.2 Režimová ochrana	46
7.3.3 Fyzická ochrana	46
7.3.4 Technická ochrana	46
8 CÍL A METODIKA PRÁCE	49

II PRAKTICKÁ ČÁST.....	51
9 SOUČASNÝ STAV BEZPEČNOSTI VODOHOSPODÁŘSKÉ INFRASTRUKTURY PRO VAK HODONÍN, POVODÍ MORAVY	52
9.1 VODOVODY A KANALIZE HODONÍN.....	52
9.1.1 Informace o distribuci pitné vody a kanalizacích.....	53
9.2 OCHRANA A BEZPEČNOST	54
9.3 ÚPRAVNÝ A ZDROJE PITNÉ VODY.....	55
9.3.1 Úpravna vody Moravská Nová ves	55
9.3.2 Úpravna vody Bzenec Přívoz.....	57
9.3.3 Úpravna vody Koryčany	61
9.3.4 Čerpací stanice Louka	63
9.3.5 Data o pitné vodě za rok 2021.....	64
9.3.6 Data o odvádění a čištění odpadní vody za rok 2021.....	65
9.3.7 Integrovaný systém managementu	66
9.4 POVODÍ MORAVY	67
9.4.1 Vodní nádrž Koryčany	67
10 ANALÝZA A VYHODNOCENÍ STAVU OCHRANY VODOHOSPODÁŘSKÉ INFRASTRUKTURY.....	70
10.1 SWOT ANALÝZA PRO SOUČASNÝ STAV OCHRANY	70
10.2 ZJIŠTĚNÉ NEDOSTATKY V OBLASTI OCHRANY	73
11 PLÁN PRO ZLEPŠENÍ SOUČASNÉHO STAVU OCHRANY VODOHOSPODÁŘSKÉ INFRASTRUKTURY PŘED MOŽNOU TERORISTICKOU HROZBOU	76
ZÁVĚR	83
SEZNAM POUŽITÉ LITERATURY.....	85
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	90
SEZNAM OBRÁZKŮ	92
SEZNAM TABULEK.....	93
SEZNAM PŘÍLOH.....	94

ÚVOD

Ochrana vodohospodářské infrastruktury představuje z hlediska významu v současnosti a budoucnosti významný prvek České republiky. Význam je důležitý především pro samotné obyvatelstvo a místní průmysl, snížení kapacity, omezení provozu nebo úplné zastavení, představuje závažný problém pro aktuální životní úroveň a zdraví obyvatel.

Teroristický útok vedený na prvky infrastruktury zaměřené na vodu může přijít kdykoliv, není to ale jen otázka času, důležitou část hraje úroveň ochrany, která má jako cíl stanoveny případné útočníky odradit, omezit, zastavit nebo alespoň zpomalit jejich plány. Otázka ochrany vody zde koluje již od pradávna, ovšem moderní otázka ohledně ochrany před terorismem je známá teprve několik desetiletí.

Terorismus je všeobecně známý pojem, ale jeho skutečný význam a podstatu nezná nikdo, definic je tolik, že pojem terorismus označuje veškeré jednání, které je proti zájmům společnosti a narušuje její klidný život. Rozsah teroristických útoků je rozmanitý a není možné se nikdy plně připravit na možné způsoby provedení. To je jeden z hlavních důvodů, proč se zabývat oblastí ochrany infrastruktury před teroristickou hrozbou.

Cílem práce je na základě teoretických informací, dat a poznatků identifikovat a vyhledávat případné slabiny mezi prvky v systému. Stanovit tak závažnost a navrhnout opatření, která povedou preventivním krokům a připravenosti na široké spektrum možností teroristického útoku.

Praktická část staví na získaných poznatcích v teoretických poznatcích a srovnává je se skutečností. Využívá se zjištěných poznatků na základě fyzického pozorování jednotlivých prvků. Aplikuje se zde metoda SWOT, které lépe zobrazuje aktuální stav. Zároveň jsou zjištěné nedostatky popsány a slovně hodnoceny.

Závěrečná část práce v podobě aplikační části je vyhrazena pro stanovení plánu jako možností pro vyřešení zjištěných nedostatků. Bodově jsou uvedeny kategorie, kde se nedostatky projevují a jsou tedy na základě znalostí a diskuze stanoveny možná opatření s teoretickým ohodnocením finanční nebo časové náročnosti.

I. TEORETICKÁ ČÁST

1 VŠEOBECNÁ TERMINOLOGIE

Kapitola zaměřená na používané výrazy pro tuto práci, které jsou potřebné pro pochopení problematiky v dané diplomové práci. Tato část obsahuje všeobecné pojmy, které nespádají do oblasti vodohospodářství, pojmům z této oblasti je vyhrazena vlastní kapitola. Jde o všeobecný přehled pojmů, které jsou čerpány z knihy „*Biologické a chemické zbrane připravenost a odpověď*“ z roku 2013 od trojice autorů: Cyril Klement, Roman Mezencev a Jiří Bajgar, dále z knihy „*Slovník pojmů krizového řízení*“ z roku 2018 od Rostislva Richtera, a několik pojmů je převzato z „*Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu*“, který v roce 2016 vydalo MV ČR.

Aerosol – disperzní soustava tvořená malými částicemi v kapalném nebo pevném skupenství, které jsou rozptýleny v plynu (Klement, Mezencev, Bajgar, 2013).

Analýza rizik – proces zahrnující podrobnou analýzu rizik, určování jejich zdrojů a velikosti, výzkum vzájemných vztahů a odhad rozsahu negativních dopadů na systém v případě vzniku krizové situace (Klement, Mezencev, Bajgar, 2013).

Bakterie – jednobuněčné prokaryotické mikroorganismy bez obsahu chlorofylu, kde buněčná stěna obsahuje polysacharid murein (peptidoglykán). Objevují se v různých tvarech a velikostech (sférické, tyčinkovité a vláknité). Oproti viru se bakterie rozmnožují a žijí nezávisle na hostiteli, platí pro příznivé podmínky (Klement, Mezencev, Bajgar, 2013).

Bakteriologie – výzkum a nauka o bakteriích, včetně rickettsií, chlamydií a mykoplazmy (Klement, Mezencev, Bajgar, 2013).

Bakteriologická zbraň – někdy taky označena jako biologická zbraň, je zbraň založená na účinku biologických agens, které mají negativní dopad na lidské zdraví nebo zdraví zvířat případně vedou až ke smrti, mohou také být škodlivé pro rostliny a způsobovat škody v oblasti zemědělství. Zbraní jako takovou se vnímá přístroj, vybavení, zařízení upravené nebo vyvinuté pro šíření či použití biologických agens (Richter, 2018).

Bezpečnost – označuje stav systému odolávat předvídatelným a známým hrozbám, které mají dále charakter vnější a vnitřní hrozby. Negativně působí na prvky nebo celý systém a jejich dopad je nežádoucí. Cílem je zachovat stabilitu, strukturu, chování a spolehlivost systému. Pro oblast v oblasti bezpečnosti státu byl vytvořen ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky (MV ČR, 2016).

Bezpečnost informací – představuje zajištění oblastí důvěrnosti, integrity a dostupnosti dat a informací.

Bezpečnostní opatření – zahrnuje souhrn činností, kdy je cílem zajistit bezpečnost informací v oblastech informačního systému, zajistit dostupnost a spolehlivost, zajistit bezpečnost sítí v kybernetickém prostředí (Richter, 2018).

Bezpečnostní rada kraje – je poradním orgánem pro přípravu na řešení krizové situace. Rada je tvořena předsedou v podobě hejtmana kraje nebo v případě Prahy primátorem hlavního města Prahy. Předseda vždy jmenuje členy rady, ale má nejvýše 10 členů mezi které patří náměstek hejtmana, příslušník Armády České republiky (dále jen „AČR“, ředitele krajského ředitelství Policie České republiky, ředitele hasičského záchranného sboru kraje (dále jen „HZS“, ředitele zdravotnické záchranné služby kraje a další osoby nezbytné pro řešení dané krizové situace. Další informace jsou obsaženy v zákoně č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, Nařízení vlády č. 462/2000 k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (Richter, 2018).

Bezpečnostní rada obce s rozšířenou působností – představuje poradní orgán obce s rozšířenou působností pro řešení a přípravu na krizovou situaci. Starosta obce s rozšířenou působností (dále jen „ORP“) je předseda této rady a jmenuje další členy rady. Rada má nejvýše 8 členů mezi něž patří místostarosta, tajemník obecního úřadu, člen HZS ČR jmenován ředitelem HZS, příslušníka Policie České republiky (dále jen „PČR“) zvoleného krajským ředitelem PČR, tajemníkem a další osoby na základě znalostí potřebných pro řešení a přípravu na krizovou situaci (Richter, 2018).

Bezpečnostní rada státu – je tvořena předsedou vlády (pro rok 2022 Petr Fiala) a dalšími členy vlády na základě rozhodnutí vlády. Rada připravuje vládě návrhy pro opatření v případech krizové situace k zajištění bezpečnosti ČR (Richter, 2018).

Bezpečnostní sbor – představují složky PČR, HZS, Vězeňská služba České republiky, Úřad pro zahraniční styky a informace, Celní správa České republiky, Generální inspekce bezpečnostních sborů a Bezpečnostní informační služba (Richter, 2018).

Bezpečnostní výzkum – zahrnuje experimenty a zkoumání v oblastech bezpečnosti, kdy je se snaží získávat data o technologické a technické úrovni zkoumaného prvku či subjektu. Na základě poznatků je potom možné tvořit preventivní a včasná opatření před možnou

hrozbou různého charakteru. Významově spadá mezi interdisciplinární výzkum, vzhledem k dlouhodobé potřebě ochrany státu a zajištění bezpečnosti prostředí (MV ČR, 2016).

Biotop – vymezená oblast skrze určité přírodní podmínky (klimatické, geologické apod.), které umožňují život vzájemně závislých rostlinných druhů a živočichů (Klement, Mezencev, Bajgar, 2013).

Dezinfekce – je usmrcení infekčních agens mimo organismus v důsledku přímé expozice účinku chemické látky nebo agens. Průběžná dezinfekce uplatňuje opatření co nejdříve po vyloučení kontaminovaného materiálu z organismu zasažené osoby (Klement, Mezencev, Bajgar, 2013).

Kategorie vodních děl – v rámci dozoru se vodní díla řadí do 4 kategorií. Každé dílo je zařazeno do jedné kategorie, na základě parametrů velikosti díla, rozsahu možných škod, velikosti možné záplavové vlny vlivem poškození vodního díla nebo na základě nadměrných srážek (Richter, 2018).

- I. **Kategorie I** – představuje ohrožení v rozsahu tisíc až desetitisíc osob, předpokládány jsou velké počty obětí, vznikají rozsáhlé škody na objektech a infrastruktuře. Vodní dílo je vyřazeno a ovlivňuje jeho význam v oblastech průmyslu apod. Má značné ekonomické důsledky ve státě, pro kraj představují závažný problém (Richter, 2018).
- II. **Kategorie II** – představuje ohrožení v rozsahu stovek až tisíců osob, jsou zde předpokládány ztráty na životech, v oblasti směrem pod vodní dílo dochází ke vzniku škod na objektech. Vyřazení vodního díla z provozu představuje značné ztráty a komplikace (Richter, 2018).
- III. **Kategorie III** – představuje ohrožení v rozsahu desítek až stovek osob, je zde riziko ztráty osob na životech, pod vodním dílem vznikají malé a střední škody. Vodní dílo je vyřazeno z provozu, ale může částečně fungovat, výpadek je plně nahraditelný (Richter, 2018).
- IV. **Kategorie IV** – nepravděpodobné ztráty na životech, území v oblasti pod vodním dílem je minimálně poškozeno, ztráty na vodním díle v důsledku škod jsou zanedbatelné (Richter, 2018).

Krizová komunikace – obnáší přenos informací mezi složkami IZS, státními orgány a územními samosprávnými orgány, kdy se využívá datového a hlasového přenosu informací

za pomoci veřejných sítí, vybraných částí soukromých sítí elektronických komunikací (MV ČR, 2016).

Krizová situace – je mimořádná událost na základě zákon č. 239/2000 Sb., o integrovaném záchranném systému, narušení kritické infrastruktury či jiné nebezpečí, kdy dochází k vyhlášení jednoho z krizových stavů (MV ČR, 2016).

Krizové opatření – představuje soubor přijatých opatření pro řešení, zmírnění nebo odstranění škod vzniklých v důsledku krizové situace. V rámci těchto opatření je možné zasahovat do práv a svobod obyvatel nebo udělovat povinnosti v rámci krize (MV ČR, 2016).

Krizové řízení – představuje řídicí činnosti orgánů v oblasti krizového řízení. To zahrnuje analýzu a vyhodnocení, plánování, organizování, realizaci, kontrolu, řešení, monitoring a zpětnou odezvu (MV ČR, 2016).

Kybernetická bezpečnostní událost – je označení pro událost, jenž může narušit bezpečnost informací v informačním systému nebo narušit bezpečnost služeb případně bezpečnost a integritu elektronických komunikačních sítí (Richter, 2018).

Kybernetický bezpečnostní incident – je projevem kybernetické bezpečnostní události, kdy došlo k narušení integrity elektronických komunikačních sítí, bezpečnostních služeb nebo bezpečnosti informací a dat v informačním systému (Richter, 2018).

Kybernetický prostor – je zastoupen v podobě digitálního prostředí, který umožňuje vznik, výměnu a zpracování informací, vytvářené v informačním systému nebo službami a sítěmi elektronické komunikace (Richter, 2018).

Mimořádná událost – nebo také situace, která vznikla v určitém prostředí vlivem živelní pohromy, ohrožením kritické infrastruktury, havárie, nezákonnou činností, nákazami, ohrožením vnitřní bezpečnosti a ekonomiky. Je řešena běžným způsobem ze strany orgánů a složek bezpečnostního systému podle zvláštních právních předpisů. Tento pojem v současných právních předpisech ČR uvádí řadu pojmů jako např. mimořádná situace, pohroma, nouzová situace, katastrofa nebo havárie (MV ČR, 2016).

Národní plány povodí – pořizuje Ministerstvo životního prostředí a Ministerstvo zemědělství v kooperaci s příslušnými správci povodí nebo příslušnými krajskými úřady dané působnosti. Tyto plány jsou schvalovány vládou ČR (Richter, 2018).

Preventivní opatření – chápeme jako přijaté opatření v důsledku nežádoucí události, jednání nebo opomenutí, ve vztahu k bezprostřední hrozbě vzniku škod, jehož cílem je předejít vzniku škod nebo je minimalizovat na přijatelnou úroveň (MV ČR, 2016).

Riziko – značí možnost určité pravděpodobnosti vzniku nežádoucí události. Riziko lze odvodit z dané hrozby. Míru či pravděpodobnost rizika je možné posoudit pomocí analýzy rizik, která posuzuje i stav připravenosti pro odolávání těmto hrozbám. Riziko můžeme také charakterizovat jako účinek nejistoty na dosažení cíle nebo pravděpodobnost vzniku nežádoucí události (MV ČR, 2016).

Územní plánování – cílem je vytvářet předpoklady pro výstavbu a udržitelnost rozvoje území, který spočívá ve vyváženém vztahu podmínek pro příznivé životní prostředí, pro hospodářský rozvoj a soudržnost společenství obyvatel. Nemůže současně ohrožovat podmínky života budoucích generací. Územní plánování zajišťuje předpoklady pro udržitelný rozvoj na území soustavným a komplexním řešením účelného využití a prostorového uspořádání území, kdy je cílem dosažení obecně prospěšného souladu veřejných nebo soukromých zájmů pro rozvoj území. Účelně tedy sleduje společenský a hospodářský potenciál místního rozvoje (MV ČR, 2016).

Veřejná infrastruktura – představuje stavby, zařízení a pozemky. Patří zde dopravní infrastruktura, občanské vybavení, veřejné prostranství a technická infrastruktura. Technická infrastruktura představuje stavby a vedení, včetně technického zařízení a vybavení. Jedná se o vodovody, vodojemy, čističky odpadních vod, kanalizace a produktovody (Richter, 2018).

Zdroj rizika – je vnímán jako nebezpečná vlastnost látky, fyzikální nebo fyzická vlastnost látky, která může vyvolat vznik závažné havárie (Richter, 2018).

2 PŘEHLED ZÁKLADNÍCH POJMŮ V OBLASTI VODOHOSPODÁŘSVÍ

V oblasti vodohospodářské infrastruktury a její ochrany, se vyskytuje značný počet odborných pojmů, které se v této oblasti používají. Následující přehled těchto pojmů slouží pro jejich charakteristiku a pochopení. Jedná se o pojmy z oblasti pitné vody a kanalizačních systémů. Nejdůležitější pojmy jsou (Tomek, Strohmandl a Rak, 2014; Richter, 2018; Vodohospodářská infrastruktura v obcích a náležitosti hospodaření s vodou, 2019, AQUASHOP, 2022):

- **Akumulace vody** – je tvorba zásob vody ve vodním systému pro zajištění bezpečného provozu vodovodu.
- **Akumulační nádrž** – je nádrž pro shromažďování vody, která tvoří součást jiného objektu. Jako příklad lze uvést čerpací stanici případně úpravnu pitné vody.
- **Dezinfekce vody** – je způsob úpravy vody na zdravotně nezávadnou za použití technologií pro její úpravu, nejčastěji za pomoci chlorace vody nebo pomocí UV záření. Dochází tak k odstranění bakterií jako jsou koliformní bakterie, psychrofilní bakterie, mezofilní bakterie (kultivované mikroorganismy) a enterokoky tedy fekální streptokoky.
- **Individuální zásobování pitnou vodou** – je zásobování vodou z jednoho dostupného zdroje, příkladem může být domovní studna, kdy denní produkce je menší než 10 m³ vody. Patří zde také zdroje zásobující maximálně 50 osob, pokud tato voda není užívána ke komerční činnosti, kde je vyžadováno užití pitné vody, nebo jde o veřejnou studnu.
- **Jímání vody** – je čerpání vody pomocí jímacího zařízení, kdy se jedná o čerpání podzemní vody.
- **Krizová situace** (dále jen „KS“) – představuje mimořádnou událost, při níž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu (tzv. krizové stavy).
- **Kanalizace** – je samostatně provozovaný soubor staveb a zařízení, které zahrnují kanalizační odtoky, objekty, čistírny odpadních vod nebo stavby určené pro čištění vody před vypuštěním do systému kanalizace (Vodohospodářská infrastruktura v obcích a náležitosti hospodaření s vodou, 2019).

- **Jednotná kanalizace** – je kanalizace sloužící pro společný odvod srážkové a odpadní vody.
- **Maximální denní potřeba vody** – je průměrná denní potřeba vody, která je násobená součinitelem denní nerovnosti, ten závisí na velikosti a charakteru oblasti spotřebiště.
- **Maximální hodinová potřeba vody** – je největší dosažená hodnota potřeby vody v časovém úseku jedné hodiny, jedná se o dny s maximální denní potřebou, vypočte se z maximální denní potřeby, která se následně vynásobí součinitelem hodinové nerovnoměrnosti potřeby.
- **Průměrná denní spotřeba vody** – je výpočetní hodnota, která se získává z hodnoty specifické potřeby vody násobením počtu příslušných jednotek.
- **Provozovatel** – je osoba, která je pověřena provozem vodovodu nebo kanalizace a je držitelem povolení k provozování této činnosti. Pověření je na základě předchozího uzavření provozní smlouvy. Může se také současně jednat o vlastníka, který současně plní funkci a povinnosti provozovatele.
- **Provozování infrastruktury** – je to souhrn všech činností potřebných pro zajištění dodávek pitné vody, odvodu a následného čištění odpadních vod. Jde tedy o dodržování technologických postupů, manipulačních řádů, provozních směrnic, provozní měření, vedení provozní dokumentace a dalších potřebných činností. Nepatří zde správa vodovodů a kanalizací, včetně jejich rozvoje.
- **Specifická potřeba vody** – je množství vody dodávané odběrateli za jednotku času, nebo potřebné na jednotku výroby za jednotku času, množství vody se udává v litrech na osobu.
- **Spotřeba vody** – je skutečné množství vody odebrané z vodovodního zařízení za danou časovou jednotku.
- **Stočné** – je finanční částka za odvod, čištění nebo likvidaci odpadní vody (cena je obvykle stanovena za 1 m³).
- **Odběr vody** – je proces odběru vody z povrchového zdroje pomocí odběrného zařízení.

- **Mimořádná situace** – představuje vzniklou situaci se souvislostí na hrozící nebo nastalou mimořádnou událostí, kdy je potřeba ji řešit řádnou činností odpovědných orgánů veřejné správy, případně činností složek integrovaného záchranného systému.
- **Mimořádná událost** (dále jen „MU“) – je událost s působením škodlivých sil a jevů, které mimořádně ohrožují život, zdraví, majetek nebo životní prostředí.
- **Náhradní zásobování pitnou vodou** – je činnost, jejímž účelem je zabezpečit potřebné množství vody požadované jakosti pro potřeby uživatelů v době, kdy dojde k přerušení dodávky vody z veřejného vodovodu v důsledku jeho oprav nebo havárií.
- **Nouzové přižití obyvatelstva** – je soubor prováděných postupů a činností věcně příslušných orgán, zapojených subjektů a občanů s cílem snížit, na co nejnížší možnou míru, negativní dopady MU.
- **Nouzové zásobování pitnou vodou** – je zabezpečení pitné vody pro obyvatelstvo v množství nezbytném pro jeho přežití a po nezbytně dlouhou dobu potřebnou pro obnovení funkce běžného zásobování pitnou vodou.
- **System nouzového zásobování pitnou vodou** – je souhrn věcných, materiálních, technických a personálních prostředků vlastníků a provozovatelů vodovodů pro veřejnou potřebu a prostředků uložených v zásobách SSHR a prostředků, jakož i soubor organizačních opatření pro koordinaci jejich činností při nouzovém zásobování vodou při vzniku MU a za krizových stavů.
- **Úpravna vody** – je soubor objektů a zařízení s technologií pro úpravu vody nebo pouze se zařízením na zdravotní zabezpečení vody bez technologie úpravy vody.
- **Úprava vody** – je souhrn technologických procesů k dosažení požadované jakosti vody.
- **Veřejné zásobování pitnou vodou** – je zásobování vodou z veřejného vodovodu, veřejné studny označené jako zdroj pitné vody, nebo soukromé studny využívané k takové komerční činnosti, kde je vyžadováno užití pitné vody.
- **Vodárenství** – je technicky zaměřený obor, který se zabývá jímáním, odběrem, úpravou, akumulací, dopravou a rozvodem vody pro potřeby obyvatelstva, průmyslu a zemědělství.

- **Vodní zdroj** – je vodní útvar povrchové nebo podzemní vody, kterou lze použít pro pokrytí potřeb člověka a společnosti. Podzemní zdroje vod jsou přednostně využívány pro zásobování pitnou vodou, případně pro účely stanovené právním předpisem. Jiné účely využití zdroje podzemních vod může povolit vodoprávní úřad, ale jen pokud to neovlivní běžné pokrytí předchozí potřeby obyvatel.
- **Vodoprávní úřad** – představuje subjekt pro správu pro oblast vodního hospodářství. Může se tedy jednat o obecní úřad, újezdní úřad na území vojenských újezdů, obecní úřad s rozšířenou působností, krajský úřad, Ministerstvo zemědělství, Ministerstvo životního prostředí, Ministerstvo dopravy a Ministerstvo obrany.
- **Vodárenský objekt** – je jednotlivý objekt vodovodu, například odběrný objekt povrchové vody, jímající objekt podzemní vody, čerpací stanice, úpravná vody, vodovodní řád, vodojem, rozvodná vodovodní síť.
- **Vodohospodářské služby** – jsou poskytované služby provozovatelem, které zahrnují služby v podobě dodávek vody, odvodu a čištění odpadní vody, službu udržování a servis pro odběratele.
- **Vodovod** – je soubor objektů a zařízení zahrnující odběrné objekty, úpravny vody, čerpací stanice, vodojemy, vodovodní řady a vodovodní síť a zabezpečující zásobování vodou.
- **Vodné** – je finanční částka za poskytnutí dodávky pitné vody (cena je obvykle stanovena za 1 m³).
- **Vodní hospodářství** – představuje skupinu činností, které jsou provázány s ochranou podzemních a povrchových zdrojů vody. Cílí na ochranu, rozvoj a užívání vodních zdrojů stejně jako na ochranu a rozvoj odtoků, včetně ochrany před škodlivým působením vody a jejího užívání.
- **Vlastník infrastruktury** – je subjekt s výlučným vlastnickým právem k vodovodu a kanalizaci. Může se také jednat o subjekt, který na základě dispozičního práva má přístup k infrastruktuře, jedná se o svazky obcí a je to stavěno na základě zákonů.
- **Vodovodní systém** – je provozně samostatný soubor staveb a zařízení zahrnující vodovodní řady a vodárenské objekty, jimiž jsou zejména stavby pro jímání a odběr

povrchové nebo podzemní vody, její úpravu a akumulaci; vodovod je vodním dílem.

- **Zásobní vodojem** – je vodojem určený k zásobování určitého tlakového pásma vodou. Jeho funkce spočívá ve vyrovnávání při nerovnoměrném odběru vody ze sítě.
- **Zásobování pitnou vodou** – je souhrn činností, jejichž účelem je zabezpečit potřebné množství pitné a požární vody stanovené jakosti spotřebitelům a pro požární odběrní místa.

3 VODOHOSPODÁŘSKÁ INFRASTRUKTURA

Vodohospodářská infrastruktura hraje důležitou roli v oblasti zajišťování a plnění funkce zásobování obyvatelstva pitnou vodou a čištěním odpadních vod. Současně je zapojena do rozvoje na daném území, řešení krizových situací a zároveň má vliv na životní úroveň. Její ochrana je tedy nezbytnou součástí pro zajištění provozu a plnění již zmíněných úkonů (Vodohospodářská infrastruktura v obcích a náležitosti hospodaření s vodou, 2019).

Česká republika (dále jen „ČR“) má část infrastruktury označenou jako veřejnou, kterou představují stavby, pozemky a zařízení. Vodohospodářská infrastruktura spadá do technické infrastruktury, kterou představuje vedení, stavby a také provozně související technické vybavení. Příkladem jsou vodojemy, vodovody, čističky odpadních vod, kanalizační sítě, zařízení a stavby určené pro nakládání s odpadem, energetická vedení, vedení komunikačních sítí, a v neposlední řadě zde patří produktovody (Šenovský, Adamec a Šenovský, 2007).

