Informační bezpečnost v subjektu ochrany obyvatelstva

Markéta Jurčová

Bakalářská práce

2024

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Markéta Jurčová**
Osobní číslo:	**L21403**
Studijní program:	**B1032A020002 Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Informační bezpečnost subjektu ochrany obyvatelstva**

Zásady pro vypracování

1. Vymezte základní pojmy a zpracujte teoretický vstup do dané problematiky.
2. Zvolte subjekt ochrany obyvatelstva vhodný pro posouzení informační bezpečnosti.
3. Proveďte analýzu informační bezpečnosti vybraného subjektu ochrany obyvatelstva.
4. Navrhněte případná opatření pro zlepšení stavu informační bezpečnosti vybraného subjektu.

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

Seznam doporučené literatury:

1. AWAD, Ali Ismail, FAIRHURTS, Michael. *Information Security: Foundations, Technologies and Applications*. London: The Institution of Engineering and Technology, 2018. ISBN 9781849199742.
2. DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
3. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC, 2019. ISBN 978-80-88168-31-7.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **1. prosince 2023**
Termín odevzdání bakalářské práce: **3. května 2024**

L.S.

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 4. prosince 2023

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou 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 – bakalářskou 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 bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne: 3.5.2024

Jméno a příjmení studenta: Markéta Jurčová

.....
podpis studenta

ABSTRAKT

Tato práce se zabývá vybraným subjektem ochrany obyvatelstva a jeho informační bezpečností. Je rozdělená na dvě části teoretickou a praktickou. Teoretická část se zabývá vstupem do dané problematiky ochrany obyvatelstva a informační bezpečnosti.

Praktická část se zabývá analyzováním informační bezpečnosti, návrhem na zabezpečení pro daný subjekt. Provedené dotazníkové šetření hodnotí znalosti potřebné k zabezpečení informací a dat. Na základě zjištěných informací práce navrhuje opatření v podobě školení pro zlepšení současného stavu.

Klíčová slova: data, informace, informační bezpečnost, zabezpečení.

ABSTRACT

This work deals with a selected subject of population protection and its information security. It is divided into two parts: theoretical and practical. The theoretical part deals with the entry into the issue of population protection and information security.

The practical part involves analyzing information security and proposing security measures for the given subject. The conducted questionnaire assesses the knowledge necessary for securing information and data. Based on the findings, the work suggests measures in the form of training to improve the current state.

Keywords: Data, Information, Information Security, Security.

Tímto bych chtěla poděkovat panu Ing. Petrovi Svobodovi Ph.D., který mou práci vedl, za jeho pomoc při psaní, a také za cenné rady a zkušenosti.

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

OBSAH

ÚVOD

Informační bezpečnost je důležitou součástí lidské společnosti. Je také základním prvkem bezpečnosti v ochraně obyvatelstva. Informační bezpečnost je dlouhodobě podceňované téma širokou veřejností. (Kolouch, 2019) Oblast ochrany obyvatelstva pracuje s velmi důležitými daty a informacemi, které mají citlivý nebo osobní charakter. Tyto informace jsou často označovány jako informace utajené, nebo vyhrazené pro osoby s povolením. Data a informace mohou mít hodnotu, která motivuje pachatelé trestné činnosti spojené s informační bezpečnosti. (Doucek, 2019)

Tato práce se zabývá subjektem ochrany obyvatelstva, který je označen jako sbor dobrovolných hasičů. Je velmi důležité zabývat se na této úrovni ochrany obyvatelstva informační bezpečností. Bezpečnost může být u sborů narušená různým způsobem. Může se jednat primárně o bezpečnost dat, správné zálohování, aktualizace a manipulace s daty, ale také jejich zabezpečení proti krádeži, úniku nebo poškození. Bezpečnost může narušit osoba, která nezná správný postup, jak správně zálohovat, aktualizovat, či šifrovat data, nebo neovládá systém, do které data ukládá. Může tak dojít k znehodnocení, nebo ztrátě dat a informací. Tento systém může být i ohrožen osobou, snažící se získat informace a data za finančním účelem, nebo za jinou motivací. (Červenka, 2012)