3.1 Historie vodohospodářské infrastruktury

Pojem infrastruktura je svým původem připisován do Francie v období 19. století. V průběhu první poloviny 20. Století byl tento pojem použit pro označení armádních zařízení. Slovo infrastruktura můžeme odvodit ze složení latinských slov *infra* (dole, vespod nebo také nízko) a slova *struere* (budovat nebo sestavovat). Spojením těchto dvou slov tedy můžeme pojem chápat jako plošné budování určitých systémů. Pojmem infrastruktura lze označit základní zařízení určené pro dlouhodobé využití v oblasti institucionálního, personálního nebo materiálního charakteru, kdy dokáže zajistit funkci dělení povinností v oblasti národního hospodářství. (Šenovský, Adamec a Šenovský, 2007).

Vznik je možné spojit s rozvojem lidské společnosti, kdy potřeba zásoby a dostatku pitné vody byla vždy jednou z priorit k dobrému žití. Prvotní zdroje pitné vody tvořily řeky, potoky nebo jezera, později byly tvořeny záchytné jímky nebo kopány studny. Již ve středověku bylo možné na našem dnešním území ČR najít první vodovody, které fungovaly na principu gravitace. Systém rozvodných trubek byl převážně ze dřeva či kamene. Zásadním problémem ale představovala odpadní a znečištěná voda, kdy její odvod byl v době středověku řešen pouze ve formě povrchových žlabů, příkopů nebo vodotečů. Nevýhody jako zápach, šíření nemocí a infekcí vedl k rozvoji v podobě zakrývání a stavbě zděné kanalizací, kdy docházelo k odvodu odpadní vody mimo město nebo vesnici.

V období 19. století se již stavěly kanalizace zděné nebo z dusaného betonu. Kanalizace ve městech byly většinou budovány pouze pro odvod odpadní vody z měšťanských domů, proto bylo době vzniku Československé republiky vybaveno tímto odvodem pouze 7 % domácností. Velký rozvoj výstavby kanalizací a následných čistíren odpadních vod, začal až v době Československé republiky.

Do 15. století spadalo zakládání vodovodu do povinností panovníka. Teprve založením zemského úřadu spadala tato povinnost na tento orgán. Uvedený způsob řízení fungoval až do roku 1948, kdy byly založeny krajské celky. Města, obce, sdružení nebo vodohospodářské svazy byly iniciátorem pro stavbu veřejných vodovodů. Pravomoci zemských úřadů v oblasti vodního hospodářství byly převedeny na krajské národní výbory (Z historie společnosti, vodárenství a kanalizací, 2022).

3.2 Pitná voda

Vodu lze vnímat pohledem chemické sloučeniny kyslíku a vodíku, případně jako v přírodě se volně se vyskytující roztok, který se zde vyskytuje již dlouhou dobu a je nezbytnou součástí života. Dle odhadů je zemský povrch pokryt zhruba 70% vody, kdy pouhá 3 % tvoří vodu pitnou. Tohle malé množství musí pokrýt potřeby celého světa, především tedy potřeby 8 miliard lidí a nespočtu jiných forem života.

3.2.1 Definice, charakteristika a výroba pitné vody

Pitnou vodu můžeme definovat jako vodu, která je určena hlavně k pití, vaření, výrobě potravin a nápojů, využití v potravinářství a určena k péči o lidské tělo spolu s dalšími potřebami. Pitná voda splňuje hygienické požadavky zdravotní nezávadnosti, je dodávána do veřejných vodovodů a podléhá trvalé kontrole, pro zamezení rizika v podobě chemické nebo mikrobiologické změny v průběhu distribuce (Kročová, 2009).

Výroba pitné vody spočívá především v použité technologii pro úpravu pitné vody. Za pitnou vodu potom považujeme zdravotně nezávadnou pitnou vodu, která se získává hlavně z vod podzemních. K výrobě lze využít pouze vodu, která splňuje kritéria specifikovaná v kategoriích A1, A2 a A3. Kontrolu kvality surové vody a vody upravené slouží plán kontroly kvality vody, který je v každé úpravně vody a je součástí provozní evidence. Vodní zdroje vyhrazené pro veřejné zásobování pitnou vodou, kdy jejich kapacita přesahuje 10 000 m³ /rok mají nutnost stanovit pásmo hygienické ochrany (Kročová, 2009).

Kvalita pitné vody v ČR je poté řízena hlavně legislativou, kdy se především řídí Zákonem o ochraně veřejného zdraví č. 258/2000 Sb. (v platném znění), včetně dalších platných vyhlášek. V souladu s Vyhláškou č. 252/2004 Sb., kterou se stanoví hygienické požadavky na pitnou a teplou vodu a četnost a rozsah kontroly pitné vody, musí mít pitná voda takové fyzikálněchemické vlastnosti, které nepředstavují žádné ohrožení veřejného zdraví a nesmí obsahovat mikroorganismy, parazity a látky jakéhokoliv druhu v počtu nebo koncentraci, které by potencionálně mohly ohrozit veřejné zdraví. Vyhláška také stanovuje ukazatele pitné vody, jejich limity a určuje minimální roční četnost pro odběr a rozsah vzorků pitné vody na vodovodních sítích. Vyhláška č. 307/2002 Sb., o radiační ochraně, poté stanovuje sledování obsahu radionuklidů (Parametry pitné vody, 2022).

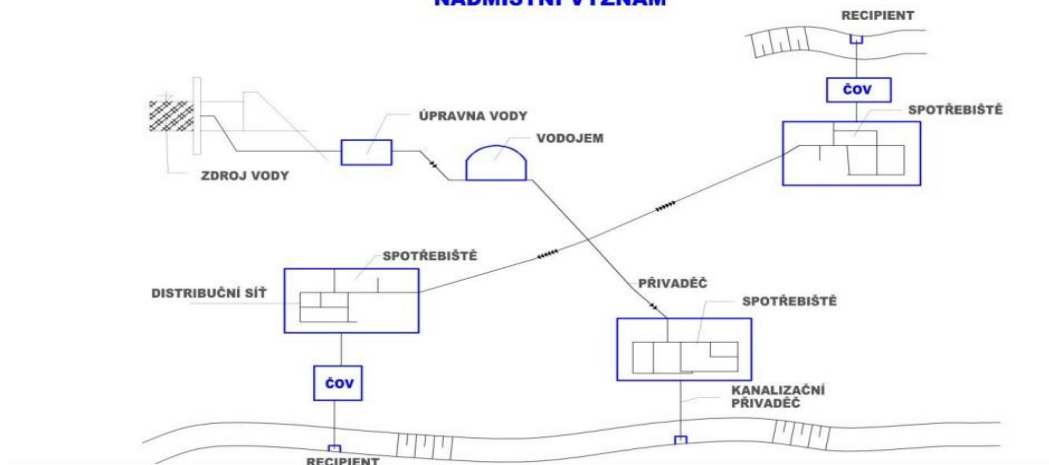
3.2.2 Distribuce pitné vody

K distribuci samotné pitné vody, která splňuje všechny požadavky, se v normálním stavu používají vodovodní sítě, vodojemy, přivaděče, tlakové stanice, přerušovací komory, redukční komory, posilovací stanice, vodovodní přípojky a také monitorovací stanice. Při distribuci se měří množství dodávané vody pomocí různých měřících zařízení, u koncového spotřebitele známý vodoměr. Samotná distribuční síť se podle významu dělí na vodovody nadmístního významu a vodovody místního významu. Na dodávkách pitné vody pomocí vodovodních sítí je v ČR závislých až 93% obyvatel. Značná část obcí a měst využívá vodovody pro veřejné potřeby a jako pohotovostní rezervu požární vody. V případě krizové situace fungují jako strategický subjekt, který musí za každé situace zajistit minimálně nouzové dodávky pitné vody pro zdravotní služby a další objekty veřejné infrastruktury (Kročová, 2009).

3.2.3 Vodovody nadmístního významu

Jejich cílem je zásobování pitnou vodou, zpravidla z centrálních povrchových zdrojů, určité počty měst a obcí. Obvykle přesahující hranici několika okresů nebo krajů. Ze strategického významu jsou zařazeny do krizového plánu kraje a v případě mimořádné události se řídí pomocí krizových plánů příslušného kraje. Ve spolupráci a kooperaci se Správou státních hmotných rezerv (dále jen „SSHR“) a HZS České republiky jsou schopny zajistit náhradní nebo nouzové zásobování pitnou vodou pro danou oblast (Kročová, 2009).

VLIV ZDROJE NA DISTRIBUČNÍ SYSTÉMY NADMÍSTNÍ VÝZNAM



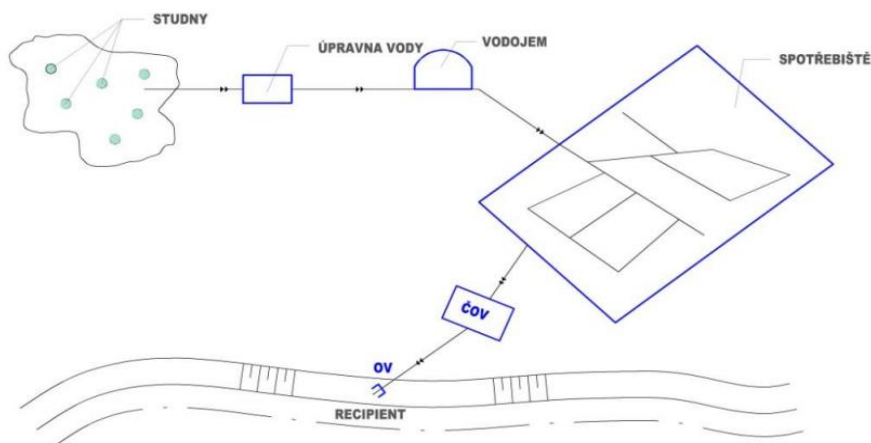
Obrázek 1: Vodovod nadmístního významu

Zdroj: Kročová, 2009

3.2.4 Vodovody místního významu

Nejsou vázány na velikost měst nebo obcí. Pitná voda je skrze ně vedena jen do příslušného celku. Původ této vody je převážně z místních podzemních zdrojů, ale v případě potřeby je doplňována z vodovodů nadmístního významu. Pro krizové řízení jsou zpracovány plány krizové připravenosti, tyto plány jsou zpracovány místní vodárenskou společností, a musí navazovat na krizové plány kraje (Kročová, 2009).

VLIV ZDROJE NA DISTRIBUČNÍ SYSTÉMY MÍSTNÍ VÝZNAM



Obrázek 2: Vodovod místního významu

Zdroj: Kročová, 2009

Z hlediska udržení a kontroly kvality pitné vody, platí pro oba dva zmíněné typy stejné podmínky pro provádění kontroly. Je potřeba mít zpracovány plány kontroly kvality vody, které popisují její kvalitu v celé distribuční síti. Příslušná vodárenská společnost musí každoročně obměnit 50 % kontrolních odběrných míst. Výsledky těchto kontrol jsou vedeny v písemné a elektronické dokumentaci, která se musí následný rok do 28. 2. odeslat na vodoprávní úřad (Kročová, 2009).

3.3 Ochrana vodohospodářské infrastruktury

Ochrana infrastruktury je celkově složitý a komplexní problém, který v sobě zahrnuje oblast prvků preventivních a represivních. Prevence se řadí na nejdůležitější pozici, protože od připravenosti se vše ostatní odvíjí, tedy pokud bude dostatečná, bude jednoduše fungovat. Chod státu a veřejné správy bude plně funkční a občan bude mít adekvátní podmínky pro život (Šenovský, Adamec, Šenovský, 2007).

Důležitou roli zde hraje strategie, kdy se jedná o dlouhodobý plán činností se zaměřením na dosažení cíle. Při ochraně vodohospodářské infrastruktury má právě význam dlouhodobá ochrana (Šenovský, Adamec, Šenovský, 2007).

3.3.1 Ochrana vod

Představuje závazek a cíle pro ochranu vod jako složku životního prostředí. Dělí se na povrchové vody a podzemní vody.

Povrchové vody: zamezit zhoršení stavu a kvality, zahrnuje i vodní útvary spadající do mezinárodních oblastí povodí. Zlepšit stav a zajistit ochranu a obnovu všech útvarů vod a dosáhnout dobrého stavu. Platí i pro umělé a silně ovlivněné vodní útvary, včetně dosahování ekologického potenciálu a dobrého chemického stavu. Prioritou je také snížení znečišťujících látek, odstraňování emisí a vypuštění nebezpečných látek (Tomek, Strohmandl a Rak, 2014).

Podzemní vody: zamezit nebo omezit kontaminaci skrze nebezpečné a závadné chemické látky do těchto vod, tím zabránit zhoršování stavu všech vod. Mezi další patří klasicky zajištění ochrany, obnova, zlepšení stavu včetně vyrovnávání v odběru a doplňování vody. Cílem je také odvrácení koncentrace nebezpečných látek jako důsledku činnosti populace (Tomek, Strohmandl a Rak, 2014).

3.3.2 Ochrana vodních zdrojů

V současné době je pojímána jako ochrana v oblasti kvantity a kvality povrchových a podzemních zdrojů vod. Je řešena pomocí územní ochrany vod, kde se jedná o právní oblast předpisů platných v ČR. Jedná se o chráněné vodohospodářské oblasti, a ve speciální přísnější ochraně vodní zdroje určené jako zdroje pitné vody, kdy se jedná o ochranné pásma (Pavlíková, 2014).

Ochranné pásmo vodních zdrojů – k ochraně nezávadnosti, vydatnosti a jakosti podzemních a nadzemních zdrojů vod, které jsou využívány pro zásobování jako pitná voda s průměrným odběrem nad 10 000 m³ za rok, zdrojů pro výrobu kojenecké vody balené a pramenité vody, je stanoveno vodoprávním úřadem ochranné pásmo opařením obecné povahy (Richter, 2018).

Dle závažnosti zdroje, může vodoprávní úřad stanovit ochranné pásmo pro zdroje i s nižší kapacitou. Současně může vodoprávní úřad změnit nebo rovnou odebrat ochranné pásmo. Jedná se o veřejný zájem (Richter, 2018).

Ochranná pásma se dělí na dva stupně, kdy první stupeň slouží k ochraně vodního zdroje v těsném okolí jímání nebo odběru. Druhý stupeň již chrání vodní zdroj v oblasti tak, aby nebyla ohrožena jeho zdravotní nezávadnost, jakost a vydatnost (Richter, 2018).

Rizikem je zde nedostatečné území ochrany vodního zdroje, malé zabezpečení po stránce přístupu do zabezpečené oblasti pro nepovolané osoby. V případě teroristického útoku s nepředpokladatelnými prostředky pro poškození nebo kontaminaci zdroje, je hrozba tohoto směru závažná. Žádný stát ani ČR neví, kdy a kde může být část této infrastruktury napadena (Tomek, Strohmandl a Rak, 2014).

4 KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost (dále jen „KB“ ve zjednodušení, představuje komplexní ochranu sítí před kybernetickými útoky a možnými hrozbami, jejíž cílem je zachovat bezpečnost informací. KB je tu již několik let, ale stále se rozvíjí a vznikají tedy nové hrozby, za zmínku stojí, že například i ve zdánlivě bezpečném systému je možné najít slabinu. ČR a EU se snaží přicházet s novým, efektivním řešením, to vše díky koordinaci a spolupráci na mezinárodní úrovni (Vláda ČR, 2022).

4.1.1 Typy informací

Každá organizace, bez rozdílu velikosti či oboru její působnosti, zpracovává určitý typ dat a informací. Cílem je identifikovat typy dat a informací, která mohou být zneužity. Data i informace se mohou vyskytovat v elektronické či papírové podobě. Podle toho jsou dále uložena na různých nosičích informací jako jsou například (Šulc, 2018):

- HDD, SSD disk počítače, servery, NAS/SAN nebo na cloudech.
- Přenosných nebo vyjímatelných médiích – optické disky (CD, DVD, BR), USB flash disky, pásky, SD a micro SD karty.
- Interní (ne)volatilní paměť.

Zde se nacházejí data a informace, které jsou vytvořené, zpracované a uložené za pomoci systému, programů nebo aplikací. Nejčastěji v podobě souboru v adresářové struktuře nebo databázi. Bez ohledu na formát dat, užití kódování a informace je níže výčet informací, které by mohli útočníka zajímat (Šulc, 2018):

Řízení lidských zdrojů:

- Osobní údaje zaměstnanců (osobní číslo, konkrétní informace, výše mzdy).
- Seznam, popis a obsazenost pracovních pozic.
- Motivační systém (systém hodnocení, bonusy).

Marketing, kde se jedná především o informace ohledně:

- Klientů nebo dodavatelích.
- Detaily o obchodech a plánech do budoucna.
- Nové produkty a služby.

- Přípravování marketingových kampaní.
- Průzkum trhu a analýzy.

Management:

- Strategické, taktické a operativní plány.
- Pracovní postupy.
- Dokumentace projektů.
- Bezpečnostní politika, směrnice a standardy.

Ve finančním řízení jde primárně o účetní doklady a výkazy.

ICT:

- Síťová infrastruktura (nastavení, dokumenty, hesla).
- Systémy, aplikace a databáze.
- Zdrojové kódy.

Facility:

- Plány budov.
- Umístění kamer, čidel a spínačů.
- Evidence členů ostražky a jejich úkoly.

4.1.2 Životní cyklus informace

Během celého životního cyklu (information life cycle), musí být informace speciálně chráněny nejen v úložišti (data at rest), ale také během jejich přenosu (data in motion) a při jejich používání (data in use). Pokud by nebyla data dostatečně chráněna, mohlo by dojít k narušení jejich důvěrnosti, integrity nebo dostupnosti. Podle důležitosti obsahu jednotlivých informací a dat jsou dle požadavků speciálně zabezpečena a chráněna (Šulc, 2018).

4.1.3 Cílené útoky

Jedná-li se o cílený útok (označován zkratkou APT) na konkrétní organizaci nebo osobu je hlavním cílem útočníka najít zranitelné místo v systému. Jakmile se útočníkovi podaří proniknout do systému, infikuje a ovládne zařízení pomocí RAT (Remote Access Tool)

backdoor. Díky použití RAT je schopný se přes vzdálený přístup připojit, vyhledat potřebná data a informace, popřípadě upravit vnitřní síť organizace pro napáchání škod. Citlivá data pak shromáždí, zašifruje a odešle na jiné zařízení (Šulc, 2018).

Předmět cílených útoků (Šulc, 2018):

- Krádeže citlivých informací (přihlašovací údaje, výrobní postupy, strategické plány).
- Převod finančního prostředků nakažením stroje, který slouží k přístupu do elektronického bankovníctví (ACH – Automated Clearing House, ETF – Electronic Funds Transfer).
- Otupení konkurence způsobením nedostupnosti služeb (útoky na e-shopy),
- Změna webových stránek (Defacement) společnosti nebo osobních stránek za účelem veřejného zesměšnění.
- Zneužití infrastruktury organizace k dalším útokům (SPAM, SCAM, phishing) nebo začlenění malware do webových stránek.
- Zprovoznění C&C serveru nebo Drop zone serveru k uložení odcizených dat na jiné místo.

Jak se bránit proti cíleným útokům:

Vlastník systému musí vynaložit nemalé úsilí a prostředky k zabezpečení a ochraně svého systému před různými typy útoků. Zato útočníkovi stačí najít drobnou vadu nebo slabé místo, kterého se dá zneužít. Pro tento účel je vhodné zavést systém řízení informační bezpečnosti (Šulc, 2018).

Opatření:

Jedná se o organizační a technická opatření, která by měla být začleněna v každé organizaci bez ohledu na jejich velikost a působnost. Pro opatření neboli protiopatření existuje řada synonym jako security measure, countermeasures, safeguard nebo controls. U všech vyjmenovaných termínů je hlavním cílem snížit riziko na akceptovatelnou úroveň (Šulc, 2018).

Podle způsobu implementace rozlišujeme opatření na (Šulc, 2018):

- Organizační (administrativní) – standardy, procedury a směrnice (definice pravidel a postupů), školení v informační bezpečnosti.

- Technická (fyzická či logická) – kontrola pohybu osob ve střežených prostorách, zabránění vstupu nepovoleným osobám, identifikace, autentizace, autorizace.

Technická se dále dělí na systémová, aplikační, databázová, komunikační, kryptografická.

- Systémová – úroveň operačního systému.
- Aplikační – úroveň aplikace.
- Databázová – úroveň databáze.
- Komunikační – aktivní síťové prvky.
- Kryptografická – implementace (ne)symetrické kryptografie.

Další časté způsoby opatření (Šulc, 2018):

- Preventivní (prevention) – zabránění realizace úmyslu a předejití nežádoucího jevu.
- Detekční (detection) – odhalení pomocí sensoru, kamer a logů.
- Reaktivní (reaction) – reakce na odhalení nežádoucí aktivity (defenzivní, ofenzivní).
- Odstrašující (detergent) – viditelná opatření sloužící k odrazení útočníka.
- Zdržující (delay) – zpomalení útočníka, detekce aktivity.
- Obnova (recovery) – obnovení funkce systému.

Kombinací různých prvků uvedených výše získáme sadu opatření proti útočníkovi. Například mříže a kamery jsou dobře viditelné a jejich odstranění zabere více času. Uvádí se také opatření (Šulc, 2018):

- Kompenzační (compensation) – nahrazení některých běžných nasazovaných opatření, které nelze použít.
- Direktivní (directive) – funkčnost jednotlivých opatření (údržba a kontrola).
- Nápravná (corrective) – zabránění opakování události (změna stávajícího procesu).

Aby byl systém bezpečný je důležité použít alespoň základní opatření a prosadit tzv. security-in-depth přístup, který spočívá v zavedení preventivních, odstrašujících, zdržujících, detekčních, reaktivních a obnovujících opatření na všech vrstvách IS (Šulc, 2018).

5 LEGISLATIVA A PRÁVNÍ PŘEDPISY

Stav běžného nebo mimořádného provozu a plnění funkcí vodohospodářské infrastruktury je ovlivněn širokou řadou faktorů. Důležitou část zde plní legislativa, která stanovuje podmínky, určuje kritéria nebo jednoduše plní funkci ověřených postupů k zajištění požadované úrovně pro provoz.

Právní předpisy tuto problematiku řeší a mohou na sebe jednotlivě navazovat. V průběhu sestavování, upravování a schvalování právních předpisů v ČR, které se zabývají vodohospodářskou infrastrukturou, je potřeba sledovat především místní podmínky, zdroje a potřebu tvorby nové legislativy. Důležitou roli plní směrnice vydané Evropskou unií (dále jen „EU“), které je potřeba respektovat a plnit. Zajímavostí mohou být následně různá doporučení mezinárodních organizací např. Světová zdravotnická organizace (dále jen „WHO“), které se zabývají danou problematikou, a to v celosvětovém měřítku. Jedná se ale spíše o nároky na kvalitu pitné vody, odvodu odpadní vody a s tím související zdravotní rizika. U nás je potom známé Sdružení oborů vodovodů a kanalizací ČR, z.s. (dále jen „SOVAK“).

5.1 Důležité směrnice a právní předpisy EU a ČR

Tyto směrnice jsou primárně zaměřeny na kvalitu a dodávky pitné vody při mimořádných událostech. Mezi ty hlavní zde patří (Tomek, Strohmandl a Rak, 2014):

- **Stanovisko Evropského hospodářského a sociálního výboru k návrhu směrnice Rady, která stanoví požadavky na ochranu zdraví obyvatelstva, pokud jde o radioaktivní látky ve vodě určené k lidské spotřebě KOM (2011) 385 v konečném znění – 2011/0170 (NLE)**, přijaté dne 27. června 2011, které navazují na Směrnici Rady 98/83/ES.
- **Směrnice rady 98/83/ES** ze dne 3. listopadu 1998 o jakosti určené pro lidskou spotřebu. Uvedená směrnice byla upravena nařízením Evropského parlamentu a Rady (ES) číslo 1882/2003 ze dne 29. září 2003 a číslo 596/2009 ze dne 18. června 2009. Základem směrnice je také doporučení od WHO a Vědeckého poradního výboru Komise pro zkoumání toxicity a ekotoxicity chemických sloučenin. Směrnice má za úkol chránit lidské zdraví před nepříznivými účinky jakéhokoli znečištění vody určené k lidské spotřebě.

- **Směrnice Evropského parlamentu a rady EU 2020/2184** ze dne 16. prosince 2020 o jakosti vody určené k lidské spotřebě.
- **Směrnice Evropského parlamentu a Rady 2000/60/ES** ze dne 23. října 2000, která stanovuje rámec pro činnost Společenství pro oblast vodní politiky. Cílem této směrnice je stanovit rámec pro ochranu vnitrozemských povrchových, pobřežních, brakických a podzemních vod.

Vodohospodářské infrastruktury je řešena především v zákoně o vodách, vodovodech a kanalizacích, směrnicích nebo dodatkových vyhláškách. Dále se v těchto předpisech řeší oblast ochrany kritické infrastruktury, krizové řízení, nakládání a hospodaření s vodou a integrovaný záchranný systém (dále jen „IZS“).

- **Zákon číslo 245/2001 Sb.**, o vodách a o změně některých zákonů (vodní zákon). Zákon má chránit povrchové a podzemní vody, stanovovat podmínky pro hospodárné využívání vodních zdrojů a pro zachování i zlepšení kvality povrchových a podzemních vod, dále také vytvořit podmínky pro snižování nepříznivých účinků povodní a sucha. Zákon zahrnuje zajištění bezpečnosti vodních děl v souladu s právem EU. Mezi další účel patří též přispívání na zajištění zásobování obyvatelstva pitnou vodou a k ochraně vodních ekosystémů a na nich přímo vázaných suchozemských ekosystémů. Upravuje tyto právní vztahy (Horáček, 2013).
- k povrchovým a podzemním vodám, vztahy fyzických a právnických osob k využívání povrchových a podzemních vod,
- k pozemkům a stavbám, s nimiž výskyt těchto vod přímo souvisí, a to v zájmu zajištění trvale udržitelného užívání těchto vod,
- bezpečnost vodních děl a ochrany před účinky povodní a sucha.

Zákon číslo 274/2001 Sb., o vodovodech a kanalizacích pro veřejnou potřebu a o změně některých zákonů (zákon o vodovodech a kanalizacích). Zákon upravuje vztahy při výstavbě, rozvoji a provozu vodovodů a kanalizací, které slouží pro veřejnou potřebu. Dále řeší přípojky na vodovodní řád a kanalizaci. Hodnota je zde také kladena na zájem o ochranu veřejného zdraví, ochranu životního prostředí a ochranu zdraví zvířat. V zákonu je obsažena i působnost orgánů územních samosprávných celků na tomto úseku, včetně příslušných správních úřadů.

Zákon neřeší oblasti týkající se vodovodů, které slouží pro rozvod jiné než pitné vody, oddílné kanalizace k odvodu srážkových vod (Odstavec předpisu 274/2001, 2022).

Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů (HOPKS), ve znění pozdějších předpisů.

Zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů, v platném znění.

Nařízení vlády č. 462/200 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.

Metodický pokyn Ministerstva zemědělství č. j. 74020/2016-MZE-15000 ze dne 22. prosince 2016, který ruší metodický pokyn Ministerstva zemědělství č. j. 102598/2001-MZE-15000 ze dne 30. 5. 2011, k zajištění jednotného postupu krajů, hlavního města Prahy, orgánů obcí s rozšířenou působností, orgánů obcí a městských částí hlavního města Prahy v systému nouzového zásobování obyvatelstva pitnou vodou při MU a za KS Službou nouzového zásobování vodou patří (Tomek, Strohmandl a Rak, 2014).

Metodický pokyn Ministerstva zemědělství ČR č. j. 21881/2002-6000 ze dne 21. června 2002 pro výběr a udržování zdrojů nouzového zásobování vodou k zajištění jednotného postupu orgánů krizového řízení krajů a okresů při výběru a zajištění zdrojů, které budou využity pro nouzové zásobování vodou, jejich zařazování do seznamu zdrojů nouzového zásobování vodou a následné udržování patří (Tomek, Strohmandl a Rak, 2014).

Nouzové zásobování pitnou vodou (Metodické doporučení SZÚ – Národního referenčního centra pro pitnou vodu) – ze dne 16. 7. 2018, č. j. SZU/02731/2018. Nahrazuje dokument „Nouzové zásobování pitnou vodou“ vydaný v roce 2007.

Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky. Zákon definuje body jako zajištění svrchovanosti a územní celistvosti, ochranu demokratických základů, ochrana zdraví, života a majetku jako základní povinnost státu.

Pro situaci, kdy bude narušena dodávka pitné vody, slouží tyto dokumenty pro řešení nouzového zásobování obyvatelstva pitnou vodou (Tomek, Strohmandl a Rak, 2014):

- Koncepce zabezpečení obyvatelstva pitnou vodou za krizových situací.
- Metodické doporučení Státního zdravotnického ústavu – Národního referenčního centra „Nouzové zásobování pitnou vodou“.
- ČSN EN 15975 – A1 Pro zabezpečení dodávky pitné vody.
- Metodické pokyny pro přípravu a realizaci regulačních opatření v systému HOPKS.

Tato odborná literatura se dále zaměřuje na oblast vodohospodářství a ochranu infrastruktury.

- TOMEK, Miroslav, Jan STROHMANDL a Jakub RAK. Zásobování obyvatelstva pitnou vodou za mimořádných situací. Praha: Academia, 2014. ISBN 978-80-7454-462-0.

Odborná publikace, která obsahuje cenné informace o technickém zabezpečení, postupy plánování, které slouží pro nouzové zásobování obyvatelstva pitnou vodou při krizových situacích. Literatura je vhodná především pro zaměstnance veřejné správy, učitelé nebo pro studenty v rámci rozšiřování znalostí v této oblasti. Nutné je také podotknout, že v rámci ochrany před terorismem může částečně sloužit jako pomůcka pro odhalení slabin vodohospodářské infrastruktury. To ale platí i na ostatní publikace zaměřené na toto téma.

- KROČOVÁ, Šárka. Strategie dodávek pitné vody. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 2009. Spektrum (Sdružení požárního a bezpečnostního inženýrství). ISBN 978-80-7385-072-2.

Díl ze série výtisků zaměřující se vodní hospodářství v ČR. Tento díl je zaměřen na nejdůležitější část veřejné infrastruktury v naší zemi, tedy strategii dodávek pitné vody. Stanovuje postupy potřebné pro zajištění dostatečného množství pitné vody za běžného stavu nebo při vzniku krizových situacích. Jsou zde uvedeny způsoby dopravy a distribuční sítě, monitoring účinnosti vodovodních sítí, požadavky pro veřejné vodovody, možná rizika a celkové požadavky na pitnou vodu. Je zde také část zaměřená na kapacitní účinnost hydrantů pro požární účely.

- HORÁČEK, Zdeněk, Miroslav KRÁL, Zdeněk STRNAD a Veronika VYTEJČKOVÁ. Vodní zákon s podrobným komentářem po velké novele stavebního zákona k 1. 1. 2013. Praha: Sondy, 2013. ISBN 978-80-86846-48-8.

Detailně zpracovaný rozbor vodního zákona. Zákon slouží jako ochrana povrchových a podzemních vody, ochrana vodních zdrojů, ochrana před povodněmi a popisuje vodní díla. Zákon také stanovuje výkon státní správy pro obce, obce s rozšířenou působností, kraje a další zapojené orgány. Obsahem jsou správní delikty při porušení povinností a společná ustanovení.

- TOMEK, Miroslav, Júlia JAKUBČEKOVÁ a Eleonóra BENČÍKOVÁ. Núdzové zásobovanie obyvateľstva pitnou vodou. Žilinská univerzita v Žilíně: EDIS, 2011. ISBN 978-80-554-0521-6.

Jde o vysokoškolskou učebnici, která poskytuje určité informace týkající se nouzového zásobování obyvatelstva pitnou vodou v případě mimořádných události nebo při krizových situacích, další části se týkají vodních zdrojů. Uplatnit ji lze v oblasti vzdělávání, pro veřejnou správu, hospodářským subjektů a veřejnosti.

- RADVANSKY, Robert a Allan MCDougall. Critical Infrastructure: homeland security and emergency preparedness. Boca Raton: CRC Press, 2010. 2nd ed. ISBN 978-14-2009-527-2.
- HAMILTON, Stuart a Ronnie MCKENZIE. Water Mananagement and Water Loss. British Library: IWA Publishing, 2014. ISBN 978-17-8040-635-0.

Zahraniční literatura zaměřená na distribuci pitné vody a její úbytky při čerpání a distribuci v sítích. V publikaci se začíná s částí o potrubí pro nízký a vysoký tlak vody, včetně jejich spojů. Následuje výpis technologií pro zjišťování a měření úniku vody ze systému s navazujícím management principů tlaků. Stanovuje se zde otázka v oblasti rozhodování pro opravu či nahrazení jednotlivých částí. Část je zde vyhrazena pro software podporu v rámci detekce a měření úniku z okruhu. Publikace je zaměřena na Spojené státy americké, ale v rámci informačního průzkumu poskytuje i informace ze zahraničí, konkrétně se jedná o Bosnu a Hercegovinu, Chorvatsko a Srbsko.

6 TERORISMUS

Celosvětově známý pojem, který není nikde přesně definován jako konkrétní význam. Může představovat jistou formu násilných činností a protiprávního jednání, které lidská společnost odsuzuje. Vyskytuje se v každé lidské společnosti, lze jej vnímat jako doprovodný jev, kdy se využívá pro dosažení vlastních cílů nebo jako řešení konfliktů. Projevy násilí můžeme v tomto smyslu považovat za jistý druh nekontrolované zbraně, pro nás tedy jisté riziko (Brzobohatý, 1999).

Vypracovaná studie od OSN pro oblast terorismu obsahovala 1866 stran, nikde ale není jednotně stanovena definice pro terorismus. Jeden ze zásadních bodů, proč není možné vytvořit jednu pevnou definice pro tento pojem, je rozvíjející se charakter a pohled na terorismus, jednoduše se terorismus stále mění (Souleimanov, 2010).

6.1 Právní dokumenty Evropské unie a České republiky v oblasti terorismu

Pro ochranu a prevenci proti terorismu bylo a je zapotřebí právně ukotvit společný cíl proti této nežádoucí aktivitě. Jedná se tedy o zákony, právní dokumenty, audity apod. Jsou tvořeny na úrovni státní nebo na úrovni EU. Mezi ty nejdůležitější můžeme zařadit (Audit národní bezpečnosti 2016, Evropská bezpečnostní strategie, 2009; Stockholmský program; Strategie ČR pro boj proti terorismu, 2013; Strategie EU pro boj proti terorismu; Zákon č. 110/1998 Sb. o bezpečnosti ČR):

- **Evropská bezpečnostní strategie** – jako jedna z prvních stanovila zásady a cíle pro prosazování bezpečnostních zájmů EU na základě společných základních hodnot ve společnosti. Staví komplexní přístup a současně je plně relevantní. Poskytuje příležitosti pro výzkum této oblasti, tedy pokrok v praxi a možnost pro zlepšení do oblasti bezpečnosti prostředí.
- **Strategie EU pro boj proti terorismu** – která se zakládá na čtyřech pilířích: prevenci, ochraně, pronásledování a reakci. V souvislosti s těmito pilíři je ve strategii kladen důraz především na hodnotu spolupráce se zeměmi třetího světa a na spolupráci s jednotlivými mezinárodními organizacemi.
- **Stockholmský program** – se zaměřuje na určení priorit EU v oblasti práva, svobody a bezpečnosti v období let od 2010 až do 2014. Navazuje na výsledky z programu z Tampere nebo Haagský program. Cílem je reagovat na budoucí rizika

a posílit tak prostor bezpečnosti, práv a svobod. Opatření, které jsou stanoveny v rámci programu, by se měla zaměřovat na zájmy a potřeby obyvatel státu.

- **Audit národní bezpečnosti 2016** - komplexní dokument, který obsahuje bezpečnostní politiku státu ČR pro aktuální bezpečnostní hrozby a související oblasti. Je schvalován vládou ČR.
- **Strategie ČR pro boj proti terorismu od roku 2013** – představuje dokument, který koncipuje Ministerstvo vnitra České republiky, k opatřením zaměřených na minimalizaci rizik a dopadů možných teroristických útoků na území ČR a proti zájmům ČR v zahraničních oblastech.
- **Zákon č. 110/1998 Sb. o bezpečnosti ČR** – upravuje oblast v rámci bezpečnosti ČR prostřednictvím regulace krizových stavů (nouzový stav, stavu ohrožení státu a válečný stav). Na jeho základě zřizuje Bezpečnostní radu státu a umožňuje zkrácené projednávání vládních návrhů pro vznik a uplatnění zákonů. Patří do celku ústavního pořádku ČR.
- **Zákon č. 253/2008 Sb. o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu** – zapracovává příslušné předpisy Evropských společenství, rovněž navazuje přímo na použitelné předpisy Evropských společenství a upravuje opatření, které jsou proti legalizaci výnosů z trestné činnosti a financování terorismu. Upravuje také některá práva a povinnosti fyzických a právnických osob při uplatňování opatření proti legalizaci výnosů z trestné činnosti a financování terorismu, a to za účelem omezit a bránit zneužívání finančního systému k legalizaci výnosů z trestné činnosti a financování terorismu. Zahrnuje rovněž tvorbu podmínek potřebných pro odhalování daného počinání.

6.2 Terorismus v České republice

Pro sledování možností teroristické hrozby na území ČR je potřeba nahlédnout do historie státu a jeho aktivit, které se odehrály v zahraničí. Tehdejší Československo sehrálo neblahou roli země, která pro „světovou revoluci“ vysílala vlastní, případně školila nebo nabízela útočiště protizápadně orientovaným zahraničním teroristům. To vše před rokem 1989 (Terorismus – MV ČR).

Významnou oblastí pro teroristické hrozby v ČR je vstup ČR do EU a NATO. Těmito kroky došlo k vyjasnění postoje země jako spojence USA a západní Evropy. Tyto události vedou tedy k rozšíření řad našich potenciálních nepřátel (Terorismus – MV ČR).

Na základě informací není ani možné vyloučit, že v islámských řadách teroristů nemohou být lidé, kteří patří mezi občany ČR, ale pocházejí původně z islámských zemí. Znají tedy dobře místní prostředí a mohou představovat větší hrozbu. K zamyšlení je možnost, že část lidí mohou být agenti, kteří pouze čekají na příležitost a mezitím vytvářejí tajnou síť (Terorismus – MV ČR).

Zatím ale nedošlo na území ČR k teroristickému útoku jako například ve Francii nebo Německu. Klasický terorismus s vazbou na širší mezinárodní seskupení se zde tedy neprojevil. Nedošlo ani k teroristickému útoku s cílem dosáhnout určitého cíle s kladením podmínek, tedy vyhrožování (Terorismus – MV ČR).

Za zmínku zde stojí, že terorismus se zde projevil především jako aktivita jednotlivce, kdy se jednalo o cílené útoky na osoby nebo firmy, nešlo tedy o extrém, který by měl za cíl zranit či usmrtit co nejvyšší počet osob nebo ochromit zásadní část infrastruktury s vážným dopadem na stát. Celková situace ohledně terorismu je v ČR velmi příznivá, ovšem je potřeba být stále připraven a neustále hledat slabá místa, která by v případě náhlé změny v geopolitice a zvýšení teroristické hrozby, mohla představovat potenciální riziko.

6.3 Charakteristika a typologie terorismu

Jako všechno ostatní má i terorismus jisté charakteristika a vyznačení. Jeho specifické rysy jej oddělují od běžných občanských povstání a převratů nebo válečných konfliktů.

Subverzivní terorismus – můžeme sledovat v podobě násilného boje (tato oblast nezahrnuje kyberprostor). Představuje akce proti držitelům moci. Jednotky jsou tvořeny v malých počtech zhruba 10 osob. Výzbroj a taktika jsou především ruční zbraně a výbušniny, použité pro atentáty, držení rukojmí nebo poškození infrastruktury. Dopad je vždy směřován na psychickou stránku osob (Mareš, 2005).

V rámci rozsahu aktivity terorismu jej můžeme dělit na (Mareš, 2005):

- **Mikroterorismus** – intenzita útoků je nízká, dochází pouze k nepodstatným škodám, u osob dochází více ke zranění než smrti, v případě počtu obětí se bavíme nejvýše o desítkách obětí.

- **Mezoterorismus** – intenzita útoků je na střední úrovni, škody na majetku jsou významné, počty obětí se pohybují v řádu stovek.
- **Makroterorismus** – intenzita útoků je nejvyšší možné úrovni, škody na majetku významně zasahují do sociální a ekonomické stability státu a kraje, počty obětí jsou v řádech tisíců.

Pro menší pochopení rozvoje terorismu se můžeme podívat na tabulku č.1, kde je srovnání tradičního a nového terorismu.

Tabulka 1: Charakteristika tradičního a nového terorismu

Terorismus	Tradiční	Nový
Organizace	Jednoznačná	Hůře určitelná
Struktura	Převážně hierarchická	Převážně lineární
Operační efektivita	Středně profesionální úroveň	Plně profesionální úroveň
Síla skupiny	Malá až středně velká	Individuální případně malá
Náborový potenciál	Silně omezený	Vysoký potenciál skrze internacionalizaci
Oblast operace	Národně a regionálně omezena	Mezinárodní úroveň
Cíle operace	Předvídatelné	Těžce předvídatelné a identifikovatelné
Počet obětí	Vybrané, střední počty obětí	Vysoký počet obětí
Kvantitativní rozměr hrozby	Omezený skrze vztah ke konkvencím a efektu	Vzrůstá se vztahem ke konkvencím a efektu
Motivace k veřejnému přihlášení	Vysoká	Nízká, klesající
Financování	Nedostatek, často způsob vydírání nebo únos, revoluční daň (ETA)	Lepší finance díky celosvětovému transferu kapitálu a legálním obchodním aktivitám
Spojení s organizovaným zločinem	Velmi malé	Intenzivní spojení, migrační společenství, legální oblasti obchodu

Zdroj: Straßner, 2003

6.4 Teroristické hrozby pro vodohospodářskou infrastrukturu

Jako všechno i vodohospodářská infrastruktura je zranitelné v různých oblastech. Především se jedná o poškození až zničení objektů, staveb a zařízení pomocí výbušnin, poškození klíčových úseků nebo rozsáhlé poškozování drobných prvků. Další klíčovou oblast tvoří kybernetická bezpečnost, kde se jedná o napadení infrastruktury v kyberprostoru, kdy následky často přechází do reálného prostoru.

Útoky proti významným cílům – jsou vedené proti významným cílům a prováděny na základě pečlivého výběru cílového objektu. Důležitost objektu pro útok spočívá ve výsledných důsledcích útoku, nejde tedy o samotný cíl útoku, ale výsledný dopad útoku. Nejčastěji jsou za cíl voleny elektrárny, průmyslová centra, vysoce postavené osoby, kritická infrastruktura, vládní budovy nebo právě pro nás zajímavá vodohospodářská infrastruktura (Brzobohatý, 1999).

Bombový útok – útok za pomoci výbušnin či celých výbušných systémů patří do skupiny nejčastějších typů útoku ze strany teroristů. Výbušniny zajišťují vždy téměř 100% splnění daného cíle, tedy je zde vysoká úspěšnost akce samotné. Výhodou je také malá pravděpodobnost odhalení pachatele, hlavně pokud není žádný digitální záznam nebo popis svědků o možném pachateli. Zároveň je možné bombové útoky rozdělit na čtyři kategorie (Brzobohatý, 1999):

- Proti osobám.
- Proti symbolickým cílům.
- Proti významným cílům.
- Série útoku (někdy označovány jako kampaně).

Za zmínku stojí ještě hrozba použití výbušniny, kdy jde převážně o planou hrozbu, ale jejím cílem je vyvolat strach, obavy, zmatek a nejistotu. Podobný účinek má poté položení falešné bomby, kdy je potřeba již postupovat ze strany dotčených osob a objektů jako při skutečné bombě. Efekt zastrašení je možné poté znásobit skutečným použitím bomby.

CBRN terorismus – chemický, biologický, radiologický a jaderný (dále jen „CBRN“) terorismus, který často označuje jako superterorismus nebo ultraterorismus, je brán jako druh terorismu, kdy dochází k použití zbraní hromadného ničení. Zhodnocení potencionálních a aktuálních zdrojů a forem CBRN terorismu je důležité pro samotnou prevenci a boj s tímto druhem terorismu. Zásadní je tvorba odpovídajících systémů na

národní, regionální a globální úrovni. Současně je nutné přijímat opatření preventivní, represivní, ochranná, nápravná a záchranná (Matoušek, Benedík, Linhart, 2007).

Bioterrorismus – jedná se o úmyslné zneužití biologických agens nebo toxických látek pro ovlivnění lidského nebo zvířecího zdraví v negativním směru. Často je s tím spojena motivace ze strany politiky, náboženství nebo ideologie (Klement, Mezencev, Bajgar, 2013).

6.5 Ochrana proti terorismu

Základem pro funkční obranu je vždy znalost protivníka. Je tedy nutné mít přehled o jeho potencionálních možnostech, strategii, taktice, síle, schopnostech a metodách. Je tedy nutné mít co největší možný přehled, mít dostatečné množství informací a dat pro vyhodnocení, toto jsou nezbytné podmínky pro zpracování efektivního a funkčního plánu pro ochranu a obranu. Řada informací je poskytována ze strany zpravodajských služeb, příkladem může být Bezpečnostní informační služba ČR, která se zaměřuje na tyto možné hrozby. Další zdroje informací mohou být knihy, odborné časopisy a publikace. Méně známý způsob je například rozhovor s odborníkem v dané oblasti (Brzobohatý, 1999).

Efektivní taktika, které se osvědčila, je sledování a vyhodnocování přichozích dat (výhružné dopisy apod.). Je také důležité sledovat aktuální trendy v oblasti terorismu, především sledovat aktuální cíle těchto skupin. Taktika i prostředky pro obranu by následně měly vycházet z úrovně hrozcícího nebezpečí. Svou roli hraje také finanční balanc, tedy kolik je vynaloženo financí na obranu objektů, jestli není obrana podhodnocena nebo naopak opatření převyšují požadavky. Vhodné je tedy mít zpracovaný plán pro ochranu objektů, prvků, zařízení a systémů (Brzobohatý, 1999).



Obrázek 3: Kdo je terorista a kdo ne?

7 TECHNICKÁ A MECHANICKÁ OCHRANA OBJEKTŮ

Člověk se už pradávna snaží chránit své území všemi dostupnými prostředky a chránit tak své nebo kolektivní hodnoty. V dnešní době je to velice složitý a komplexní úkol, který může začínat jako snadné oplocení objektu a končit až u elektronicky provázaného bezpečnostního systému, který je téměř neproniknutelný a nabízí vysoký stupeň ochrany v důsledku stálého pokroku technologií. Ochrana objektů začíná již na první pohled z vnější části objektu, kde jsou nejčastěji mechanické ochranné systémy pro odrazení pouhých zvědavých jedinců. Čím blíže ale jdeme k prvku, jenž je potřeba chránit, tím roste úroveň zabezpečení, tedy se stupňují nároky na jeho překonání. První roli tedy hraje pouhé odrazení, kdy se ochrana stupňuje a jejím cílem je minimálně co nejvíce stupňovat obtížnost pro vstup do objektu a nejlépe tomu činu úplně zamezit.

7.1 Integrovaný bezpečnostní systém

Každý systém, v tomto konkrétním případě integrovaný bezpečnostní systém, je složen z řady technických a organizačních prvků, které jsou mezi sebou navzájem propojeny a bez nichž by systém nedosahoval požadovaných výsledků (Uhlář, 2005).

Integrovaný bezpečnostní systém (systémově užívaná zkratka: IBS) je tvořen ze tří základních prvků (Uhlář, 2005):

- První prvkem struktury IBS jsou mechanické zábranné systémy (systémově užívaná zkratka: SM);
- Druhým prvkem struktury IBS jsou signalizační zařízení a monitorovací prostředky (systémově užívaná zkratka: SE);
- Posledním prvkem struktury IBS jsou organizační opatření a ostraha (systémově užívaná zkratka: SO).

Každý z výše uvedených prvků má v IBS svou funkci:

- a) **Mechanické zábranné systémy (SM)** tvoří první linii obrany při narušení objektu. Cílem mechanického zábranného systému je vytvořit překážku, která zabráni útočníkovi proniknout do zabezpečeného objektu či jiného chráněného prostoru. Účinnost mechanického zábranného systému se vyjadřuje pomocí vzorce:
- b) **Signalizační zařízení a monitorovací prostředky (SE)** zaznamenávají informace o narušení nebo pokusu o narušení SM a následné informace dále předává centrále. Informace o napadení chráněného objektu by ideální případě měly obsahovat bližší

údaje o útočnickovi, napadené pozici a způsobu, jakým se útočník rozhodl proniknout do objektu. Informace by měli být následně předány centrále (systému organizačního opatření a ostraze). Často se ovšem můžou informace o napadení objektu prezentovat pouze formu zvukového signálu, jako je například alarm u osobního automobilu, který pouze informuje své nejbližší okolí o napadení chráněného objektu, ale nepředává jakékoliv podrobnější informace.

- c) **Organizační opatření a ostraha (SO)** mají za úkol vyhodnocení informací získaných od SE o narušení objektu. Systém organizačního opatření a ostrahy na základě získaných informací od SE provede hodnocení nastalé situace a provede kroky nutné k navrácení stavu před napadením chráněného objektu. Cílem SO je rovněž udržovat rovnováhu celého integrovaného bezpečnostního systému a pokusit dosáhnout optimální bezpečnosti.

Optimální bezpečnost je stav, kdy jsou všechny hlavní prvky integrovaného systému rozděleny tak, že poskytují maximální možnou míru ochrany chráněného objektu.

Integrovaný bezpečnostní systém má smysl pouze v případě, že je schopen útočnickovi zabránit způsobit škodu na chráněném zájmu (Uhlář, 2005).

7.2 Zabezpečovací systémy

Zabezpečovací systémy v posledních desetiletích prošly nezanedbatelným vývojem kupředu, díky kterému jsou zabezpečovací systémy účinnější než kdykoliv předtím. Zabezpečovací systémy se staly významným prostředkem k potírání trestné činnosti. Díky dnes již zcela běžnému používání zabezpečovacích systémů k ochraně chráněného zájmu, je již spousta procesů využívající zabezpečovací systémy zbytečná. Přesto je stále žádoucí, aby tyto procesy byly nadále zkoumány z koncepčního, taktického nebo z technického hlediska a získané výsledky byly nadále uplatňovány k neustálému vylepšování zabezpečovacích systémů, jenž povedou k lepší ochraně chráněného zájmu.

Zabezpečovací systém je soubor opatření a procesů nutných k ochraně chráněného zájmu. Opatření a procesy, zajišťující požadovanou bezpečnost chráněného zájmu, jsou poskytovány v rovině organizačních, technických a taktických opatření. Při bližším pohledu je možné opatření a procesy tvořící zabezpečovací systém rozdělit na dvě navzájem se ovlivňující hlediska (Uhlář, 2005):

- Operační hledisko.
- Technické hledisko.

7.3 Základní druhy ochrany

Existují základní čtyři druhy ochrany. K nejlepšímu možnému zabezpečení ochrany chráněného objektu je vždy nutné provádět ochranu komplexně, tedy se zapojením všech základních druhů ochrany. Základní druhy ochrany jsou (Uhlář, 2005):

- Klasická ochrana.
- Režimová ochrana.
- Fyzická ochrana.
- Technická ochrana.

7.3.1 Klasická ochrana

Je vývojově nejstarší typ ochrany a je využívána člověkem téměř od jeho vzniku. Princip klasické obrany spočívá ve využití mechanických zařízení, která jsou schopná ochránit chráněný objekt. Jedná se o vytváření různých zábran, překážek apod., která mají za cíl zabránit poškození nebo odcizení chráněného zájmu. Případně je úkolem daných zábran a překážek co nejvíce zkomplikovat pachateli dostání se k jeho cíli.

Klasická ochrana měnila svou podobu v závislosti na technické úrovni civilizace. V době kamenné a bronzové měla klasická obrana např. formu palisádového opevnění a příkopů kolem tehdejších obydlí obyvatel. Z období středověku jsou neznámějším příkladem klasické ochrany majestátní hrady postavené na těžko dobytých pozicích nebo kované truhlice. V dnešní době má klasická obrana především formu různých plotů a zámků, jenž chrání chráněný zájem před zloději apod. Historie nám ovšem ukázala, že ať má klasická ochrana jakoukoliv manifestaci, nikdy není schopna poskytnout stoprocentní ochranu chráněnému zájmu a způsoby, jak klasickou ochranu překonat kráčeli vždy bok po boku vývoje klasické ochrany. Zřejmě nejzářivějším příkladem jsou opět nedobytné kamenné hrady a pevnosti, které i přes svou majestátnost bylo možné pomocí obléhacích strojů dobýt (Uhlář, 2005).

S klasickou obranou se setkáváme dennodenně v různé podobě téměř u každého objektu. Klasická obrana je totiž základním stavebním prvkem každého zabezpečovacího systému. V mnoha případech je klasická ochrana brána rovněž jako jediná potřebná ochrana, přestože ochrana objektu může být posouzena pouze z hlediska doby, kterou potřebuje útočník k překonání mechanického zábranné systému a vniknutí do chráněného objektu. Klasická obrana by v nejlepším možném případě měla být zkombinována s ostatními druhy ochrany k dosažení co největší ochrany (Uhlář, 2005).

7.3.2 Režimová ochrana

Rozdíl od klasické ochrany nezajišťuje režimová ochrana mechanické zabezpečení chráněného objektu, ale zabývá se organizačními a administrativními opatřeními a rovněž postupy, které zajišťují správné plnění funkce ochrany chráněného objektu. Režimová ochrana koordinuje a sladuje postupy zbývajících tří druhů ochrany k zajištění jejich největší efektivity s co nejmenším odporem mezi sebou navzájem (Uhlář, 2005).

S režimovou ochranou se nejčastěji setkáme ve formě vnitřních předpisů a směrnic podniků a organizací. Přesto, i když má podnik či jiná instituce soukromého nebo státního charakteru směrnice upravující režimovou ochranu, může být celková bezpečnost chráněného objektu na nízké úrovni, pokud nejsou procesy a postupy ve směrnici režimové ochrany implementovány nebo pokud není jejich pravidelně kontrolováno jejich řádné plnění (Uhlář, 2005).

Režimovou ochranu dělíme na vnější a vnitřní (Uhlář, 2005):

- Vnitřní ochrana řídí procesy ochrany uvnitř chráněného objektu. V praxi se jedná například o pravidla pro vstup a výstup do objektu, pravidla pro pohyb uvnitř objektu, pravidla pro návštěvníky, možnost s nakládáním s informacemi atd.
- Vnější režimová ochrana nalezne uplatnění třeba při přepravě chráněného aktiva mezi chráněnými objekty.

7.3.3 Fyzická ochrana

Je stářím velmi blízko klasické ochraně. Princip fyzické ochrany spočívá v tom, že chránění objekt je přímo na místě hlídán/ chráněn fyzickou osobou. Většinou se hlídáním chráněného objektu účastní vrátní, hlídači, strážníci, policie atd. Fyzická ochrana je prozatím nejlepším druhem ochrany, protože zbylé ochrany jsou stejně v konečném důsledku závislé na reakci lidského faktoru. V případě fyzické ochrany je lidský faktor na místě. Přesto fyzická ochrana je ze všech druhů ochrany finančně nejdražší a z legislativního hlediska nejméně ošetřená. Osoba zajišťující fyzickou ochranu chráněného objektu v případě, že nejedná o příslušníka policie apod. nemá žádné vyšší pravomoci oproti běžnému občanovi. Ostraha smí pachatele, který se snaží proniknout do chráněného objektu, pouze zadržet do příjezdu PČR (Uhlář, 2005).

7.3.4 Technická ochrana

Patří k nejmladším ze všech druhů ochrany a vznikla díky rozvoji technologií, které vytvořilo zcela nové možnosti v oblasti zabezpečení objektů a prostor. Rovněž ze všech

výše zmíněných ochran se jedná v poměru cena / výkon o nejúčinnější formu ochrany. Avšak technická ochrana je účinná pouze v případě, že užitá jako podpora klasické ochrany nebo případně fyzické ochrany (Uhlář, 2005).

Technická ochrana totiž ve své podstatě není ochranou v pravém slova smyslu. Jedná se o prostředky technického charakteru, převážně různá detekční zařízení, která sbírají informace o chráněném prostoru a tyto informace jsou přeposílány na informační středisko. Jedná se o prostředky typu snímače pohybu, kamery, fotopasti, různá čidla apod., která reagují na změnu v chráněném prostoru. Informace o změně v chráněném prostoru mohou uvést v akci policejní síly apod., které jsou schopny zabránit pachateli v další trestné činnosti (Uhlář, 2005).

Prostředky technické ochrany jsou dnes snadno dostupné a díky tomu jsou i velmi rozšířené. Mnohdy jsou majitelé chráněných objektů vybaveni technickou ochranou přesvědčeni, že se jedná o naprostou ochranu. Bohužel i technická ochrana není dokonalá, za nesplnění její funkce je velmi často na vině především její nesprávná instalace, která může mít pro majitele objektu i nepříjemnou právní dohru (např. když kamerový systém zabírá pozemek souseda). Pro správné fungování je třeba si uvědomit, že hlavními úkoly technické ochrany jsou především podpora klasické ochrany anebo zvyšování efektivity fyzické ochrany (Uhlář, 2005).

7.4 Hledisko prostorového zaměření

Oblast technické ochrany objektů dělíme na 5 druhů, jedná se o ochranu typu (Uhlář, 2005):

- **Obvodová** – slouží pro signalizaci v případě narušení obvodu objektu. To značí jeho vymezené hranice za pomoci umělých nebo přírodních bariér (ploty, zdi, příkopy apod.) Jedná se převážně o venkovních technické prvky určené pro vnější ochranu (Uhlář, 2005).
- **Plášťová** – slouží pro signalizace při porušení mechanických překážek tedy pláště objektu. Zabýváme se samostatným objektem nebo určitými prostory. Jedná se o narušení konvenčních i nekonvenčních vstupů (Uhlář, 2005).
- **Prostorová** – slouží pro varování možných událostí s charakterem nebezpečí v dané oblasti. Neoprávněná osoba se již vyskytuje v chráněné oblasti. Zabezpečovací čidla detekující pohyb jej detekují jen v bezprostředním prostoru kolem objektů (Uhlář, 2005).

- **Předmětová** – někdy také jako bodová ochrana nám značí jasnou přítomnost neoprávněné osoby u chráněného prvku v případě napadení nebo i při neoprávněné manipulaci s chráněným předmětem.
- **Klíčová** – nám odhaluje narušení v oblastech možného pohybu neoprávněných osob jako jsou schodiště, chodby apod. (Uhlář, 2005).

Zkombinováním jednotlivých typů ochrany je možné dosáhnout vícestupňové úrovně ochrany. Ovšem vždy záleží na podmínkách: co chceme chránit, jak moc to musíme chránit a kolik do toho můžeme investovat.

8 CÍL A METODIKA PRÁCE

Použité metody jsou (Závěrečné práce – metodika, 2013):

- **Analýza** – „je proces reálného nebo myšlenkového rozkladu zkoumaného objektu (jevu, situace) na dílčí části, které se následně stávají předmětem dalšího zkoumání. Jde o rozbor vlastností, vztahů, faktů postupující od celku k částem. Analýza předpokládá, že v každém jevu je určitý systém (množina prvků, mezi nimiž jsou vztahy a které tvoří daný celek) a platí v něm ustálené zákonitosti fungování systému. Proto analýza umožňuje odhalovat různé vlastnosti jevů a procesů. Analýza má nepostradatelnou roli v rámci poznávání podstaty jevů a pro stanovení taktiky vědeckovýzkumné činnosti. Analýza (a interpretace) se prolíná průběhem kvalitativního výzkumu a je nedělitelnou součástí každého jejího jednotlivého kroku. Analýza patří, spolu se syntézou, mezi základní a nejpoužívanější vědecké metody.“
- **Dedukce** – „jde opačným směrem než indukce – postupem od méně obecného k obecnějšímu. Jde však o přesnější vyvozování nových tvrzení při dodržování pravidel logiky. Dedukce je proces, ve kterém testujeme, zda vyslovená hypotéza je schopna vysvětlit zkoumaný fakt.“
- **Indukce** – „je vyvozování obecného (teoretického) závěru na základě poznatků o jednotlivostech. Indukce umožňuje dojít k podstatě jevů, stanovit jejich zákonitosti. Induktivní závěr lze považovat za hypotézu, protože nabízí vysvětlení, i když těchto vysvětlení může být v praxi více. Závěry induktivních myšlenkových pochodů jsou vždy ovlivněny subjektivními postoji (zkušenostmi, znalostmi) a mají proto omezenou platnost. Východiskem indukce je statistické zpracování a vyhodnocení údajů, na jejichž základě formulujeme obecnější závěry platné pro zkoumanou oblast.“
- **Pozorování** – „je základem jakékoli výzkumné metody. Na rozdíl od běžného pozorování je systematické – jde o záměrné (má vytýčený cíl pozorování) a plánovité (předem je stanovena doba nebo počet pozorování) sledování určitých jevů a zákonitostí. Výsledkem pozorování je nejen popis skutečnosti ale i její vysvětlení.“
- **Syntéza** – „je myšlenkové spojení poznatků získaných analytickými metodami v celek. Syntéza je základem pro pochopení vzájemné souvislosti jevů. Syntéza je sumarizací poznatků vedoucí k získání nových poznatků, vztahů a zákonitostí ve kvalitativně vyšší úrovni – vede k objasňování nových nebo dříve nedefinovaných vztahů a zákonitostí.“

Pro zpracované analýzy jsem použil následující metodu (SWOT analýza, 2022):

- SWOT analýza – jde o vysoce efektivní a jednoduchá analýza pro zjištění skutečného stavu, žádaných změn, možných rizik a nutných kroků pro přeměnu slabých stránek na silné. Je to komplexní metoda kvalitativního vyhodnocení veškerých relativních stránek definovaného tématu. Zahrnuje kroky technik strategické analýzy. Často ji lze vidět jako součást důležitých strategických dokumentů.

Základem metody je definice a hodnocení jednotlivých faktorů, které jsou definovány na čtyři kategorie: Strengths (silné stránky), Weaknesses (slabé stránky), Opportunities (příležitosti), Threats (hrozby).

Silné a slabé stránky jsou považovány za vnitřní faktor. Příležitosti a hrozby následně tvoří vnější faktor (SWOT analýza, 2022).

II. PRAKTICKÁ ČÁST

9 SOUČASNÝ STAV BEZPEČNOSTI VODOHOSPODÁŘSKÉ INFRASTRUKTURY PRO VAK HODONÍN, POVODÍ MORAVY

Současný stav v oblasti bezpečnosti pro vodohospodářskou infrastrukturu je v klidovém stavu. Tedy aktuálně není zájem ze strany potencionálních útočníků, provádět útoky na tuto část infrastruktury. Důvodů může být několik, s největší pravděpodobností se jedná o upřednostnění jiných cílů, které nabízejí snadnější provedení a rychle dosažitelné výsledky. Další roli hraje zabezpečení této infrastruktury, kdy se její ochrana stále posunuje směrem vpřed ve všech směrech, v dnešní době hlavně po stránce kybernetické bezpečnosti, a zvyšuje tak svoji odolnost vůči možným teroristickým hrozbám. Společnosti investují nemalé finanční prostředky do oblasti zabezpečení a ochrany svých objektů, systémů a personálu.

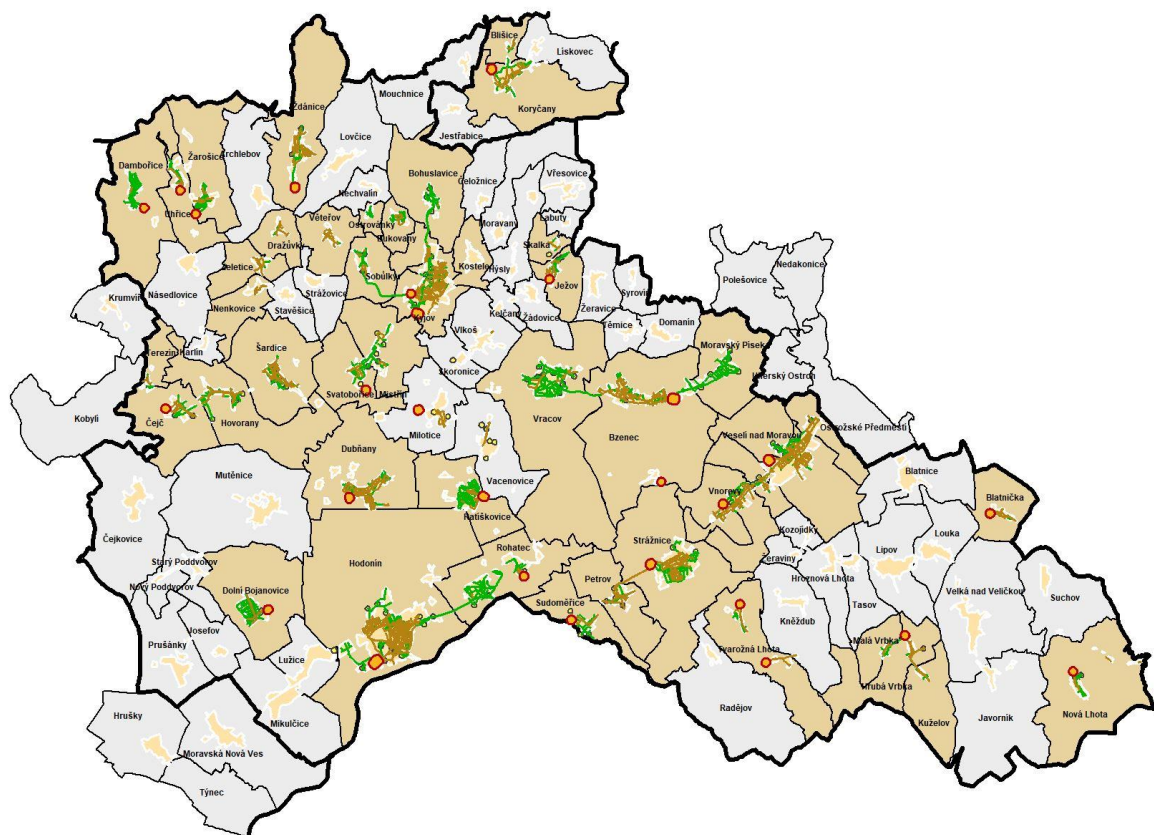
9.1 VODOVODY A KANALIZE HODONÍN

Vodovody a kanalizace Hodonín a.s. (dále jen „VaK Hodonín“) představují akciovou společnost v oblasti zásobování kvalitní pitnou vodou pro obyvatelstvo a průmysl. Vize společnosti, kterou se řídí v současnosti a míří s ní k budoucnosti (VAK Hodonín, 2022).

„Jsme a budeme inovativní, moderní, ryze českou společností, vlastněnou městy a obcemi regionu, ve kterém společně žijeme. Denně Vám do Vašich kohoutků dodáváme kvalitní a zdravou pitnou vodu, kterou po jejím použití vracíme čistou do přírody. Tak, dle našich možností, přispíváme k trvalému uchování zdravého životního prostředí na Hodonínsku.“ (VaK Hodonín, 2022).

Zaměřuje se na vyhledávání, zaváděné nové a pokrokové technologie s cílem směřovat k úsporným opatřením v oblastech energií a chemikálií, v rámci zlepšování produktů a poskytovaných služeb. Vodě věnuje maximální pozornost, především v oblastech technologie úpravy, distribuce, kontroly a v neposlední řadě její ochraně. To stejné platí pro oblast čištění odpadních vod a technologiím v této oblasti. Cíl je pak maximální kvalita vyčištěné vody, která se vrací zpět do vodních toků a přírody. Společnost se rovněž staví za oboustrannou efektivní komunikaci (VaK Hodonín, 2022).

Vznik společnosti se datuje k roku 1950, kdy se na základě vládního usnesení z téhož roku, došlo v oblasti státní správy k rozdělování funkce orgánů, došlo k oddělení správních a hospodářských činností. Krajské výbory byly nuceny zřídit tzv. Krajskou vodohospodářskou službu. V letech 1954 došlo k další reorganizaci v oblasti vodního



Obrázek 5: Mapa působnosti VaK Hodonín a.s. – Kanalizační síť

Zdroj: VaK Hodonín, 2022

9.2 Ochrana a bezpečnost

Ochrana vodohospodářské infrastruktury, především v oblasti výroby a distribuce pitné vody, představuje složitý organizační celek. Kde jsou jednotlivé prvky pro zajištění ochrany provázány. Důležitost ochrany je zde na vysoké úrovni.

Objekty jsou zabezpečeny systémem ASSET a LATIS SQL. Jedná se o systémy určené pro ochranu a zabezpečení objektů na základě aplikace moderní technologie a výzkumu. Současně plní státní a evropské normy pro oblast bezpečnosti. Systém komunikace mezi jednotlivými prvky se dost podobná a komunikuje se systémem PČR.

Představuje to integrovaný bezpečnostní systém. Je to kombinace softwarového zajištění a hardwarových prvků, řeší bezpečnost a kontrolu objektů. Systém je napojen na dohledové a poplachová přijímací centra, poplachové zabezpečovací a tísňové systémy, elektronickou kontrolu vstupů, kamerové systémy a požární signalizaci. Spolupráce zde probíhá s PČR, konkrétně se jedná o skupinu technické ochrany. Společnosti mají tedy vypracovanou

dokumentaci bezpečnostních systémů pro jednotlivé objekty. Bohužel tato dokumentace a náležitě informace jsou interní záležitostí a není možné se k těmto dokumentům dostat.

9.3 Úpravny a zdroje pitné vody

Úpravny vody jsou technická zařízení, která jsou určena pro mechanickou a chemickou úpravu surové vody, které je čerpána z vodního zdroje, kdy se jedná o povrchovou vodu nebo podzemní. Samotný proces úpravy vody je závislý na dané technologii, ale v zásadě jde o úpravu vody po stránce chemické a biologické. Platí zde pravidlo, čím je surová voda ze zdroje kvalitnější, tím snadnější je její úprava na vodu pitnou.

Zdroje pitné vody jsou veškeré zásoby vody (rybníky, nádrže, přehrady, studny, vrty a prameny), které jsou vhodné pro úpravu na vodu pitnou.

9.3.1 Úpravna vody Moravská Nová ves

Úpravna čerpá vodu z pramenů v oblasti Podluží, kde se nachází celkem 4 čerpací stanice, které čerpají vodu z podzemních vrtů v dané lokaci.

Technologie pro úpravu vody se zde označuje jako dvoustupňová s předchozím krokem aerací s cílem odkyselit a odstranit nežádoucí plyny. Následuje alkalizační čiření s aplikací vápenného hydrátu. Následuje první separační stupeň, kdy dochází k sedimentaci suspenze vloček v nádržích pro sedimentaci. Druhý stupeň separace zahrnuje filtraci na otevřených filtrech moderního filtračního systému Leopold. Filtrace upravené vody je založena na dvou stupních, které na sebe sériově navazují. U prvního stupně filtrace na rychlofiltrech je náplň s názvem Filtralite, druhý stupeň filtrů je na bázi aktivního uhlí. Dochází k odstranění mikročásticového znečištění ze surové vody. Na filtry se ještě aplikuje roztok manganistanu draselného s cílem odmanganovat vodu na filtrech. V konečné fázi se voda zabezpečuje skrze její hygienu pomocí oxidu chloričitého (VaK Hodonín, 2022).



Obrázek 6: Úpravná vody Moravská Nová Ves – vstupní brána

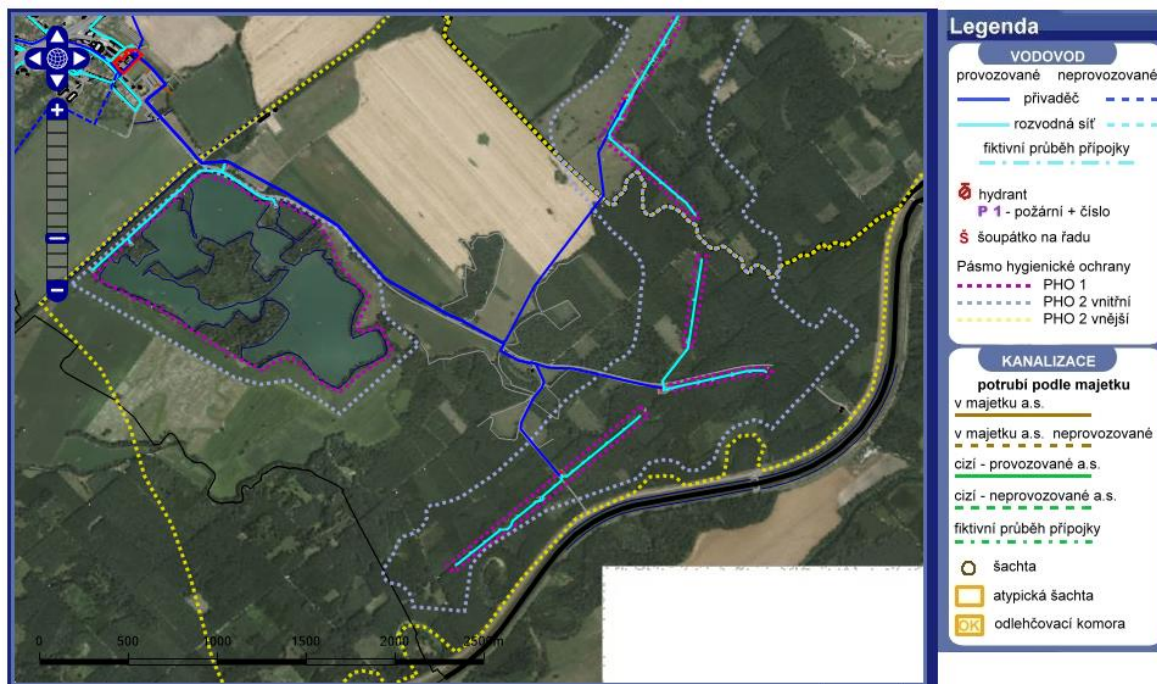
Zdroj: Vlastní

Z těchto zdrojů vody, bez možnosti náhrady z jiného zdroje, jsou zásobena tyto města a obce (VaK Hodonín, 2022):

- Čejč, Terezín, Krumvíř, Čejkovice, Dolní Bojanovice, Lužice, Moravská Nová Ves, Prušánky, Starý Poddvorov, Josefov, Nový Poddvorov a Hrušky.

V roce 2021 byla do úpravně investována částka 16 285 000 Kč na rekonstrukci filtrační části úpravy vody (VZ VAK Hodonín, 2021).

Pro lepší představu můžeme použít obrázek číslo 6 z portálu iGIS pro VaK Hodonín a.s.



Obrázek 7: ÚV Moravská Nová Ves a pásma hygienické ochrany

Zdroj: iGIS, 2022

9.3.2 Úpravna vody Bzenec Přívoz

Společně s rozvojem okresu Hodonín byla věnována pozornost i do sektoru pro zajištění dostatku pitné vody obyvatelstvu a průmyslu. Tento rozvoj dal vzniknout vodohospodářskému dílu skupinový vodovod Bzenec – Kyjov – Hodonín, kdy bylo cílem dostat pitnou vodu do částí, kde jí byl nedostatek, jednalo se o část Kyjovska a Hodonínské oblasti. Dalším bodem bylo nahradit slabé zdroje pitné vody z oblastí Bzenec a Veselí nad Moravou. Začátek výstavby počal v sedmdesátých letech minulého století, kdy došlo k realizaci vrtů, stavbě sběrných studní, výstavbě potrubí a samotné čerpací stanice. Byly zde umístěny i rozvaděče pro pitnou vodu o rozměrech 400 mm, 500 mm a 600 mm. Cílem bylo dostat vodu do vodojemu Vracov II, který nabízel akumulární komory vody s kapacitou 6 000 m³. Tento vodojem následně směřoval silnější přivaděče o průměru 600 mm na Kyjov a slabší přivaděč 500 mm na Hodonín. Výstavba samotné úpravní vody byla zahájena v roce 1986, kdy přes několik komplikací byla až roce 1993 podrobena zkouškám a otestována, posledním krokem bylo její oficiální spuštění do provozu (VaK Hodonín, 2022).

Čerpací stanice prošly rozsáhlou opravou a technickým zlepšením v průběhu roku 2005 a 2006. Opravy se týkaly výměny čerpadel za silnější modely. V roce 2008 a 2009 se týkala

údržba aktivně využívaných vrtů, kde došlo k výměně násoskové řady na pramenech. Současně bylo v rámci lepší ochrany prameniště u Moravského Písku oploceno. Modernizace úpravny vody probíhaly v roce 2008 a 2010, kdy se jednalo o výměnu strojních zařízení pro úpravu pitné vody. Byla navýšena kapacita pro vodojem Vracov II, kde stoupla kapacita nádrží na 12 000 m³. Opravy a modernizace nezasáhly do dodávek pitné vody (VaK Hodonín, 2022).

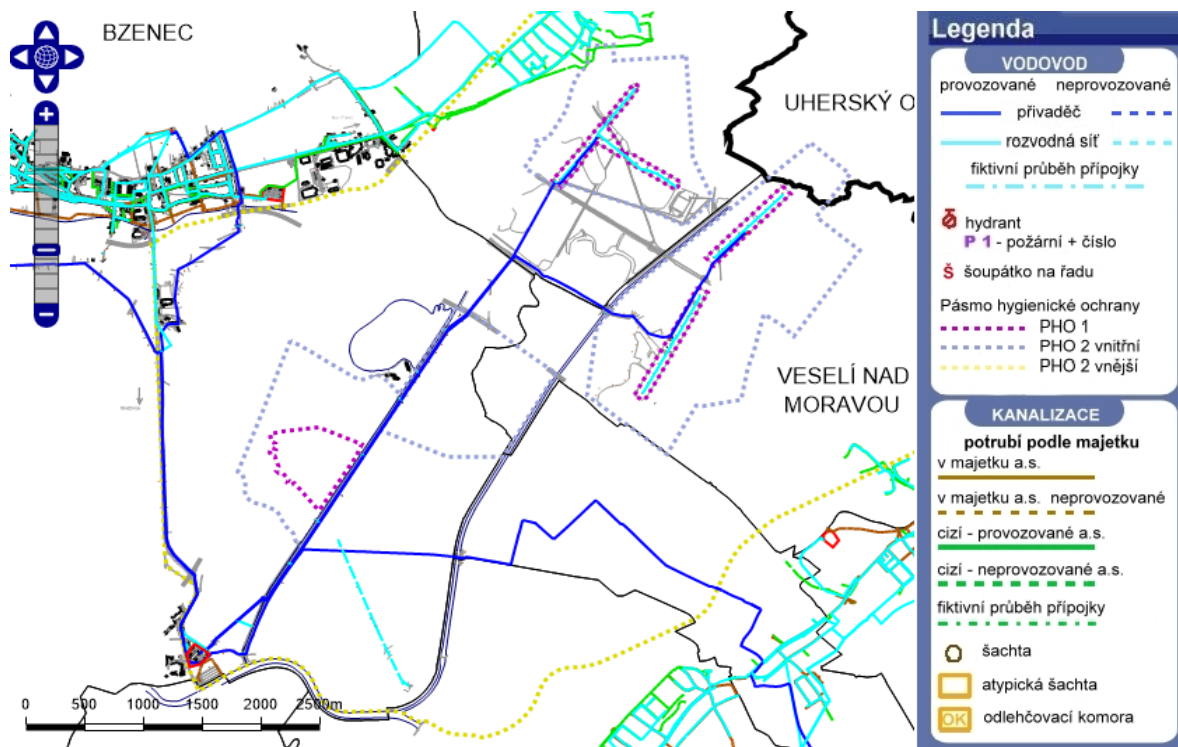
Výkon úpravny vody je okolo 400 litrů za sekundu. Oblast označená jako Bzenec-komplex je nejproduktivnější jímací soustava pro Jižní Moravu. Zdroje jsou zde jedny z nejkvalitnějších a chystají se nové hlubší vrty, tedy potenciálně ještě kvalitnější pitná voda. Zajímavostí je, že v roce 2012 bylo z této úpravny čerpáno přes 10 000 m³ na tehdejší lesní požár (VaK Hodonín, 2022).

Úpravna vody také disponuje zázemím a personálem pro vzorkování a analyzování pitné vody, vody povrchové a podzemní. Laboratoř splňuje akreditaci podle národního akreditačního orgánu, Český institut pro akreditaci, s číslem osvědčení 1330. Je zde zavedený systém v oblasti jakosti ČSN EN ISO 17 025/IEC pro provádění vzorkování a zkoušení pitné, podzemní a povrchové vody ve stanoveném rozsahu. Hlavní náplní práce laboratoře je plnění požadavků na kontrolu kvality vody ze zdrojů a v sítích (VaK Hodonín, 2022).

Prameniště Bzenec I – je tvořeno na tři linie jímacích vrtů o pěti, šesti a osmi jímacích vrtech. Jednotlivé vrty v liniích jsou připojeny na násoskový řad z litiny, který vodu přivádí do sběrné studny, která je umístěna v bezprostřední blízkosti čerpací stanice na surovou vodu. Čerpací stanice čerpá surovou vodu výtlačným řadem surové vody do úpravny vody Bzenec – Přívoz. Výtlačný řad je vyroben z litiny DN 400 a dlouhý 5 700 m (IS IEA, 2005).

Prameniště Bzenec III sever – je tvořeno soustavou dvou linií jímacích vrtů o šesti a pěti jímacích vrtech. Vrty ze dvou linií vrtů se napojují každý na jeden litinový násoskový řad, který vodu přivádí do sběrné studny. Studna je umístěna centrálně vůči dvěma liniím vrtů. V bezprostřední blízkosti sběrné studny se nachází čerpací stanice vybavená jak evakuačními stanicemi pro evakuaci násosek, tak čerpací technikou pro čerpání surové vody do úpravny vody Bzenec – Přívoz. Voda je poté čerpána do výtlačného řadu, který je společný pro vodu z prameniště Bzenec III – jih. Řad je litinový DN 500, dlouhý 6 080 m. Prameniště je v rámci jeho zabezpečení oploceno v rozsahu ochranného hygienického pásma I. Stupně (IS IEA, 2005).

Prameniště Bzenec III jih –opět je tvořeno na dvě linie jímacích hydrogeologických vrtů o pěti a čtyřech vrtech. Vrty v každé linie jsou napojeny na samostatný litinový násoskový řad, který přivádí vodu do sběrné studny. Sběrná studna se nachází centricky vůči oběma liniím násoskových řadů. V bezprostřední blízkosti sběrné studny je umístěna čerpací stanice pro surovou vodu. V čerpací stanici se nachází evakuační stanice pro evakuaci násosek a čerpací technika pro čerpání surové vody do ÚV Bzenec – Přívoz. Voda se čerpá výtlačným řádem z litiny DN 300 s délkou 1 084 m, který je napojen na prameniště Bzenec III – jih, označeným jako společný výtlačný řad z litiny DN 500 o délce 6 080 m. Prameniště je opět oploceno v rozsahu ochranného hygienického pásma I. Stupně (IS IEA, 2005).



Obrázek 8: Úpravna vody Bzenec-komplex a pásma hygienické ochrany zdrojů vody

Zdroj: iGIS, 2022



Obrázek 9: Úpravna vody Bzenec

Zdroj: Vlastní

Technologie pro úpravu vody je zde založena na dvoustupňové bázi, navíc je zde předřazená aerace směřovaná k odkyselování a odvětrání nechtěných plynů. Následuje alkalizační čiření s využitím vápenného hydrátu. Následuje flokulace pomalým mícháním v určených nádržích a následně se přechází na první separační stupeň, dochází k sedimentaci. Druhý separační stupeň zahrnuje filtraci na otevřeném pískovém rychlofiltru. Na filtry se aplikuje roztok manganistanu draselného, skrze odmanganování. Konečnou úpravou je aplikace oxidu chloričitého nebo plynným chlórem (VaK Hodonín, 2022).

Z těchto zdrojů vody, bez možnosti náhrady z jiného zdroje, jsou zásobena tyto města a obce (VaK Hodonín, 2022):

- Ježov, Skoronice, Svatobořice-Mistřín, Šardice, Vlkoš, Žádovice, Žeravice, Kelčany, Vřesovice, Čeložnice, Hýsly, Kostelec, Labuty, Skalka, Bzenec, Moravský Písek, Petrov, Strážnice, Sudoměřice, Tvarožná Lhota, Veselí nad Moravou, Vnorovy, Vracov, Kozojídky, Hrubá Vrbka, Kuželov, Malá Vrbka, Radějov, Dubňany, Milotice, Mutěnice, Ratíškovice a Vacenovice.

9.3.3 Úpravna vody Koryčany

Úpravna vody v obci Koryčany byla budována společně se vznikem vodní nádrže. Uvedena do provozu byla v průběhu roku 1959 se zvyšujícím se požadavkem obyvatel a průmyslu na zásobování pitnou vodou. Úpravna vody se nachází v severovýchodní části Koryčan na hranici s obcí Lískovec, od vodního díla je vzdálená 1,2 km. Voda k úpravě se do úpravný dostává díky převýšení vodního díla. Využívá se potrubí o průměru 400 mm a voda se tlačí díky gravitaci, nejsou zde tedy pomocná čerpadla v úseku vodního díla a úpravný vody. Výkon průtoku se pohybuje okolo 35 litrů za sekundu, díky těmto hodnotám spadá do kategorie menších úpraven. Mimo Koryčany je odsud vedena voda směr Kyjov a Ždánice. Úpravna byla kompletně modernizována dle nových požadavků koncem 20. století, tedy po 40 letech provozu. (Vodárenství, 2022).

V rámci modernizace došlo k modernizaci v oblasti elektrického zařízení, jednalo se hlavně o elektro rozvaděče a elektro kabeláž pro vedení silnoproudu a měření s možností regulace. Došlo také k úpravám v rámci zlepšení vnějšího a vnitřního vzhledu objektu jako jsou úpravy provozně administrativní, technologické, podlahy, okna, nová střecha apod. (Kozlík, Vaněk, 2016).

Zmíněná modernizace objektu se týkala také řídicího systému a napojení na systém centrálního vodárenského dispečinku, to umožňuje řídit úpravnu z části v režimu bez obsluhy. Tedy pracovní směna je pouze přes den a noční provoz je již bez zaměstnanců. Pro případ výpadku elektrické energie je zde umístěn dieselové elektrocentrála s nádrží na 5000 litrů nafty. Pouze v případě narušení objektu, závady nebo problém, je zde pracovník pohotovosti, který může pomáhat při provádění zásahu v kooperaci s dispečerem společnosti VaK Hodonín a.s. (Kozlík, Vaněk, 2016).



Obrázek 10: Úpravna vody Koryčany

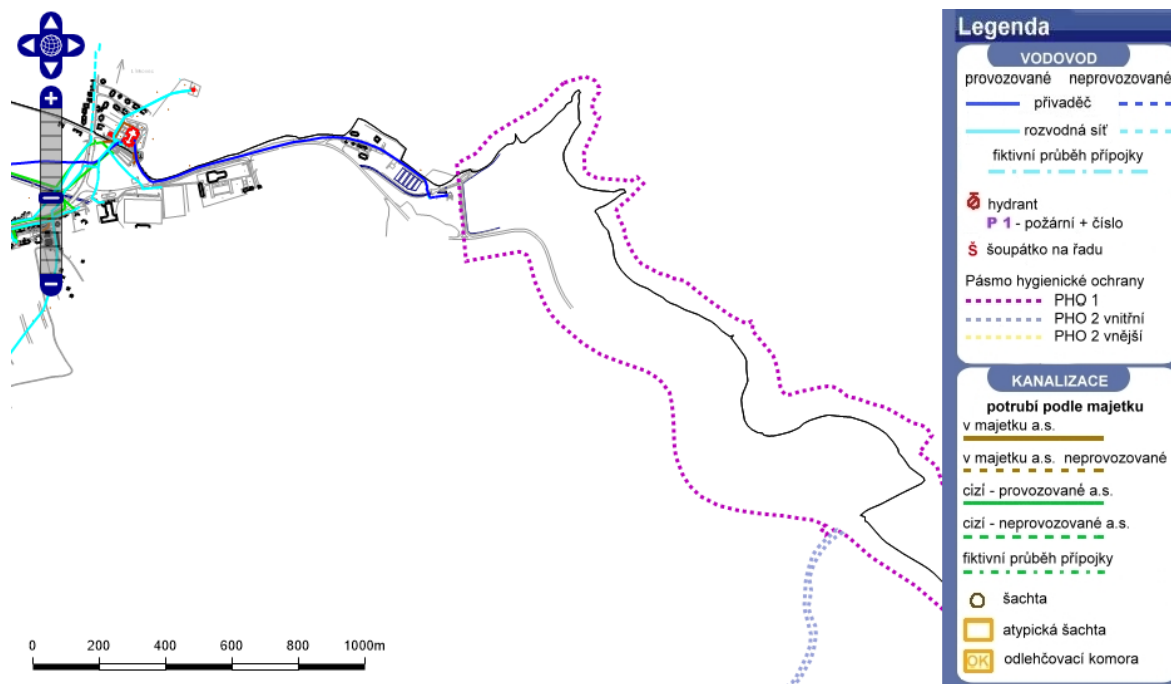
Zdroj: Vodárenství, 2022

Technologie pro úpravu vody v této úpravně je stanovena jako dvoustupňová pomocí chemické úpravy. První separační stupeň tvoří číření s vločkovým vznášeným mrakem. Druhý separační stupeň poté tvoří 6 otevřených rychlofiltrů na bázi filtračního písku. Před prvním stupněm se dává železitý koagulant v podobě síranu železitého a manganistanu draselného. Před druhým stupněm se poté dává alkalizační hydroxid sodný. Následná desinfekce již upravené vody se dokončuje chlórdioxidu (VaK Hodonín, 2022).

Města a obce zásobené pitnou vodou z úpravny vody Koryčany, které není možné zásobovat z jiného zdroje a v případě výpadku je potřeba přejít k náhradnímu zásobování pitnou vodou krajně až nouzové zásobování pitnou vodou. Jde tedy o města a obce (VaK Hodonín, 2022):

- Archlebov, Ždánice, Koryčany, Mouchnice a Haluzice.

Ostatní města a obce je v případě výpadku úpravny vody Koryčany nebo vodního zdroje, začít zásobovat z úpravny vody Bzenec.

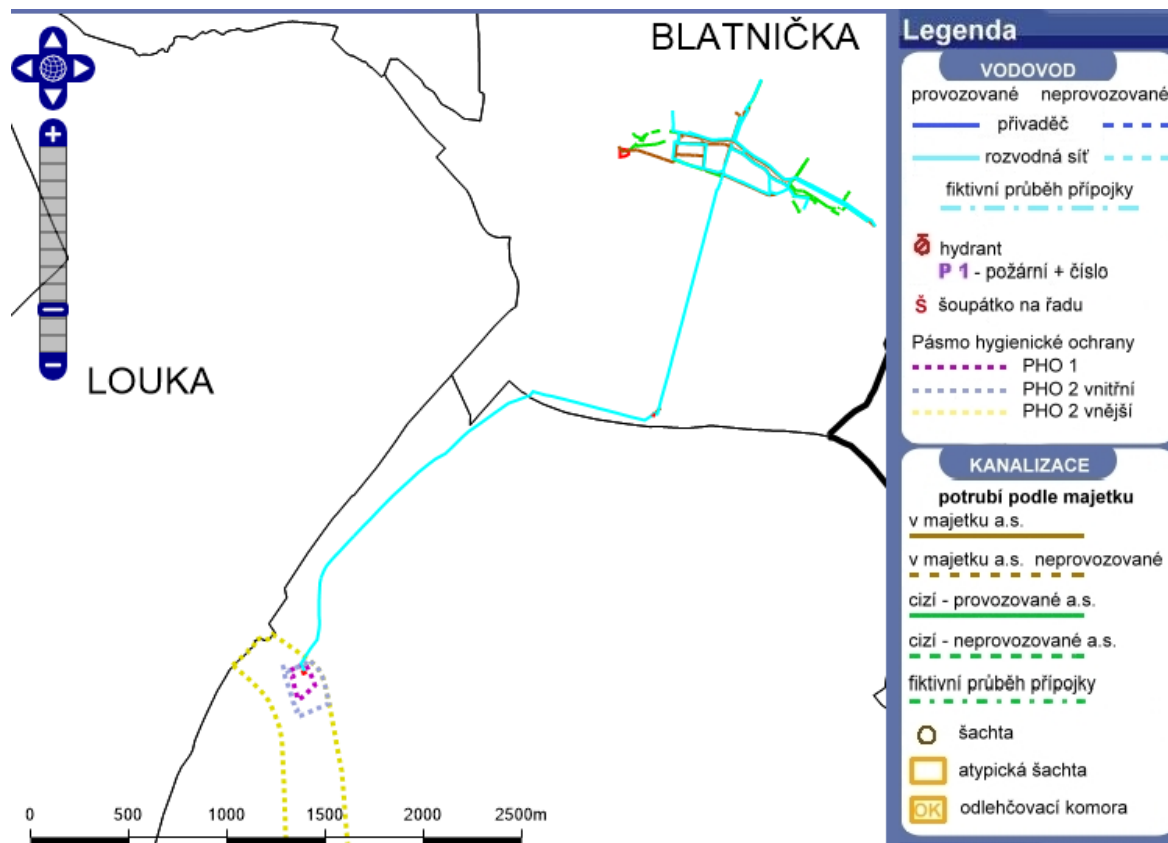


Obrázek 11: Úpravna vody Koryčany a hygienické pásmo vodního díla Koryčany

Zdroj: iGIS, 2022

9.3.4 Čerpací stanice Louka

Jde o vyhrazený zdroj, velmi kvalitní vody a není třeba jej upravovat a tlačit přes soustavy filtrů, jako je tomu u ostatních zdrojů pitné vody. Je pouze hygienicky zabezpečen chlordioxidem. Čerpací stanice se nachází na okraji východní části obce Louka, ale samotnou obec Louka nezásobuje, ta je zásobena z vlastní studny, která se nachází mezi samotnou Loukou a Lipovem. Čerpací stanice prošla modernizací po stránce techniky, tedy zde bylo umístěno nové silnější čerpadlo, které tlačí vodu do vodojemu Blatnička, který zajišťuje tlak a kryje výkyvy z odběru vodovodního řádu. V roce 2021 se uskutečnila investice ve výši 1 546 000 Kč, kdy došlo k částečné rekonstrukci vodovodu (VZ VaK, 2021).



Obrázek 12: Čerpací stanice Louka a pásmo hygienické ochrany

Zdroj: iGIS, 2022

9.3.5 Data o pitné vodě za rok 2021

V roce 2021 akciová společnost VaK Hodonín, dodala svým zákazníkům 6255 tis. m³ pitné vody, z toho 4 396 tis. bylo dodáno domácnostem a 1 859 tis. m³ zbývajícím odběratelům. Společnost splnila své závazky vůči zákazníkům na 100,1 % a celková hodnota předané dosáhla 881 tis. m³. V roce 2021 činila průměrná spotřeba 86,4 l vody na osobu a den. Celkové ztráty pitné vody v trubní síti tvořil 5,2 % (VZ VaK Hodonín, 2021)

Podrobnější data a informace za rok 2021 a srovnání s předchozím rokem 2020 a 2019 je možné hodnotit podle tabulky č.2 (VZ VaK Hodonín, 2021).

Tabulka 2: Vybrané údaje o distribuci vody a vodovodech

Provoz vodovodů	Měrné jednotky	2019	2020	2021
Délka vodovodní sítě provozované celkem	km	1 130	1 133	1 134
Délka vodovodní sítě v majetku společnosti	km	788	789	787
Délka vodovodní sítě cizí provozované	km	342	344	347
Počet vodovodních přípojek	ks	40 055	40 271	40 571
Délka vodovodních přípojek	km	319	321	323
Počet úpraven vody celkem	ks	4	4	4
- z toho v provozu	ks	3	3	3
Voda vyrobená ve vlastních vodohospodářských zařízeních z:	tis. m ³	7 678	7 788	7 638
- vody povrchové	tis. m ³	518	721	784
- vody podzemní	tis. m ³	7 160	7 067	6 854
Voda předaná	tis. m ³	875	877	881
Počet obyvatel napojených na vodovod	osob	137 213	138 606	138 776

Zdroj: VZ VaK Hodonín, 2021

9.3.6 Data o odvádění a čištění odpadní vody za rok 2021

Plán pro rok 2021 na objem fakturace odpadních vod byl splněn na 100,7 %. Celkem bylo fakturováno na 5 863 tis. m³ stočného, obyvatelstvo tvořilo hodnotu v počtu 3 437 tis. m³ a ostatní odběratelé dosáhli hodnoty 2 426 m³ (VaK Hodonín, 2022).

Podrobnější data a informace za rok 2021 a srovnání s předchozím rokem 2020 a 2019 je možné hodnotit podle tabulky „Tabulka Vybrané údaje o kanalizacích“ ta se nachází v části přílohy. Důvodem pro umístění této tabulky do příloh je, že práce se nezaměřuje na ochranu odpadní vody, kanalizací a čističek odpadních vod (VZ VaK Hodonín, 2021).

9.3.7 Integrovaný systém managementu

Společnosti VaK Hodonín a.s. záleží na kvalitě nabízených produktů. Kvalitu nabízených produktů se společnost rozhodla zajišťovat a deklarovat získáním certifikátů integrovaných systémů řízení, které se těší mezinárodního uznání. Jedná se o certifikaci (VZ VaK Hodonín, 2021):

- Management kvality ISO 9001:2015,
- Systém enviromentálního managementu ISO 14001:2015
- Management hospodaření s energií ISO 50001:2018.

Ve dnech 21. – 26. června roku 2021 byl ve společnosti proveden během 5,5 dnů kontrolní audit. Během kontrolního auditu byla provedena obnovena certifikace s končícím datem platnosti a došlo rovněž k zavedení normy ISO 50001:2018 do integrovaného systému managementu společnosti. Výsledky, který byly dodány po auditu, ratifikovaly, že normy ISO 9001:2015, ISO 14001:2015 a ISO 50001:2018 implementované do integrovaného systému managementu jsou nadále platné a jsou dodržovány v požadovaném rozsahu. Výsledek auditu o správném dodržování výše zmíněných zavedených norem je zárukou pro všechny stakeholdery, že nabízené produkty dosahují té nejvyšší možné kvality. Podnik přešel na standard ISO 50001:2018 dle vyžadovaných postupů dané normy. Přejechod byl pozitivně hodnocen ze strany kontrolního auditu, zejména díky začlenění, do již užívaného systému managementu hospodaření s energiemi do zavedených systémů ISO 9001:2015 a ISO 14001:2015 (VZ VaK Hodonín, 2021).

Pandemie Covid-19 donutila podnik pokračovat již v dříve zavedených protipandemických opatřeních z roku 2019, s cílem zajistit nepřetržité zásobování obyvatelstva pitnou vodou, provádění čištění odpadních vod a ochrany zdraví zaměstnanců.

Kontrolní audit rovněž vyhodnotil procesy podniku v rámci enviromentálního hlediska s ohledem na nakládání s energiemi potřebné pro dané procesy. Výsledky dokládají, že procesy uskutečňované v rámci podniku jsou efektivní a dosahují profesionální úrovně. Kontrolní komise během návštěvy rovněž pozitivně ohodnotila investované zdroje do infrastruktury společnosti na základě dříve provedené identifikace rizik. Bylo zejména pozitivně vnímáno (VZ VaK Hodonín, 2021):

- Zvýšení kapacity výtlačného řádu z ÚV Bzenec do nedalekého vodojemu Vracov s cílem zajistit bezproblémové dodávky pitné vody pro místní obyvatelstvo.
- Zabezpečení zpracování veškeré produkce kalů z ČOV VAK Hodonín pro následné budoucí využití.
- Výrazné snížení nutné spotřeby bioplynu sloužícího k vytápění a navýšení spotřeby bioplynu pro potřebu v kogenerační jednotce díky instalaci řídicího systému na ČOV Hodonín.

9.4 POVODÍ MORAVY

Povodí Moravy, s.p. se řadí mezi státní podniky, zaměřující se na provoz, správu a údržbu v oblasti vodních toků a vodohospodářských objektů spadajících do povodí Moravy. Na území, které dosahuje rozlohy 21 133 km², obstarává a spravuje 10 835 km vodních toků, kdy je 3 760 významných, dále zde patří ochranné hráze o celkové délce 1 060 km, 29 významných vodních nádrží, 135 ostatních vodních nádrží, 171 jezů, 13 plavebních komor a 15 malých vodních elektráren (Povodí Moravy, 2022).

Správa povodí je následně rozdělena do tří závodů, kdy sídlí v Olomouci, Uherském Hradišti a Náměšti nad Oslavou. Působí v 67 ORP na území 7 krajů. Základní činnosti jsou stanoveny zakládací listinou a vyplývají ze zákonem stanovených norem, především ze zákona č. 254/2001 Sb. O vodách a o změně některých zákonů (vodní zákon), zákona č. 305/2000 Sb. "o povodích" a zákona č. 77/1997 Sb. "o státním podniku" v platném znění. V zákonech se stanovuje především provoz a údržba vodních děl, činnosti v oblasti plánování podle vodního zákona a poradenskou činnost. (Povodí Moravy, 2022).

9.4.1 Vodní nádrž Koryčany

Vodní nádrž Koryčany, nacházející se 308,25 m. n. m., je možno nalézt na toku potoka Kyjovka ve vzdálenosti jednoho kilometru východně od obce Koryčany. Nádrž má celkový objem 2,564 mil. m³ a rozloha zatopené plochy přesahuje 35 hektarů. Vodní nádrž Koryčany je primárně určena k shromažďování vody pro vodárenský odběr do skupiny vodovodů Kyjov, dále k udržování minimálního povoleného průtoku, snížení průtoku v případě rizika vzniku povodně a dodávky vody pro malou vodní elektrárnu (Povodí Moravy, 2022).

O výstavbě hráze bylo rozhodnuto na počátku 50. let, kvůli narůstající spotřebě vody v dané oblasti, zejména pak kvůli rozvoji průmyslu a nutnosti zásobování obyvatelstva pitnou vodou. Výstavba vodní nádrže v Koryčanech byla schválena v lednu 1952 a stavba byla povolena tehdejší Krajský národní výbor v Gottwaldově, tedy dnešním Zlíně. Řeka Kyjovka pramenící ve Chříbech měla zalesněné povodí, a představovala tedy vhodné podmínky pro vodárenskou nádrž. Stavba hráze započala odstraněním veškeré vegetaci z prostor připravované zátopy v roce 1953. Stavba nádrže byla dokončena již v roce 1958, ale po napuštění nádrže bylo zjištěno, že v některých místech u dna hráze a v hrázi samotné došlo ke zjištění, že přirozenými skalními puklinami v podloží hráze prosakuje voda. do pro provozu byla nádrž uvedena až o pět let později v roce 1963. Kvůli splaveninám přinášející kyjovský potok byla při přítoku do nádrže postavena malá záchytná nádrž. Bohužel nádrž v letních měsících vysychala a tvořil se v ní plankton. Díky čemuž docházelo k negativnímu poklesu kvality vody v nádrži. Záchytná nádrž proto byla v 80. letech přebudována k rybolovným účelům a samotná Kyjovka v současnosti vtéká do nádrže přímo (Povodí Moravy, 2022).

Technický popis hráze – na hráz nádrže byla, jako v povodí Moravy, použita konstrukce sypaná zeminou z několika různých materiálů. Vnitřek hráze je tvořen z jílového těsnícího jádra, pod kterým je uložen betonový blok s přístupovou štolou. Délka hráze je 180 metrů s šířkou 8,5 metrů. Po šířce hráze vede zpevněná asfaltová komunikace určená pro členy údržby, komunikace je ohraničena zídka, která má ochranou funkci proti pádu z hráze a rovněž slouží jako vlnolam. Přístup do odběrné věže není možný z hráze, jediná cesta do odběrné věže vede skrz 94 metrů dlouhou štolu pod hrázi.

Protipovodňová ochrana – v případě nebezpečného navýšení hladiny je hráz vybavena bočním přelivem se skluzem na pravém břehu. Tři metry široký skluz ústí pod do hrázi. Maximální kapacita přelivu se přibližně 26 metrů krychlových za sekundu. Výpust nádrže je umístěn ve spodní části nádrže je tvořena potrubím, potrubí je ovládáno uzávěrem kuželovitého tvaru a stavítkem kanalizace. Zachování minimálního vodního průtoku vody pod hrázi je užíváno asanační potrubí s poloměrem 100 milimetrů (Povodí Moravy, 2022).

Výroba elektrické energie – nádrž je ve spodní části vybavena potrubními výpustěmi o poloměru 400 milimetrů, které je ovládané regulačním šoupákem a kanalizačním stavítkem. Odhadovaná kapacita dole umístěných výpustí je přibližně 8 krychlových metrů za sekundu. Potrubí určené k převádění asanačního průtoku o poloměru 100 milimetrů, na

kterých byla v 90. letech instalována malá vodní elektrárnička typu Banki. Elektrická energie již není v současné době vyráběna (Povodí Moravy, 2022).

Pitná voda – pitná voda z nádrže je obyvatelům dodávána pomocí vodovodu Kyjov. Objekty sloužící k úpravě pitné vody jsou umístěny u pravého břehu přehrady. Z objektů nejvíce vyčnívá 28 metrů vysoká kruhová budova odběrné věže, kde se ukrývají možnost provádět vodárenské odběry. Potrubí s pitnou vodou prochází pod hrází a vede až do úpravní vody (Povodí Moravy, 2022).

Ochrana kvality vody – kvalita vody v nádrži a přítoku je kontrolována dvakrát do roka pomocí zónačního měření. Povodí Kyjovky má bohužel krátce před vstupem do nádrže zhoršenou kvalitu vody, což se negativně projevuje zejména na ukazatelích chemické spotřeby kyslíku dichromanem a fosforu. Z jakostní ročenky vodárenských nádrží vyplývá, že Koryčany se řadí mezi velmi slušně mezotrofní nádrže, to značí střední obsah života (Povodí Moravy, 2022).



Obrázek 13: Brána horní části hráze Koryčany

Zdroj: Vlastní

10 ANALÝZA A VYHODNOCENÍ STAVU OCHRANY VODOHOSPODÁŘSKÉ INFRASTRUKTURY

Přes všechny technické, materiální a personální možnosti zabezpečení a ochrany prvků nebo systémů vodohospodářské infrastruktury, není možné nikdy dosáhnout sto procentní jistoty, že se nemůže nic stát. V praxi ohledně bezpečnosti platí, že žádný systém není bezpečný, stejně tak jako je tomu se silou řetězu, který je pevný jako jeho nejslabší článek. Důležité je tedy ochranu nejen budovat, ale také prověřovat její schopnost odolávat daným hrozbám. Z těchto důvodů se tedy aplikují různé metody analýzy rizik, z důvodu jistého odhalení možných bezpečnostních hrozeb. Díky tomu je možné učinit patřičné kroky pro včasnou nápravu. Zároveň aby byla analýza efektivní, je potřeba k tomu mít názor jak experta, tak i řadového zaměstnance nebo odborníka na danou oblast problematiky.

10.1 SWOT analýza pro současný stav ochrany

Zhodnocení stavu v oblasti ochrany vodohospodářské infrastruktury pro možnost teroristického útoku na tuto technickou infrastrukturu státu ČR. Analýza SWOT je rozdělena na čtyři části, kde můžeme sledovat působení aplikovaných dat ve směru pozitivním či negativním. Díky informacím a datům je možné odhalit slabiny, následně se na tyto nedostatky zaměřit pro jejich posílení nebo úplnou eliminaci. Analýza obsahuje zpracovanou tabulku číslo 3, kde jsou jednotlivé informace a data z výzkumu rozděleny do kategorie:

- Silné stránky.
- Slabé stránky.
- Příležitosti.
- Hrozby.

Navazující tabulka číslo 3 je upravena pomocí hodnot, kdy stanovuje důležitost pro jednotlivé body a určuje jejich hodnocení. Díky tomu je možné vytvořit a znázornit současný stav a určit strategii pro tvorbu opatření v řešené oblasti.

Tabulka 3: SWOT analýza stavu ochrany vybrané vodohospodářské infrastruktury

Silné stránky	Slabé stránky
<ul style="list-style-type: none"> ➤ Vnitřní zabezpečení objektů ➤ Postupné modernizace prvků ochrany ➤ Norma ISO ➤ Školení zaměstnanců ➤ Bezpečnostní a kontrolní systémy 	<ul style="list-style-type: none"> ➤ Neprovádění cvičení ➤ Nedostatečné zabezpečení vnějšího prostředí objektů ➤ Ochrana vodních zdrojů ➤ Rozsáhlá distribuční síť ➤ Pouze denní směny
Příležitosti	Hrozby
<ul style="list-style-type: none"> ➤ Prověřovací cvičení ➤ Větší investice do oblasti ochrany ➤ Dotace státu nebo EU pro rozvoj infrastruktury ➤ Spolupráce se společnostmi v rámci ochrany a bezpečnosti ➤ Školení zaměstnanců 	<ul style="list-style-type: none"> ➤ Napadení čerpací stanice ➤ Kontaminace vody ➤ Sabotáž ze strany zaměstnanců ➤ Dostupnost informací (prvky vodohospodářské infrastruktury) ➤ Nedostatek záložních zdrojů

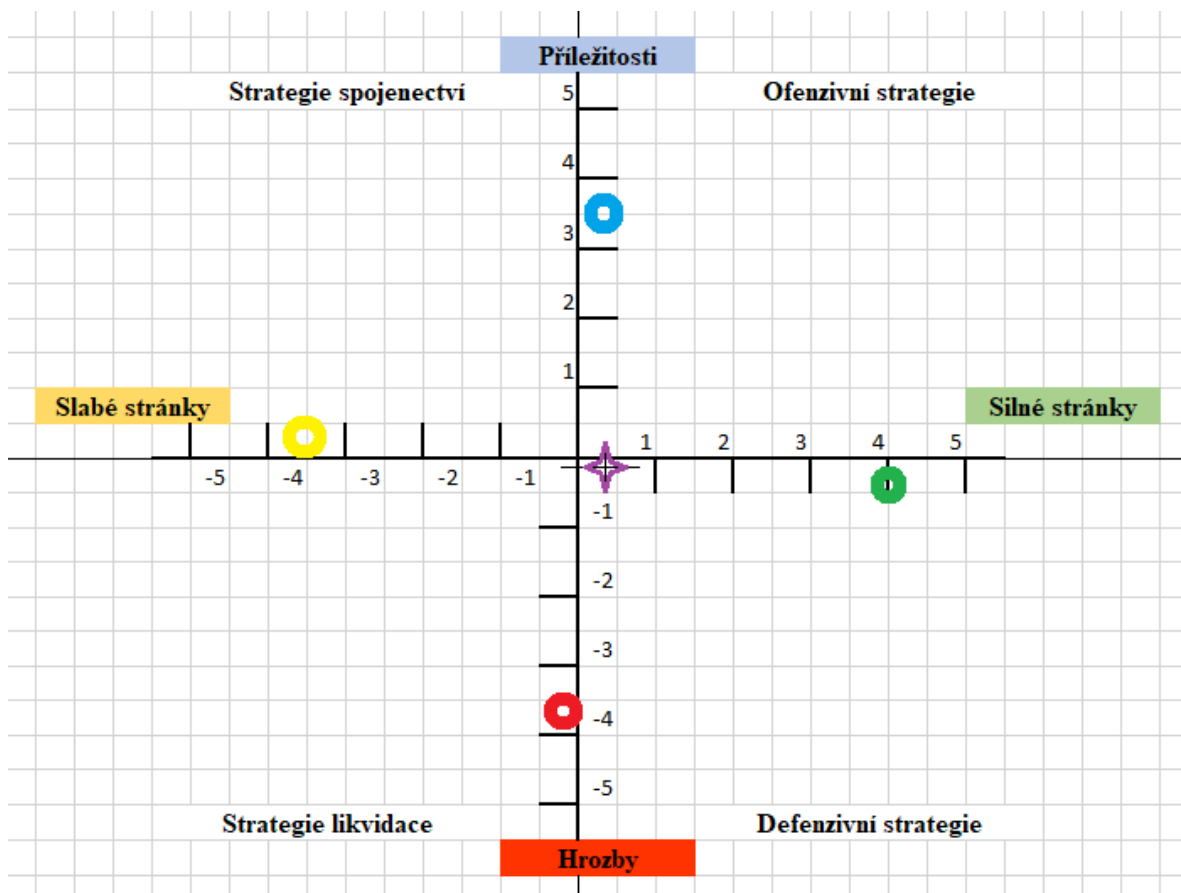
Zdroj: Vlastní

Obsah tabulek je založen na dostupných a zjištěných informacích. Jednotlivé body jsou zvoleny na základě týmové spolupráce. Nejedná se tedy o subjektivní názor autora práce. Spolupráce ze strany společnosti VaK Hodonín a.s. a Povodí Moravy s.p. je zde čistá nula, důvodem je zachování interních dokumentů zaměřených na ochranu a bezpečnost v tajnosti.

Tabulka 4: Ohodnocená tabulka SWOT analýzy

Silné stránky			Slabé stránky		
Důležitost	Hodnocení	Výsledek	Důležitost	Hodnocení	Výsledek
0,3	5	1,5	0,2	-3	-0,6
0,2	3	0,6	0,2	-3	-0,6
0,1	4	0,4	0,2	-4	-0,8
0,1	3	0,3	0,3	-5	-1,5
0,3	4	1,2	0,1	-1	-0,1
Součet		4	Součet		-3,6
Příležitosti			Hrozby		
Důležitost	Hodnocení	Výsledek	Důležitost	Hodnocení	Výsledek
0,3	4	1,2	0,3	-5	-1,5
0,2	3	0,6	0,3	-4	-1,2
0,1	3	0,3	0,1	-2	-0,2
0,3	4	1,2	0,2	-2	-0,4
0,1	2	0,2	0,1	-3	-0,3
Součet		3,5	Součet		-3,6

Zdroj: Vlastní



Graf 1: Grafické vyjádření strategie pro SWOT analýzu

Zdroj: Vlastní

Na základě tabulky 4 – ohodnocená tabulka SWOT analýzy, kde z vnitřních faktorů převažují po vyhodnocení silné stránky. Dominuje zde vnitřní zabezpečení objektů. V části vnějších faktorů je minimální rozdíl v prospěch hrozby. Tady je riziko v podobě napadení čerpacích stanic. Podle uvedených hrozeb je možné také navrhnout a uskutečnit opatření. Může to sloužit jako vodítko pro zvýšení ochrany a odolnosti v případě teroristické hrozby.

V grafu 1 následně po zpracování hledáme aktuální strategii. Ta je stanovena podle fialového bodu, který nám sděluje aktuální situaci. Výkyv je velmi malý a drží se hodně u středu, ale nachází se v oblasti pro defenzivní strategii, blíže hraničí k ofenzivní strategii. Defenzivní strategie je založena silných stránkách, za pomoci silných stránek se snažíme minimalizovat možné hrozby, kde je v čele vnitřní zabezpečení objektů, je velice obtížné se dostat dovnitř budov. V případě pokolení zabezpečení proti vniku do budovy jsou zde systémy, které ihned nahlásí neoprávněné vniknutí a pohyb osob. Další silnou stránkou je postupná modernizace prvků a systémů pro ochranu. Možností je také hledat smysl u ofenzivní strategie, kdy se využívají příležitosti skrze silné stránky.

10.2 Zjištěné nedostatky v oblasti ochrany

Popis aktuálního stavu ochrany vodohospodářské infrastruktury z vnějšího pohledu na objekty a jejich zabezpečení před vnikem do oblasti. Tyto poznatky jsou založeny na základě vlastního výzkumu z veřejně dostupných informací a osobním výzkumem v podobě fyzického průzkumu daných objektů. Jde o popis zjištěného stavu vybraných prvků a systémů.

Mechanické zábranné systémy obvodové ochrany – při zkoumání jednotlivých prvků vodohospodářské infrastruktury, byly odhaleny nedostatky v podobě poškozené obvodového plotu pro vyhrazení pozemku nebo pásma hygienické ochrany. Především u vodního zdroje, který se nachází v zalesněných částech. Poškození je zde způsobeno pádem větví, kdy těžší větve dokážou pádem plot poškodit. Další zjištění se týká stáří oplocení na několika místech, koroze je již v pokročilejší fázi a železný drát tím ztrácí svoji pevnost (lze jej poškodit bez potřebného vybavení). Ostatný drát je záležitost sama o sobě, někde je umístěn ve dvou řadách nad oplocením, ale například na samotné bráně se již nenachází, především v případě, kdy zde nejsou kamerové systémy je toto zjištění matoucí. Oplocení je v zásadě klasické drátěné, tedy pro nůžky na drát žádná výzva. Brány jsou nejčastěji zajištěny pomocí visacího zámku v mechanismu brány (tloušťka třmenu se

pohybovala okolo 10 milimetrů), zámek tedy již vyžaduje štípací kleště pákové nebo jiné ruční nářadí. Úroveň zabezpečení brány můžeme hodnotit na obrázku číslo 14.



Obrázek 14: Úroveň zabezpečení ochranného pásma I. stupně

Zdroj: Vlastní

Kamerové systémy – při sledování a vyhledávání kamer určených pro venkovní monitorování objektů byla pozorována přítomnost těchto systémů pouze u úpravěn vody a vodního díla. Kamery jsou často směřovány na kontrolu vstupních bran a dveří. Některé objekty mají více bran ovšem kamera byla zjištěna pouze u té hlavní. U prvků jako vodojemy, čerpací stanice a samotné vrty nebyla zjištěna přítomnost kamerového systému (až na pár případů, kdy se jedná o větší vodojem). U vodního díla Koryčany se kamerové systémy nacházejí pouze v oblasti pod hrází, kde slouží pro kontrolu budovy Povodí Moravy s.p., další kamery se nacházejí přímo na hřebenu hráze, kdy jsou umístěny na přítomném sloupovém osvětlení a jednu kameru je možné pozorovat na odběrné věži. Kamery zde jsou orientovány na přístupové cesty, hřeben hráze a část svahu tvořící hráz. Bohužel zde chybí další kamery pro dozor nad zbytkem vodního díla a hlídána je pouze oblast s hrází. To může umožnit útočníkům kontaminaci vodního zdroje v nehlídané oblasti, kontaminace by měla být včas detekována v přilehlé úpravně vody.

Fyzická kontrola – část výzkumu pojatá spíše na pozorování a sledování reakce ze strany osob spravujících dané objekty. Nikde nebyl ani náznak nějaké preventivní kontroly cizích osob pohybujících se v okolí objektu, které si pořizují digitální záznamy daného areálu, kamer, oplocení apod. Je zde sice kamerový záznam a určitou dobou ukládání, ale to platí pouze pro objekty, kde jsou kamerové systémy.

Prověřovací cvičení – společnosti nekonají cvičení v rámci zjištění aktuálního stavu ochrany dané infrastruktury. Není tedy zjištěn stav úrovně bezpečnosti a spolehlivosti pro bezpečnostní systémy v objektech, a neznámá doba reakce na případnou hrozbu. Cvičení v podobě napadení objektu nebo jeho systémů se také neprověřuje. V případě zásahu PČR není možné provést co nejefektivnější zásah, především z důvodu neprovádění taktického cvičení a neznalosti parametru objektů.

Dostupnost informací – zásadní problém z mého pohledu v oblasti ochrany vodohospodářské situace hraje dostupnost informací na internetu. Jedná se o veřejně dostupné informace, které mohou usnadnit plánování a volbu cílů v případě teroristického útoku na danou část infrastruktury. Jedná se především o iGIS.WEB, který je volně přístupný. Na mapě je možné sledovat vodovodní síť, kanalizační síť, úpravny vody, vodojemy, umístění hydrantů, pásma hygienické ochrany, čerpací stanice, vrty apod. Informace jsou tedy snadno zneužitelné, pro stanovení důležitosti prvků pro infrastrukturu v oblasti dodávek pitné vody. Dále se jedná o informace, které se týkají procesů jako je například technologie úpravy pitné vody atd.

Záložní zdroje – touto částí je myšlena připravenost pro extrémní případy jako je napadení a odstavení čerpadel v čerpacích stanicích, útok na úpravnu a vyřazení zařízení pro úpravu pitné vody, vyřazení přívodné sítě elektrické energie k jednotlivým prvkům. Úpravny vody a čističky odpadních vod disponují v případě odstávky elektrické energie vlastním náhradním zdrojem v podobě dieselové elektrocentrály, které výkonem stačí na pokrytí všech zařízení a systémů. Problém nastává v případě výpadku elektrické energie pro čerpadla nacházející se v čerpacích stanicích. Záložní elektrocentrály se musí v případě výpadku elektrické energie dovážet, není jich ani dostatek na pokrytí všech čerpacích stanic. Podobná situace platí pro čerpadla, kdy náhradních dílů je skromný počet pro občasné závady nebo opotřebení. V případě napadení čerpadel a jejich zničením (například pomocí výbušniny) je nahrazení nemožné. Rovněž kontaminace zdroje vody by měla fatální následky.

11 PLÁN PRO ZLEPŠENÍ SOUČASNÉHO STAVU OCHRANY VODOHOSPODÁŘSKÉ INFRASTRUKTURY PŘED MOŽNOU TERORISTICKOU HROZBOU

Aplikační část navrhuje možné zavedení nového opatření nebo zlepšení jeho současného stavu, který působí jako nedostatečný. Vycházíme z praktické části práce, kde se objevují zjištěné nedostatky. Návrh jsou tvořeny na základě týmového rozhovoru a informací od pracovníku z uvedených firem. Finanční náročnost jednotlivých návrhů vychází pouze jako možný odhad.

Plán je postaven na jednotlivých bodech, podle kterých je možné se řídit a postavit se tak k aktuální situaci.

Prověřovací cvičení

- Doporučuji uskutečnit cvičení v rámci zjištění skutečného stavu ochrany vodohospodářské infrastruktury. Cvičení by mělo být tvořeno několika body, kdy se budou prověřovat všechny části ochranných systémů a jednotlivých prvků. Cvičení by mělo mít charakter teroristického útoku, kdy se může jednat o fyzické útok na objekt a prvky (obsazení úpravny vody, poškození technického zařízení apod.) nebo se může jednat o kybernetický útok s cílem ochromit tuto infrastrukturu (blokování systémů, úpravy hodnot apod.) Prověřit postupy dle interní dokumentace společnosti pro řešení vzniklé krize a jejich nápravných opatření. V rámci bezpečnosti také prověřit zaměstnance, jestli vědomě či nevědomě neposkytují tajné informace.

Celé cvičení patřičně zdokumentovat pro interní účely, na základě zjištěných hodnot vytvořit vyhodnocení a zaměřit se na eliminaci případných nedostatků.

Do cvičení zapojit složky IZS a patřičné orgány, pro lepší připravenost jednotlivých složek a orgánů na různé scénáře v případě teroristického útoku. Důležitá je akceschopnost ze strany IZS a podniku minimalizovat dopady.

V rámci návrhu četnosti těchto cvičení, záleží hodně na rozsahu daného cvičení. Cvičení vyhrazené pro fyzické napadení v podobě teroristického útoku, by bylo vhodné uskutečnit alespoň 1x v průběhu 4 let. Cvičení na prověření kybernetické bezpečnosti se doporučuje provádět minimálně 1x za rok. Důvodem je neustálý pokrok informačních a komunikačních technologií.

Cvičení by nemělo narušit dodávky pitné vody a odvod odpadní vody. Finanční rozsah je zde podle rozsahu cvičení, jestli se bude jednat pouze o cvičení na prověření ochrany, postupu složek a řízení provozu při fyzickém napadení objektu, budou náklady minimální (v rámci desítek tisíc Kč). Náročnější bude prověření kybernetické bezpečnosti, kdy kompletní prověření všech systémů, může dosahovat v řádech milionů Kč.

Zabezpečení a ochrana objektů

- Cílem je udržovat nebo zvyšovat úroveň zabezpečení a ochrany pro důležité objekty. Důležitá je připravenost a přítomnost vhodných opatření. Podstatnou roli tady hrají zákony státu, doporučení a normy EU, ochrana objektů je také stanovení instrukcí v usnesení Bezpečnostní rady státu.

Provádět kontrolu zpracované vnitřní dokumentace k zabezpečení ochrany objektů. Prověření havarijních a krizových plánů. Školení zaměstnanců v oblasti ochrany objektů a prověřování osob, prohledávání vozidel pouštěných do areálu, najmutí ostrahy, prověřování elektrického zabezpečovacího systému, prověřování dodavatelských firem. Zavedení kontroly vnitřních prostorů budov, vymezení důležitých prostorů se zvýšenou ochranou a dozorem.

Dále je nutné zdůraznit doporučení na umístění mříží na vnější stranu okenních otvorů, která se nacházejí výškově do 2 metrů nad úroveň terénu. Toto opatření bylo možné pozorovat u jedné z úpraven vody. Psychologický efekt odrazení útočníka je poměrně vysoký a úroveň ochrany se tak značně zvyšuje.

Finanční náklady zde budou v řádu milionů Kč a opatření zaberou značné časové období.

Ochrana vodních zdrojů

- Ochrana této části je dosti specifická, aktuálně spadá do kategorie ochrany kvality a kvantity pro podzemní a povrchové zdroje vod. Oblast řeší uzemní ochrana vod a legislativa ČR, která je dobře zpracovaná, ale stále nabízí prostor pro zpřísnění vybraných požadavků v rámci ochrany zdrojů. Pro zdroje pitné vody se jedná o stanovení ochranných pásem I. stupně a II. stupně.

Vhodné by bylo přepracování vodního zákona v oblasti pásma vodních zdrojů, kdy by bylo vhodné stanovit větší rozsah těchto pásem a nařídit jejich zabezpečení.

Zákon stanovuje zákaz vstupu a vjezdu do pásma I. stupně, kdy je vstup povolen pouze osoby oprávněné k odběru vody, které patří k vlastníkům vodního díla.

Návrh je udělovat povolení pro vstup do pásma I. stupně pouze osobám, které budou patřičně prověřeny. Jako příklad uvádím, že pro určitou lokalitu by mělo mít přístup pouze několik vybraných lidí.

Dalším krokem pro zlepšení ochrany je lepší ohraničení oblasti ochranného pásma. Umístění výstražných cedulí s upozorněním na neoprávněný vstup do zakázané oblasti.

Zlepšit komunikaci mezi společnostmi provozující vodovody a kanalizace s Ministerstvem životního prostředí, které stanovuje zásady pro změny ochranných pásem vodních zdrojů.

Do oblastí pořídit kamerové systémy napojené na dispečink společnosti se stálým dohledem pracovníka.

Zlepšit oplocení pásem a vodních děl v podobě vyššího plotu, který je v horní části opatřen ostnatým drátem ve dvou řadách, po celé délce objektu. Zároveň je možné v ostnatém drátu mít přidaný elektrický kabel napojený na signalizaci pro přestřížení drátu.

Vhodná je i kombinace nového oplocení s kamerovým systémem v rámci zvýšení efektu ochrany a zabezpečení.

Finanční náklady jsou znatelné, řádově se budou pohybovat v milionech Kč.

Dozor distribuční sítě

- Rozsáhlejší distribuční sítě pitné vody a kanalizační soustavy představují i zvýšenou potřebu kontroly. Síť je vybavena různými čidly a senzory pro stálý dozor. Hlídí se hodnoty jako průtok a tlak skrze možné úniky na potrubí nebo se kontrolují chemické hodnoty.

Část sítí je však stále bez těchto čidel a senzorů nebo jsou již opotřebená a vykazují nereálné hodnoty. Návrh je tedy pořídit nová čidla a senzory od stejného výrobce a se stejnými parametry – důvodem je jednotnost a identičnost prvků v celé síti, pro vyloučení možných závad v důsledku nekompatibility.

S dozorem nad distribuční sítí se také pojí fyzická kontrola, kdy doporučuji vizuální kontroly oblastí, kudy sítě vedou. Zabrání se tak možnému porušení zákona, který stanovuje odstup od vodovodní sítě, vůči nepovoleným zásahům (různé výkopy, terénní úpravy, vysazování vegetace apod.). Častější kontroly tak mohou předejít spoustě problémů.

Finanční náklady jsou znatelné, řádově se budou pohybovat v desítkách milionech Kč.

Častější fyzické kontroly

- Zjištění problém v oblasti nedostatečné a málo časté kontroly v oblasti areálu. Doporučení je klást důraz na zaměstnance, aby častěji prováděli kontroly v prvků, systémů a objektů. Sledovali podezřele se chovající osoby jak v okolí, tak na pracovišti. Kontroly provádět vždy řádně. Tady bych doporučil vytvořit jednoduchý checklist, který bude obsahovat oblasti daného objektu. Pro tuto část bych doporučit vybrat dva zaměstnance, jeden hlavní a druhý jako záložní. Budou se řídit podle seznamu bodů, tedy checklistu, a prověřovat jednotlivé oblasti od funkčnosti zámků až po správné nastavení úhlu kamer. Vhodné by bylo takového pracovníka poslat na vzdělávací kurzy v oblasti ochrany a zabezpečení objektů

Je to čistě preventivní opatření pro kontrolu. Finanční náročnost se projeví pouze na možném motivačním příplatku pro zvoleného zaměstnance a případného placeného přesčasu. Nákladnější může být kurz pro rozšíření znalostí vybraného pracovníka, řádově se bude jednat o desítky tisíc Kč.

Zabezpečení techniky

- Problém spočívá v nedostatku záložních zdrojů, tedy čerpadel, elektrocentrál a zařízení pro úpravu pitné vody. V případě rozsáhlejšího výpadku elektrického proudu dochází k zastavení čerpadel umístěných v čerpacích stanicích. Elektrocentrál je pouze omezené množství, které pokryje pouze zlomek z počtu všech čerpadel. Při teroristickém útoku, s cílem vyřadit čerpadla u jednotlivých stanic dochází k problému, že nejsou náhradní čerpadla. To samé platí pro útok na úpravnu vody, ta je pro případ výpadku elektrické energie opatřena záložním zdrojem, ale zařízení na úpravu vody je z důvodu vysoké pořizovací ceny opravdu jen to provozované v síti.

Řešení pro čerpací stanice je dokoupit odpovídající počet elektrocentrál, aby bylo možné pokrýt alespoň jednu třetinu produkce čerpané vody. Zároveň by zde byla možnost v krajním případě půjčka elektrocentrál od SSHR, ale to je pouze dočasné řešení.

Pro zvýšení ochrany čerpacích stanic před fyzickým útokem, bych doporučil vyměnit současné oplocení za odolnější typ pletiva s dvojitou řadou ostnatého drátu. Do objektu umístit venkovní kamerový systém napojený na centrální kamerový systém pro stálý dohled, včetně pohybových čidel pro signalizaci případného pohybu osob v oblasti. Rychlá reakce zde může být klíčová.

Náročnost zde bude jak časová, tak i finanční. Cena jedné, podmínky splňující, elektrocentrály se pohybuje od 50 000 Kč a výše.

Prověřování a školení zaměstnanců

- V rámci posilování jednotlivých prvků v ochraně a bezpečnosti se nesmí opomenout lidský faktor, který hraje nejdůležitější roli. Jeden zaměstnanec dokáže napáchat fatální škody, když k tomu bude mít důvod a možnost nebo nebude mít dostatečné znalosti a praxi.

Prověřovat zájemce o volné pracovní pozice. Každého vážného zájemce o pracovní pozici důkladně prověřit, především se zaměřit na jeho pracovní minulost a volnočasové aktivity a zájmy. U pracovního pohovoru by měl být přítomen specialista na lidské chování a vypracovat na danou osobu posudek.

Prověřovat stálé a dlouhodobé zaměstnance společnosti. Opět využít formu rozhovoru a zjišťovat aktuální zájmové činnosti daného pracovní ve volném čase. Zjišťovat i názory od ostatních kolegů. Kontrolovat pracovní náplň, kvalitu provedené práce, monitorovat pracovní hovory, emaily a schůzky.

Provádět školení zaměřené na rozšíření znalostí o potencionálním nebezpečí teroristické hrozby. Jak se preventivně chovat v případě podezření, že cizí osoba má možné zlé úmysly. Příkladem může být sdělování interních informací přes telefon nebo email, útočník je velice schopný v sociálním inženýrství a osoby, které nejsou informovány jsou nejnepříznivější kořistí. Další model je osobní komunikace, kdy zaměstnanec otevře neznámé osobě bránu či dveře, bez informací o dané osobě (cizí se představí pod falešným jménem a údaji). Rozšiřovat tedy informace o těchto lidech, kteří získávají důležité informace.

Finanční náklady za školicí kurzy se budou pohybovat v řádu desítek až stovek tisíc Kč. Vše se bude odvíjet od daného kurzu, jeho náročnosti a specifičnosti.

Omezení veřejně dostupných informací

- Informace a data poskytované a volně dostupné na internetové síti mohou být snadno zneužity. Především konkrétní informace dávají útočníkům podklady pro snadnější a efektivnější provedení útoku.

Doporučení je tedy přehodnotit aktuální informace a data, které jsou volně dostupné na internetu. Rizikové části nejlépe zcela odstranit nebo omezit přístup uživatelů.

Před nahráním dat a informací na internet je nejprve přehodnotit, jestli nemůžou prozradit důležité vnitřní údaje a poté je teprve v případě schválení nahrát na server. Veškeré dokumenty by měla kontrolovat kompetitivní osoba pro oblast kybernetické bezpečnosti.

Omezit přístup k citlivým informacím pouze pro osoby, které tyto informace potřebují v rámci provádění nezbytných procesů.

Zde bude finanční náročnost malá, ale je potřeba vynaložit čas a úsilí pro prověření aktuálně volně dostupných informací a dat, následně tuto kontrolu udržet.

Spolupráce s Národním úřadem pro kybernetickou a informační bezpečnost

- V rámci posledního návrhu opatření pro zvýšení ochrany a bezpečnosti vodohospodářské infrastruktury doporučuji spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost, který je ústředním správním orgánem v oblasti kybernetické bezpečnosti, zaměřuje se na informační a komunikační systémy a kryptografickou ochranu.

Zmíněný úřad poskytuje celou řadu školení zaměřených na různé skupiny (běžné administrativní pracovníky, správce sítí a speciality, systémy firem apod.)

V příloze je poté možnost čerpat z doporučení vydanými právě Národním úřadem pro kybernetickou a informační bezpečnost, které jsou dle mého názoru vhodné a dostačují na posun ve vzdělání.

Tímto tedy doporučuji aplikovat normy z řady ISO 27 000. Konkrétně normu ISO 27 001: 2013 pro systém řízení bezpečnosti informací, je ideální výchozí normou

pro GDPR a potencionální hrozby jako je terorismus. Norma je rovněž kompatibilní a návazná na normu ISO 9001. Dále doporučuji rovněž aplikovat normu ISO 27002:2022 zaměřenou na informační bezpečnost, kybernetickou bezpečnost a ochranu soukromí, kontrolu bezpečnosti informací.

Cenový rozsah stanovit nelze, je to komplikovaný proces zavádění nového systému do již funkčního odlišného systému, většinou je původní systém zcela nahrazen.

ZÁVĚR

Diplomová práce se zaměřil na oblast ochrany vodohospodářské infrastruktury před možnou teroristickou hrozbou. Infrastruktura byla vybrána v oblasti jižní Moravy, kde se nachází akciová společnost Vodovody a Kanalizace Hodonín, která zajišťuje pitnou vodu zdejšímu průmyslu, ale především dodává kvalitní pitnou vodu téměř pro 140 000 obyvatel. Jedním ze zdrojů pitné vody je vodní dílo Koryčany, které spravuje státní podnik Povodí Moravy.

Záminkou pro volbu a následné zpracování je současný stav v oblasti pitné vody a nejisté bezpečnosti ve vztahu k možnému teroristickému útoku. Oblast je ovlivňována také globální situací, kdy dochází ke změnám klimatických podmínek a objevují se nová bezpečnostní rizika, kterým je potřeba čelit a být na ně připraven.

První část práce se zaměřuje na zpracování teoretické části, tedy teoretických poznatků o dané oblasti, jenž je v práci řešena. Značný prostor je poskytnut hned na úvodu práce terminologii, kdy se jedná o všeobecnou a následně konkrétnější terminologie pro danou problematiku. Její poznání je podmínkou pro chápání jednotlivých pojmů. Navazuje část infrastruktury a vodního hospodářství, důraz je kladen na význam pitné vody, její výroby a distribuci, neboť se jedná důležitý produkt. Část je věnována pro ochranu vod a vodních zdrojů. Doplnují to právní předpisy Evropské unie a České republiky, podle kterých se vodohospodářství řídí. Teorie v rámci ochrany pojednává o kybernetické bezpečnosti, důvod je zcela jasný, neustálý vývoj a pokrok technologií, které se implementují do procesů a systémů firem, to se týká i vodního hospodářství, značná část je v dnešní době řízena za pomoci počítačů. Někdy zcela bez dozoru lidí. Významné části jsou také terorismus, v rámci pochopení a definice, co všechno může tento pojem skrývat a jaké jsou metody teroristických útoků. Proti tomu je postavena technická a mechanická ochrana objektů, která se snaží chránit důležité zájmy například proti terorismu. Poslední část zde tvoří cíl a metodika práce.

Praktickou část tvoří získané informace a data pro naše konkrétní téma a oblast působnosti. Je zde uveden popis společnosti Vodovody a Kanalizace Hodonín a.s. a Povodí Moravy s.p. Jsou zde řešeny záležitosti týkající se aktuálního stavu ochrany a bezpečnosti, které jsou platné pro zvolené úpravny vod, vodní zdroje a distribuční soustavu. Následně je na základě zjištěných dat vytvořena analýza SWOT, která nám blíže určuje aktuální stav. Dále

se zde nachází v rámci analýzy popis zjištěných nedostatků a problémů, které ovlivňují úroveň ochrany po stránce vnější nebo vnitřní.

Poslední částí práce je tvorba aplikační části, kde je tato část zvolena formou plánu, který je stanoven bodově a poukazuje na zjištěné nedostatky, kdy se navrhuje vhodná opatření a zlepšení pro jednotlivé části. Mezi významné opatření můžeme zařadit budování nových plotů, širší pokrytí kamerovým systémem, posílení kybernetické bezpečnosti, školení zaměstnanců a v neposlední řadě lepší technické zabezpečení.

Přenesením poznatků, zjištění a vyhodnocení, by bylo možné ovlivnit část současného stavu ochrany vodohospodářské infrastruktury ve vztahu k teroristickému útoku.

Data je potřebné čerpat z historie, jelikož se jedná o skutečné události, ke kterým došlo a nebylo to žádné cvičení nebo simulace. Data mohou napomoci odhalit, jaké cíle nejspíše bude potřeba chránit a jaké prostředky budou ty nejefektivnější. Bohužel potřebné zkušenosti na to být připraven na sto procent není možné získat uskutečněním cvičení. Cvičení nám pouze může určit směr, jakým směrem se vydat.

SEZNAM POUŽITÉ LITERATURY

1. Vodohospodářská infrastruktura v obcích a náležitosti hospodaření s vodou, 2019. *Deník veřejné správy* [online]. [cit. 2022-01-24]. Dostupné z: <http://www.dvs.cz/clanek.asp?id=6774867>
2. ŠENOVSKÝ, Vilém ADAMEC a Pavel ŠENOVSKÝ, 2007. *Ochrana kritické infrastruktury*. Ostrava: Sdružení požárního a bezpečnostního inženýrství. ISBN: 978-80-7385-025-8.
3. Z historie společnosti, vodárenství a kanalizací, 2022. *Vodovody a kanalizace Hodonín* [online]. [cit. 2022-01-24]. Dostupné z: https://www.vak-hod.cz/?page_id=3447
4. KROČOVÁ, Šárka, 2009. *Strategie dodávek pitné vody*. Ostrava: Sdružení požárního a bezpečnostního inženýrství. ISBN: 978-80-7385-072-2.
5. Parametry pitné vody, 2022. *Severomoravské vodovody a kanalizace Ostrava* [online]. [cit. 2022-01-24]. Dostupné z: <https://www.smvak.cz/parametry-pitne-vody>
6. TOMEK, Miroslav, Jan STROHMANDL a Jakub RAK, 2014. *Zásobování obyvatelstva pitnou vodou za mimořádných událostí*. Praha: Academia. ISBN: 978-80-7454-462-0.
7. PAVLÍKOVÁ, Irena, 2014. *Enviromentální aspekty ochrany vod a půd: studijní opora*. Ostrava: VŠB – Technická univerzita. ISBN: 978-80-248-3576-1.
8. HORÁČEK, Zdeněk et al., 2013. *Vodní zákon s podrobným komentářem po velké novele stavebního zákona k 1. 1. 2013*. 2. Praha: SONDY. ISBN 978-80-86846-48-8.
9. Odstavec předpisu 274/2001 - Zákon č. 274/2001 Sb., o vodovodech a kanalizacích pro veřejnou potřebu a o změně některých zákonů, 2022. *Ministerstvo zemědělství České republiky* [online]. [cit. 2022-01-24]. Dostupné z: <https://eagri.cz/public/web/mze/legislativa/pravni-predpisy-mze/tematicky-prehled/100053200.html>

10. RICHTER, Rostislav, 2018. *Slovník pojmů krizového řízení*. Praha: Ministerstvo vnitra, generální ředitelství Hasičského záchranného sboru České republiky. ISBN: 978-80-87544-91-4.
11. Ministerstvo vnitra ČR, 2016. *Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování ochrany státu* [online]. Praha: Odbor bezpečnostní politiky a prevence kriminality [cit. 2022-07-20.] Dostupné z: <https://www.mvcr.cz/clanek/terminologicky-slovník-krizove-rizeni-a-planovani-obranystatu.aspx>.
12. Závěrečné práce – metodika, 2013. *LORENC.INFO* [online]. [cit. 2022-01-24]. Dostupné z: https://lorenc.info/zaverecne-prace/metodika.htm?fbclid=IwAR3Q4ZML72_io4vOTxaFAGf00I2APKhBSuBA9g_cT7p
13. VLÁDA ČR, 2022. *Kybernetická bezpečnost*. VLÁDA ČESKÉ REPUBLIKY [online], [cit. 2022-07-24]. Dostupné z: <https://www.vlada.cz/cz/evropske-zalezitosti/umela-inteligence/kyberneticka-bezpecnost/kyberneticka-bezpecnost-192766/>
14. SWOT analýza, 2022. *Krajské zařízení pro další vzdělávání pedagogických pracovníků a informační centrum*. Nový Jičín [online]. [cit. 2022-01-24]. Dostupné z: <https://www.kvic.cz/soubor/1343/SWOTanaliza.pdf>
15. BRZYBOHATÝ, Marian; 1999. *Terorismus I*. Praha: POLICE HISTORY. ISBN: 80-902670-1-7.
16. Strategie ČR pro boj proti terorismu od roku 2013. Ministerstvo vnitra České republiky [online]. [cit. 2022-06-07]. Dostupné z: <https://www.mvcr.cz/soubor/strategie-ceske-republiky-pro-boj-proti-terorismu-pdf.aspx>
17. SOULEIMANOV, Emil a kolektiv, 2010. *Terorismus pokus o porozumění*. Praha: SOCIOLOGICKÉ NAKLADATELSTVÍ. ISBN: 978-80-7419-038-4.
18. Audit národní bezpečnosti 2016. Vláda České republiky [online]. [cit. 2022-06-07]. Dostupné z: <https://www.vlada.cz/cz/media-centrum/aktualne/auditnarodnibezpecnosti-151410/>

19. Stockholmský program. Eur-lex [online]. [cit. 2020-05-05]. Dostupné z <https://eurlex.europa.eu/legal-content/CS/TXT/?uri=LEGISSUM%3Ajl0034>
20. Evropská bezpečnostní strategie. Rada Evropské unie [online]. [cit. 2022-06-07]. Dostupné z <https://www.consilium.europa.eu/cs/documentspublications/publications/european-security-strategy-secure-europe-better-world/>
21. Strategie EU pro boj proti terorismu. Rada Evropské unie [online]. [cit. 2022-06-07]. Dostupné z <https://www.consilium.europa.eu/cs/policies/fight-against-terrorism/eustrategy/>
22. Zákon č. 110/1998 Sb. o bezpečnosti ČR. Zákony pro lidi [online]. [cit. 2022-06-07]. Dostupné z <https://www.zakonyprolidi.cz/cs/1998-110>
23. MV ČR, 2022. *Terorismus a jeho projevy v někdejších Československu a dnešní České republice*. Ministerstvo vnitra České republiky [online], [cit. 2022-07-24]. Dostupné z: <https://www.mvcr.cz/clanek/terorismus-a-jeho-projevy-v-nekdejsim-ceskoslovensku-a-dnesni-ceske-republice.aspx>
24. MAREŠ, Miroslav, 2005. *Terorismus v ČR*. Brno: Centrum strategických studií, o.s. ISBN: 80-903333-8-9.
25. KindPNG. Anonymous Person Transparent [online], [cit. 2022-07-24]. Dostupné z: https://www.kindpng.com/imgv/TJTwiJ_anonymous-person-transparent-hd-png-download/
26. ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství ALEŠ Čeněk, s.r.o. ISBN: 91788073807375
27. STRAßNER, Alexander, 2003. *Die dritte Generation der "Roten Armee Fraktion"*. Publisher: VS Verlag für Sozialwissenschaften. ISBN: 3531141147.
28. KLEMENT, Cyril, Roman, MEZENECV, Jiří BAJGAR, 2013. *Biologické a chemické zbrane – připravenost a odpověď*. Banská Bystrica: Vydavateľstvo PRO. ISBN: 978-80-89057-43-6.
29. AQUA SHOP, 2022. *DEZINFEKCE VODY*. [online], [cit. 2022-07-24]. Dostupné z: <https://www.aqua-shop.cz/desinfekce-vody/>

30. UHLÁŘ, Jan, 2005. *Technická ochrana objektů II*. Praha: Policejní akademie České republiky. ISBN: 80-7251-189-0.
31. VaK Hodonín a.s. *Historie a vznik společnosti* [online]. [cit. 2022-08-02]. Dostupné z: <https://vak-hod.cz/spolecnost/z-historie-spolecnosti-vodarenstvi-a-kanalizaci/historie-a-vznik-spolecnosti/>
32. VaK Hodonín a.s. *Základní údaje* [online]. [cit. 2022-08-02]. Dostupné z:
33. VaK Hodonín a.s. *Chemická služba* [online]. [cit. 2022-08-02]. Dostupné z: <https://vak-hod.cz/sluzby/chemicka-sluzba/#>
34. VaK Hodonín a.s. *Mapa působnosti* [online]. [cit. 2022-08-02]. Dostupné z: <https://vak-hod.cz/wp-content/uploads/2021/12/mapaVodaBig.jpeg>
35. Informační systém EIA. *REKONSTRUKCE A INTENZIFIKACE ÚPRAVNY VODY A PRAMENIŠTĚ BZENEC* [online]. [cit. 2022-08-02]. Dostupné z: https://portal.cenia.cz/eiasea/detail/EIA_JHM147?lang=cs
36. VAK Hodonín a.s. *Mapa působnosti* [online]. [cit. 2022-08-02]. Dostupné z: <https://vak-hod.cz/wp-content/uploads/2021/12/mapaKanalBig.jpeg>
37. VaK Hodonín a.s. *Výroční zpráva 2021* [online]. [cit. 2022-08-02]. Dostupné z: <https://vak-hod.cz/vak/vyrocnizpravy/VyrocniZprava2021.pdf>
38. VaK Hodonín a.s. *20 LET ÚPRAVNY VODY BZENEC – PŘÍVOZ* [online]. [cit. 2022-08-02]. Dostupné z: https://vak-hod.cz/vak/dokumenty/20let_uvBzenec.pdf
39. VaK Hodonín a.s. *Informace o chemických látkách použitých při úpravě vody* [online]. [cit. 2022-08-02]. Dostupné z: https://vak-hod.cz/vak/dokumenty/info_o_chem_latkach.docx
40. Povodí Moravy s.p. *Vodní dílo Koryčany* [online]. [cit. 2022-08-02]. Dostupné z: <http://www.pmo.cz/cz/o-podniku/vodni-dila/korycany/>
41. VODARENSTVI.CZ. *Chřiby: Voda z hor pro Kyjovsko 2018* [online]. [cit. 2022-08-02]. Dostupné z: <https://www.vodarenstvi.cz/2018/05/11/chriby-voda-z-hor-pro-kyjovsko/>
42. Povodí Moravy s.p. *Činnost podniku* [online]. [cit. 2022-08-02]. Dostupné z: <http://www.pmo.cz/cz/o-podniku/predmet-cinnosti/>

43. VODARENSTVI.CZ. *Úpravna vody Koryčany* [online]. [cit. 2022-08-02]. Dostupné z: <https://www.vodarenstvi.cz/2018/05/11/chriby-voda-z-hor-pro-kyjovsko/>
44. MORAVSKÁ VODÁRENSKÁ, a.s. *Postupná modernizace úpravny vody Koryčany* [online]. [cit. 2022-08-02]. Dostupné z: <https://www.smv.cz/res/archive/014/001672.pdf>
45. iGIS.Web. *Mapa sítí v majetku a správě VaK Hodonín a.s.* [online]. [cit. 2022-08-02]. Dostupné z: <http://i-gis.vak-hod.cz/iGISWeb/map.aspx>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AČR	Armáda České republiky
ACH	Automated Cleaning House
Apod.	A podobně
APT	Pokročilá paralelní technologie
a.s.	Akciová společnost
BIS	Bezpečnostní a informační služby
BR	Počítače a informační technologie (Bit Rate)
CBRN	Chemické, biologické, radiologické a nukleární
CD	Kompaktní Disk
ČOV	Čistička odpadních vod
ČR	Česká republika
ČSN EN	Česká technická norma
DVD	Digital Video Disc
EIA	Environmental Impact Assessment
ETF	Electronic Funds transfer
EU	Evropská unie
GDPR	Obecné nařízení o ochraně osobních údajů
HDD	Pevný disk
HOPKS	Hospodářská opatření pro krizové stavy
HZS	Hasičský záchranný sbor
HZS ČR	Hasičský záchranný sbor České republiky
IS	Informační systém
IZS	Integrovaný záchranný systém
KB	Kybernetická bezpečnost
KOM	Komise Evropského Společenství

KS	Krizová situace
MU	Mimořádná událost
MV ČR	Ministerstvo vnitra České republiky
MZE	Ministerstvo zemědělství
NAS	Network Attached Storage (datové úložiště na síti)
NATO	North Atlantic Treaty Organization/Severoatlantická aliance
NLE	Síťové vrstvy síťování, Nelineární síť
NV	Nařízení vlády
ORP	Obec s rozšířenou působností
PČR	Policie České republiky
RAT	Remote Access Tool
C&C	Command and Control server
SAN	Storage area network
Sb.	Sbírký
s.p	Státní podnik
SCAM	Podvod, Analýza zdrojového kódu a manipulace
SD	Secure Digital
SOVAK	Sdružení oboru vodovodů a kanalizací ČR
SPAM	Nevyžádaná e-mailová pošta
SSD	Solid-state drive
SSHR	Správa státních hmotných rezerv
USA	Spojené státy americké
USB	Universal Serial Bus
VaK Hodonín	Vodovody a kanalizace Hodonín (akciová společnost)
WHO	World Health Organization

SEZNAM OBRÁZKŮ

OBRÁZEK 1: VODOVOD NADMÍSTNÍHO VÝZNAMU	25
OBRÁZEK 2: VODOVOD MÍSTNÍHO VÝZNAMU	25
OBRÁZEK 3: KDO JE TERORISTA A KDO NE?	42
OBRÁZEK 4: MAPA PŮSOBNOSTI VAK HODONÍN A.S. – VODOVODNÍ SÍŤ	53
OBRÁZEK 5: MAPA PŮSOBNOSTI VAK HODONÍN A.S. – KANALIZAČNÍ SÍŤ	54
OBRÁZEK 6: ÚPRAVNA VODY MORAVSKÁ NOVÁ VES – VSTUPNÍ BRÁNA	56
OBRÁZEK 7: ÚV MORAVSKÁ NOVÁ VES A PÁSMA HYGIENICKÉ OCHRANY	57
OBRÁZEK 8: ÚPRAVNA VODY BZENEC-KOMPLEX A PÁSMA HYGIENICKÉ OCHRANY ZDROJŮ VODY	59
OBRÁZEK 9: ÚPRAVNA VODY BZENEC	60
OBRÁZEK 10: ÚPRAVNA VODY KORYČANY	62
OBRÁZEK 11: ÚPRAVNA VODY KORYČANY A HYGIENICKÉ PÁSMO VODNÍHO DÍLA KORYČANY	63
OBRÁZEK 12: ČERPACÍ STANICE LOUKA A PÁSMO HYGIENICKÉ OCHRANY	64
OBRÁZEK 13: BRÁNA HORNÍ ČÁSTI HRÁZE KORYČANY	69
OBRÁZEK 14: ÚROVEŇ ZABEZPEČENÍ OCHRANNÉHO PÁSMO I. STUPNĚ	74

SEZNAM TABULEK

Tabulka 1: Charakteristika tradičního a nového terorismu	40
Tabulka 2: Vybrané údaje o distribuci vody a vodovodech	65
Tabulka 3: SWOT analýza stavu ochrany vybrané vodohospodářské infrastruktury	71
Tabulka 4: Ohodnocená tabulka SWOT analýzy	72
Graf 1: Grafické vyjádření strategie pro SWOT analýzu	72

SEZNAM PŘÍLOH

Příloha P I: CERTIFIKÁT VODOVODY A KANALIZACE HODONÍN

(Vak Hodonín,2022)

Příloha P II: PŘÍLOHA CERTIFIKÁTU VODOVODY A KANALIZACE HODONÍN

(Vak Hodonín,2022)

Příloha P III: TABULKA VYBRANÉ ÚDAJE O KANALIZACÍCH (Vak Hodonín,2022)

Příloha P IV: PODBROBNÉ TECHNICKÉ ÚDAJE VODNÍ DÍLO KORYČANY

(Povodí Moravy, 2022)

Příloha P V: DOPORUČENÍ NÚKIB I (NÚKIB, 2022)

Příloha P VI: DOPORUČENÍ NÚKIB II (NÚKIB, 2022)

PŘÍLOHA P I: PŘÍLOHA CERTIFIKÁTU VODOVODY A KANALIZACE HODONÍN



Současný certifikát vystaven: 15. červenec 2021
Platnost certifikátu do: 26. srpen 2022
Identifikační číslo certifikátu: 10378231

První certifikát vystaven:
ISO 14001 - 21. únor 2005
ISO 9001 - 21. únor 2005
ISO 50001 - 27. srpen 2016

Certifikát

Potvrzujeme, že systém managementu společnosti:

Vodovody a kanalizace Hodonín a. S.

Purkyňova 2/2933, Hodonín

byl schválen společností Lloyd's Register podle následujících standardů:

ISO 14001:2015, ISO 9001:2015, ISO 50001:2018

Číslo smlouvy: ISO 14001 – 0053488, ISO 9001 – 0053489, ISO 50001 – 0047308

Tento certifikát je platný pouze ve spojení s přílohou certifikátu označenou stejným číslem, kde je uveden seznam certifikovaných míst.

Rozsah certifikace je uplatněn na:

Provozování vodovodů a kanalizací pro veřejnou potřebu a související činnosti.

Paul Graaf

Chief Operating Officer, Management Systems, MSIS

Vystaveno v: Lloyd's Register EMEA

v zastoupení: Lloyd's Register Quality Assurance Limited



Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract. Issued by: Lloyd's Register EMEA, Tábořská 31, 140 00 Prague 4, Czech Republic for and on behalf of: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

PŘÍLOHA P II: CERTIFIKÁT VODOVODY A KANALIZACE HODONÍN



Identifikační číslo certifikátu: 10378231

Příloha certifikátu

Provozovny	Činnosti
Vodovody a kanalizace Hodonín, a.s. Purkyňova 2/2933, Hodonín	ISO 14001:2015, ISO 9001:2015, ISO 50001:2018 Provozování vodovodů a kanalizací pro veřejnou potřebu a související činnosti.
Provozní středisko Hodonín Na Salajce 4330, 695 01 Hodonín, Česko	ISO 14001:2015, ISO 9001:2015, ISO 50001:2018 Provozování vodovodů a kanalizací pro veřejnou potřebu a související činnosti.
Provozní středisko Kyjov Za humny 3281, 697 01 Kyjov, Česko	ISO 14001:2015, ISO 9001:2015, ISO 50001:2018 Provozování vodovodů a kanalizací pro veřejnou potřebu a související činnosti.
Provozní středisko Veselí nad Moravou Masarykova 1196, 898 01 Veselí nad Moravou, Česko	ISO 14001:2015, ISO 9001:2015, ISO 50001:2018 Provozování vodovodů a kanalizací pro veřejnou potřebu a související činnosti.



Lloyd's Register Group Limited, its affiliates and subsidiaries, including Lloyd's Register Quality Assurance Limited (LRQA), and their respective officers, employees or agents are, individually and collectively, referred to in this clause as 'Lloyd's Register'. Lloyd's Register assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant Lloyd's Register entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.
Issued by: Lloyd's Register EMEA, Tábořská 31, 140 00 Prague 4, Czech Republic for and on behalf of: Lloyd's Register Quality Assurance Limited, 1 Trinity Park, Bickenhill Lane, Birmingham B37 7ES, United Kingdom

PŘÍLOHA P III: TABULKA VYBRANÉ ÚDAJE O KANALIZACÍCH

Vybrané údaje o kanalizacích

Provoz kanalizací	Měrné jednotky	2017	2018	2019	2020	2021
Délka kanalizační sítě provozované celkem	km	594	602	602	619	620
Délka kanalizační sítě v majetku společnosti	km	294	295	297	297	297
Délka kanalizační sítě cizí provozované	km	300	307	305	322	323
Počet kanalizačních přípojek	ks	25 831	25 577	25 690	26 920	27 022
Délka kanalizačních přípojek	km	200	200	201	212	213
Počet ČOV provozovaných společnostmi	ks	24	24	25	26	26
- z toho mechanicko-biologické	ks	24	24	25	26	26
Počet ČOV v majetku společnosti	ks	14	14	14	14	14
Objem čištěných odpadních vod na ČOV	tis. m ³	7 321	7 297	8 294	9 568	8 916
Počet obyvatel napojených na kanalizaci	osob	105 315	105 351	105 412	108 316	108 232

PŘÍLOHA P IV: PODROBNÉ TECHNICKE ÚDAJE VODNÍ DÍLO KORYČANY

Základní údaje:

Nádrž:	VD Koryčany
Tok:	Kyjovka, km 74,50
Správce:	Povodí Moravy
Závod:	závod Střední Morava
Účel:	zajištění MQ, vodárenský odběr, protipovodňová ochrana
Uvedení do provozu:	1959

Nádrž:

Stálé nadržení:	0,102 mil. m ³
Hladina stálého nadržení:	293,10 m n.m.
Zásobní prostor:	2,130 mil. m ³
Hladina zásobního prostoru:	306,20 m n.m.
Prostor retenční neovladatelný:	0,332 mil. m ³
Hladina retenčního neovladatelného prostoru:	307,20 m n.m.
Celkový objem:	2,564 mil. m ³

Hráz:

Typ hráze:	zemní sypaná
Těsnění:	střední jílové těsnění
Kóta koruny:	308,25 m n.m.
Šířka koruny:	8,50 m
Délka hráze v koruně:	180,0 m
Výška hráze nade dnem:	20,00 m

Spodní výpusti:

Počet x průměr:	1 × 800, 1 × 600 mm
Provozní uzávěr:	kuželový
Kapacita při max. hladině:	7,33 + 2,77 m ³ /s

Asanační výpusti:

Počet x průměr:	1 × 200 mm
Kapacita při max. zás. hladině:	0,25 m ³ /s

Bezpečnostní přeliv:

Typ bezpečnostního přelivu:	boční, nehrazený
Počet polí x délka přelivu:	1 × 27,5 m
Kóta přelivu:	306,20 m n.m.
Kapacita při max. hladině:	55 m ³ /s

Hydrologické údaje:

Číslo hydrologického pořadí:	4-17-01-068
Plocha povodí:	27,61 km ²
Průměrný dlouhodobý roční průtok:	0,068 m ³ /s
Q ₁₀₀ :	42,500 m ³ /s
Q355d:	0,010 m ³ /s

Účinek nádrže:

Neškodný odtok:	8,000 m ³ /s
Minimální odtok:	0,010 m ³ /s

PŘÍLOHA P V: DOPORUČENÍ NÚKIB I

BEZPEČNOSTNÍ DOPORUČENÍ NÚKIB PRO ADMINISTRÁTORY 4.0



INFRASTRUKTURA



ČLEŇTE SÍŤ NA MENŠÍ CELKY (SEGMENTACE) A STRIKTNĚ ODDĚLUJTE UŽIVATELSKÁ PRÁVA NAPŘÍČ UŽIVATELI (SEGREGACE)
s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.

BLOKUJTE ŠKODLIVÉ IP ADRESY A DOMÉNY NA ÚROVNI GATEWAY (BLACKLISTY).

NASAŤTE SÍŤOVÉ SYSTÉMY DETEKCE / PREVENCE PRŮNIKU (IDS/IPS)
používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.

SLEDUJTE SÍŤOVÝ PROVOZ

pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.

UCHOVÁVEJTE SÍŤOVÝ PROVOZ

zřídlo kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu doporučujeme uchovávat po dobu minimálně 12 měsíců, více podle místních okolností a významu sítě – v případě kritické informační infrastruktury (KII) a u informačních systémů základní služby (PZS) podle zákona o kybernetické bezpečnosti a návazných vyhlášek je minimální lhůta 18 měsíců. V případě sítí strategického významu zvažte i možnosti automaticky aktivovaného píňého záznamu datového provozu (PCAP), a to jak na primárních, tak záložních systémech (např. webových nebo systémových serverech).

KONTROLUJTE PŘÍCHODÍ E-MAILY

pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokuje podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

POUŽÍVEJTE ŠIFROVANÉ SPOJENÍ MEZI POŠTOVNÍMI SERVERY (TLS)

pro zajištění důvěrnosti e-mailové komunikace, v ideálních případech použijte DANE (DNS-based Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je e-mailový provoz dešifrován.

PROVÁDĚJTE AUTOMATIZOVANOU DYNAMICKOU ANALÝZU OBSAHU E-MAILŮ A WEBŮ
prováděnou v sandboxu – hledejte podezřelá chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.

POVOLTE NA FIREWALLU POUZE ŽÁDOUNI SLUŽBY A STANDARDNÍ PROVOZ.
V případě koncových stanic nezapomeňte také blokovat spojení z Vámi nekontrolované sítě.

KONTROLUJTE POUŽÍVANÉ KLÍČE / CERTIFIKÁTY

především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.

ZAJIŠTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ
(povolených a blokových) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.

APLIKUJTE WHITELISTING WEBOVÝCH DOMÉN

pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistová malá procenta škodlivých domén.

VOLTE JEDNODUCHÉ DOMÉNOVÉ NÁZVY,

aby byly jasné viditelné případné záměny písmen ve phishingových e-mailech.

NASAŤTE ANTI-DDoS TECHNOLOGIE,

kteř můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Anti DDoS ochranu nasadte na kompletní IP rozsahy vaší organizace.

VYPRACUJTE DISASTER RECOVERY PLAN (DRP)

a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřazené pracovníky a CERT/CSIRT týmy.



STANICE A SERVERY



UDRŽUJTE AKTUÁLNÍ OPERAČNÍ SYSTÉM

pravidelnými aktualizacemi a v co nejkratší době aplikujte všechny vydané bezpečnostní záplaty.

UDRŽUJTE AKTUÁLNÍ SOFTWARE.

pravidelně kontrolujte verze instalovaného softwaru. U neaktuálního softwaru proveďte v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů nebo firmwarů zařízení.

NEPOUŽÍVEJTE NEPODPOROVANÉ PRODUKTY,

používejte pouze produkty (software i operační systémy), pro které jsou dostupné bezpečnostní záplaty.

OVĚŘUJTE IDENTITU APLIKACÍ A SOUBORŮ

a povolte jen ty důvěryhodné včetně skriptů a DLL knihoven. V prostředí Windows použijte Device Guard, AppLocker, popřípadě Zásady omezení softwaru (SRP).

PROVÁDĚJTE HARDENING KONFIGURACE UŽIVATELSKÝCH APLIKACÍ

– povolte jen funkcionality, která je vyžadována pro práci uživatelů. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.

POUŽÍVEJTE OBECNÉ PREVENTIVNÍ MECHANISMY,

kteř mohou pomoci ochránit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention) nebo SELinux v linuxových systémech.

AKTIVUJTE IDS/IPS SYSTÉMY NA KONCOVÝCH STANICÍCH

detekující anomální chování jako např. injekci kódu do jiných procesů, změnu chráněných registrových klíčů, zachytávání sísků kláves, načítání neznámých ovladačů, snahu o zajištění persistence a další.

ZAJIŠTĚTE CENTRALIZOVANÉ A ČASOVĚ SYNCHRONIZOVANÉ LOGOVÁNÍ SÍŤOVÝCH UDÁLOSTÍ

(povolených a blokových) s okamžitým automatickým vyhodnocováním a uložením pro kritickou informační infrastrukturu (KII) a provozovatele základní služby (PZS) po dobu minimálně 18 měsíců, pro významné informační systémy (VIS) po dobu minimálně 12 měsíců a pro ostatní systémy podle místních okolností a významu sítě.

FILTRUJTE OBSAH E-MAILŮ A PROPOUŠTĚJTE POUZE RELEVANTNÍ DRUHY PŘÍLOH

– po důkladné analýze chování uživatelů určete typy souborů, které potřebují posílat e-mailem. Ostatní formáty příloh blokuje – především spustitelný kód. Dále ověřte soulad přípony souboru a jeho skutečného formátu.

PRÁVIDELNĚ ZÁLOHUJTE DŮLEŽITÁ A CITLIVÁ DATA

jako např. obsah webového serveru, databázi nebo konfiguraci služeb. Zálohu umístěte do odděleného prostředí mimo produkční síť. Pravidelně testujte, jestli dokážete data obnovit a jestli jsou data po obnově funkční.

ZAVEĎTE STANDARD OPERATING ENVIRONMENT (SOE)

se standardizovanou konfigurací pro pracovní stanice i servery, kde budou vypnuty všechny nevyžádané funkcionality.

ZAMEZTE PŘÍMÉMU PŘÍSTUPU PRACOVNÍCH STANIC NA INTERNET

a směrujte provoz přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte vynutit pro IPv4 i IPv6.

POUŽÍVEJTE ANTI/VIROVÝ A BEZPEČNOSTNÍ SOFTWARE

a nástroje, které zakazují spouštění nebezpečných aplikací (mimo přesně definovaný seznam privilegovaných aplikací), či nástroje, které pomáhají chránit systém v době, kdy nejsou dostupné klasické bezpečnostní aktualizace.

ŠIFRUJTE DISKY

– zejména u přenosných počítačů – včetně centrální evidence klíčů.

VYUŽÍVEJTE TRUSTED PLATFORM MODULE (TPM),

tedy zabezpečený kryptografický modul pro generování a uložení hesel a kryptografických klíčů. Je-li jím počítač vybaven.

NASTAVTE HESLO UEFI/BIOS

unikátní pro každou stanici s centrální správou hesel.

VYNUCÍTE SECURE BOOT

a nastavte pořadí zařízení určených pro boot systému. Boot manager musí být zabezpečen heslem.

CHRAŇTE SE PŘED ÚTOKY NA HESLA

v všech služeb, kam se přihlašují uživatelé. Například pomocí fail2ban, využití funkcí určených pro ukládání hesel (Argon2, bcrypt, scrypt, PBKDF2) nebo CAPTCHA.

PRO SPRÁVU SERVERŮ POMOCI SSH VYUŽÍVEJTE PRO PŘIHLÁŠENÍ KLÍČE, ZAKAŽTE HESLA.

Pro svázaný otisk klíče se serverem, kde je použitý, využijte SSHFP záznamy v DNS ideálně v kombinaci s DNSSEC, který zajistí autenticitu odpovědí obsahující SSHFP záznam.

PROVÁDĚJTE HARDENING KONFIGURACE SERVEROVÝCH APLIKACÍ

tj. databází, webových aplikací, CRM systémů, účetních systémů, HR systémů a dalších systémů ukládání dat.

KONTROLUJTE PŘENOSNÁ MÉDIA

jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.

OMEZTE PŘÍSTUP K SERVER MESSAGE BLOCKU (SMB) A NETBIOSU

na pracovních stanicích a serverech, kdekoliv je to možné.

POUŽÍVEJTE REŽIM CHRÁNĚNÉHO PŘÍSTUPU PŘI PRÁCI SE SOUBORY NA ÚROVNI PRACOVNÍCH STANIC

může se např. jednat o Protected View nebo Protected mode.

VYNUCÍTE VYTÁČENÍ VPN,

pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.

ZAJIŠTĚTE FYZICKOU BEZPEČNOST IT TECHNIKY



SPRÁVA ÚČTŮ



ZAVEĎTE CENTRÁLNÍ SPRÁVU UŽIVATELSKÝCH ÚČTŮ A OPRAVNĚNÍ

a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci softwaru, úpravy registru atd.

VYNUCÍTE VÍCEFAKTOROVOU AUTENTIZACI

zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.

ODDĚLTE ADMINISTRÁTORSKÉ ÚČTY

Pro správu používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora je použit pouze ke správě Domain Controlleru (tzn. nepřistupuje na klientské stanice a servery).

PŘÍDĚLTE KAŽDÉMU ADMINISTRÁTORŮVI VLASTNÍ ÚČET

pro správu systémů. Nepoužívejte sdílené účty.

ZABEZPEČTE LOKÁLNÍ ADMINISTRÁTORSKÉ ÚČTY.

Nastavte unikátní heslo na každé stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).

VYNUCÍTE POUŽÍVÁNÍ SILNÝCH HESEL

s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovnkových výrazů. Vynutte změnu hesla, existuje-li podezření, že bylo kompromitováno.

PRÁVIDELNĚ KONTROLUJTE UŽIVATELSKÉ ÚČTY A JEJICH OPRAVNĚNÍ

a to jak lokální, tak centrálně spravované.



PŘÍLOHA P VI: DOPORUČENÍ NÚKIB II

BEZPEČNÝ POHYB V KYBERSVĚTĚ

JAK SI ZABEZPEČÍM POČÍTAČ NEBO SMARTPHONE?

OMEZÍM PŘÍSTUP DALŠÍCH OSOB K SOUKROMÝM I PRACOVNÍM ZAŘÍZENÍM.

CHRÁNÍM SVÁ DATA PRO PŘÍPAD ODCIZENÍ ČI ZTRÁTY ZAŘÍZENÍ.
Využívám silné heslo, číselný kód, gesto nebo jiný způsob zabezpečení.

NIKDY SI NEUKLÁDÁM PŘIHLAŠOVACÍ ÚDAJE K ZAŘÍZENÍM A ÚČTŮM V JEJICH BLÍZKOSTI.
Pro uchování přihlašovacích údajů používám šifrovaného správce hesel.

UJISTÍM SE, ŽE PŘI ZADÁVÁNÍ PŘIHLAŠOVACÍCH ÚDAJŮ JE NIKDO CIZÍ NEVIDÍ, NAPŘÍKLAD POHLEDEM PŘES RAMENO.

ZAMKNU ZAŘÍZENÍ POKAŽDÉ, KDYŽ OD NĚJ ODCHÁZÍM.
U počítače s Windows je nejjednodušší způsob rychlého zamknutí klávesová zkratka WIN + L a u mobilního zařízení stisknutí vypínacího tlačítka na jeho boku. Pokud odcházím na delší dobu, ukončím správce hesel a všechny doposud používané aplikace a služby s citlivými údaji jako e-mail nebo internetové bankovníctví.

AKTUALIZUJI SOFTWARE A NEVYPÍNÁM PRAVIDELNĚ AUTOMATICKÉ AKTUALIZACE SYSTÉMU.
Díky tomu zajistím opravu známých zranitelností, které by mohly ohrozit mé zařízení.

POUŽÍVÁM AKTUALIZOVANÝ ANTIVIROVÝ SOFTWARE A FIREWALL.

ZAPOJÍM WI-FI, BLUETOOTH, NFC A DALŠÍ BEZDRÁTOVÉ TECHNOLOGIE, JEN POKUD JE VYUŽÍVÁM.
Pro útočníka představují potenciální cestu do zařízení.

POKUD VYUŽÍVÁM NEZABEZPEČENOU WI-FI SÍŤ, VYUŽÍVÁM Tzv. VPN (VIRTUAL PRIVATE NETWORK) NEBOLI VIRTUÁLNÍ SOUKROMOU SÍŤ, KTERÁ ZABEZPEČÍ MOU KOMUNIKACI NA POTENCIÁLNĚ NEBEZPEČNÉ SÍTI.


ŠIFRUJI CITLIVÁ DATA NA EXTERNÍM DISKU A DALŠÍCH PŘENOSNÝCH ZAŘÍZENÍCH.
Tak budou v případě ztráty nebo odcizení nečitelná.

PRAVIDELNĚ ZÁLOHUJI DATA.
Využití mohu například externí disk. Důležité je, aby záloha byla na jiném místě než v mém zařízení, byla šifrována a připojena pouze v okamžiku zálohování.

DO MÝCH ZAŘÍZENÍ NEPŘIPOJUJI NEZNÁMÉ USB FLASH DISKY, EXTERNÍ DISKY A JINÁ PAMĚŤOVÁ ZAŘÍZENÍ.
Mohou obsahovat malware. V případě nutnosti připojit neznámé médium provedu jeho antivirovou kontrolu. Zaměstnavatel může k tomuto účelu poskytnout tzv. antivirovou pračku, tedy počítač bez připojení k internetu, kde je nainstalovaný aktualizovaný antivirový program.

PŘI PROCHÁZENÍ WEBU PREFERUJI WEBOVÉ STRÁNKY ZABEZPEČENÉ POMOCÍ PROTOKOLU HTTPS.
Https protokol poznáme podle zámku v adresním řádku:

 Stránky zabezpečené pomocí HTTPS

 <https://> Stránky s částečným šifrováním, nebo bez něj.
Nedoporučeno pro odesílání citlivých dat.

DÁVÁM POZOR, NA KTERÉ ODKAZY KLIKÁM.
Je-li to technicky možné, zkontroluji, že odkaz nevede na pozdělou URL adresu. Pokud nemohu ověřit, kam odkaz vede, neklikám na něj.

VYPÍNÁM NEŽÁDOUCÍ SLUŽBY OPERAČNÍHO SYSTÉMU.
Například monitorování polohy, odesílání diagnostických dat, ovládání vzdáleného počítače na dálku, apod.

JAK MÁM SPRÁVNĚ A BEZPEČNĚ KOMUNIKOVAT?

K INFORMACÍM NA INTERNETU PŘÍSTUPUJI KRITICKY, NEMUSÍ BÝT PRAVDIVÉ.
Při práci s informacemi mohu využít rady, které sepsala iniciativa ZVOLSLINFO ve svém Surfarové průvodci internetem.

NEZVEŘEJŇUJI OSOBNÍ ANI CITLIVÉ INFORMACE O MNĚ, MĚ RODINĚ, PŘÁTELECH NEBO SPOLUPRACOVNÍCÍCH.
Data narození, náboženské vyznání nebo fotografie mohou být zneužity.

INTIMNÍ FOTOGRAFIE A VIDEA NEVYTVÁŘÍM, NEUMISŤUJI JE NA INTERNET ANI JE NIKOMU NEPOSÍLÁM.
Nikdy nevím, kdy může být takový materiál zneužit.

PŘI KOMUNIKACI SI VŽDY OVĚŘUJI IDENTITU PROTISTRANY.
Mohu se zeptat přítele nebo si dotyčného vyhledat na internetu. Pokud si nejsem jist, zda mi skutečně volají například z IT oddělení naší instituce, nebo mě po telefonu úkoluje nadřízený, kterého neznám, zavěším a zavolám zpátky na telefonní číslo z oficiálního seznamu.

NIKDY NEOTEVÍRÁM PHISHINGOVÉ E-MAILY A PODEZŘELÉ PŘÍLOHY A INFORMUJI IT ODDĚLENÍ.
V práci podezřelý e-mail neotevírám a informuji o něm IT oddělení. Stejně tak neotevírám podezřelé přílohy. Pokud mi takový e-mail dorazí do mé osobní schránky, mohu to nahlásit provozovateli schránky.

JAK PHISHING POZNÁM?
"Phishing je podvodná technika, prostřednictvím které se útočníci snaží například získat mé osobní nebo citlivé informace (přihlašovací údaje, datum narození, číslo platební karty atd.), nasměrovat mě na podvodnou stránku, nebo mi zaslat závadnou přílohu. Phishing se nejčastěji šíří formou e-mailových zpráv, které vypadají jako odeslané z důvěryhodných institucí." Podvodník používá obecná oslovení typu „Vážený pane/í“ bez uvedeného jména, v textu e-mailu mohou být gramatické, stylistické a grafické chyby, obsahuje podezřelé vyhlížející odkazy typu <https://www.xbamka.cz>.

V KOMUNIKACI NEJSEM ZBYTEČNĚ SDÍLŇ.
Vše, co na sebe prozradím, může být zneužito.

NENÍ OBĚD ZADARMO A TO ANI V ONLINE SVĚTĚ.
Zpozorním, jsou-li mi zdarma nabízeny jindy placené služby nebo produkty. Pokud za produkt neplatím, jde o má data.

RANSOMWARE JE PROGRAM, KTERÝ ZAŠIFRUJE DATA NEBO CELÝ OPERAČNÍ SYSTÉM A NABÍZÍ JEJICH ZPŘÍSTUPNĚNÍ AŽ PO ZAPLACENÍ VÝKUPNĚHO.
Do zařízení se mi může takový program dostat po otevření neznámé přílohy v e-mailu, z webového prohlížeče nebo tím, že navštívím infikovanou webovou stránku. Před známými druhy ransomware mě chrání aktualizovaný antivirový program. Svá data chráním také pravidelným zálohováním.

PŘI KOMUNIKACI NESPĚCHÁM A VŠE SI PROMYSLÍM.
Útočníci rádi pracují s časovou tísň - teď je třeba něco vykonat, napravit, sdělit. Klid! Škoda z prodlení bývá menší, než důsledky neuvážených činů.

JAK ZABEZPEČÍM MÉ ONLINE ÚČTY?

PŘÍSTUPY K PRACOVNÍM I OSOBNÍM ÚČTŮM SI CHRÁNÍM SILNÝM HESLEM.
Hesla nikdy nepišu na papírky a nenechávám například na monitoru nebo pod klávesnicí. To platí jak v kanceláři, tak i doma.

U SILNÉHO HESLA ZADÁVÁM ALESPŮŇ 12 ZNAKŮ A VÍCE.
Při jeho tvorbě jsem originální a kreativní. Využívám malá a velká písmena, číslice, speciální znaky a další symboly. Mohu si zvolit například unikátní větu nebo souvětí, které si lze snadno zapamatovat.

PRO KAŽDOU SLUŽBU POUŽÍVÁM JINÉ UNIKÁTNÍ HESLO.
To platí u pracovních účtů a zařízení bez výjimky. V soukromí se této zásady držím u služeb, které mohou obsahovat osobní a citlivé informace.

NEVYUŽÍVÁM ONLINE NÁSTROJE ČI SLUŽBY PRO KONTROLU SILY HESLA.
Výsledkem může být to, že heslo předám útočníkovi, který si díky tomu doplní vlastní databázi používaných hesel.

PROTOŽE JE OBTÍŽNĚ ZAPAMATOVAT SI VŠECHNA HESLA, VYUŽÍVÁM PRO TA MĚNĚ VÝZNAMNÁ SPRÁVCE HESEL.
Ten mi umožňuje bezpečně uložit a spravovat velké množství hesel. Přístup do něj je chráněn jedním silným zastrešujícím heslem ideálně v kombinaci s vícefaktorovým ověřením.

NESDÍLÍM PŘIHLAŠOVACÍ ÚDAJE K VLASTNÍM ÚČTŮM A SLUŽBÁM.
V případě pracovního e-mailu, pracovního intranetu, docházkového systému nebo hesla do počítače může mít takové jednání závazné následky.

U KRITICKÝCH SLUŽEB JAKO ELEKTRONICKÉ BANKOVNICTVÍ, PRACOVNÍ NEBO SOUKROMÝ E-MAIL VŽDY VYUŽÍVÁM VÍCEFAKTOROVOU AUTENTIZACI.
Příkladem může být elektronické bankovníctví, kdy musím přihlášení v prohlížeči potvrdit zadáním kontrolní SMS nebo potvrzením výzvy v mém mobilním telefonu. Pokud se do služby přihlašuji z mobilního telefonu, nechám si potvrzovací SMS zaslat na jiné zařízení.

ODDĚLÍM ADMINISTRÁTORSKÝ ÚČET OD BĚŽNÉHO
Administrátorský účet používám pouze pro správu systému. Pro ostatní pracovní aktivity jako odesílání e-mailů nebo procházení webu využívám běžný neprivilegovaný účet.

NEPOUŽÍVÁM KONTROLNÍ OTÁZKY PRO OBNOVENÍ HESLA.
Nepoužívám kontrolní otázky pro obnovení hesla. Nikdy si jako alternativu k heslu nezadávám kontrolní otázky typu "přijmení třídní učitelky z páté třídy" nebo "nejmenší planeta sluneční soustavy". Podobné informace jsou dohledatelné z veřejných zdrojů. Je-li kontrolní otázka povinná, chovám se k ní jako k heslu a volím ji tak, aby nebyla dohledatelná. Např. k otázce „Jaké bylo vaše jméno za svobodna“ zvolím odpověď „N9qy5_@79b7G8_tp“.