Subjektem ochrany obyvatelstva byl vybrán Sbor dobrovolných hasičů, na kterém bude hodnocená informační bezpečnost. Práce se zabývá odhalením slabých míst, jejich hodnocením a doporučením na zlepšení. Aktuálnost této problematiky v posledních letech narůstá ve významu páchání trestné činnosti spojené s odcizením vybavení. Pokud pachatelé dokážou nepozorovaně vniknout na stanici, mohou se dostat k informacím a datům, které mohou zneužít, nebo k zařízením, které mohou odcizit a získat z nich informace. Těchto případu v několika posledních letech přibývá, sbory začaly více řešit fyzickou bezpečnost budov, avšak ne samotných informací. (Vraný, 2021)

Je proto nezbytné se problematikou informační a kybernetické bezpečnosti zabývat na úrovni sborů dobrovolných hasičů, riziko v dalších letech poroste a prevence může sehrát svou důležitou roli v řešení incidentů. Vybraný subjekt se může stát cílem hrozeb ze stran jeho členů mnohem více, než že by se stal cílem pachatelů, přesto je potřeba hrozby umět pojmenovat a uvědomit si jejich riziko, které subjektu hrozí. Na základě těchto znalostí se dá aplikovat bezpečné předcházení hrozeb, nebo jejich neprodlené odvrácení.

Cílem práce je posouzení informační bezpečnosti vybraného subjektu. Tento hlavní cíl bude naplněn pomocí následujících dílčích cílů. Zpracování teoretického vstupu do dané

problematiky, provedení zhodnocení informační bezpečnosti subjektu, dotazníkové šetření pro zjištění současného stavu znalostí informační bezpečnosti subjektu, návrh opatření pro zvýšení informační bezpečnosti vybraného subjektu. Navrhnuté opatření je školení, které by zvýšilo znalost informační bezpečnosti v subjektech zabývající se ochranou obyvatelstva. Popis informačního systému byl proveden na základě konzultace s vybraným subjektem a metodou pozorování v daném subjektu. Pozorování zahrnovalo několik osobních schůzek v daném subjektu s odpovědnou osobou, následovala prohlídka bezpečnostních prvků a konzultace. Práce se zaměřila především na výjezdovou jednotku z důvodu, zaujetí nejpodstatnější části, je zde také nejvíce členů. Výjezdová jednotka nejvíce pracuje se zařízeními a s osobními a citlivými údaji.

Práce se zabývá ochranou dat a informací primárně v digitální podobě. Práce odhalila nedostatek ve vzdělávání v oblasti informační bezpečnosti, toto tvrzení se potvrdilo v dotazníkovém šetření. Na základě dotazníkového šetření bylo provedeno školení, které mělo za cíl zlepšení kvality vzdělání v dané oblasti. Školení přineslo zlepšení znalosti osob vybraného subjektu a navrhlo financování a realizaci školení i pro jiné sbory dobrovolných hasičů.

Analýza je zahrnuta v praktické části v posuzování současného stavu subjektu a navržení opatření, je zahrnuta také v hrozbách pro subjekt. V teoretické části byla využita metoda analýzy, která se zabývala dostupnými zdroji, ze kterých byl vytvořen teoretický vstup do problematiky pomocí metody syntézy. Deskripce je využitá v seznámení s vybraným objektem ochrany obyvatelstva a jeho funkce. Dotazníkové šetření kvantitativní metoda sběru informací byla využitá pro hodnocení v praktické části. Indukce využitá v teoretické části při stanovení obecného závěru na konci části. Dedukce se nachází v praktické části při popisu informační bezpečnosti vybraného subjektu. Pozorování v praktické části aktuální zabezpečení subjektu a následné implementace zabezpečení. Komparace v práci je srovnávání využito v praktické části při porovnání dotazníkového šetření před a po školení. Syntéza spojení jednotlivých částí do konečného celku v závěru praktické části.

I. TEORETICKÁ ČÁST

1 PRÁVNÍ NORMY

Zákon č.1/1993 Sb., Ústava České republiky

„*Ústava České republiky, zákon č. 1/1993 Sb., je základním právním dokumentem České republiky. Byla přijata 16. prosince 1992 a stala se účinnou 1. ledna 1993. Česká republika je svrchovaný, jednotný a demokratický právní stát, který respektuje práva a svobody občanů. Česká republika dodržuje závazky z mezinárodního práva. Lid je zdrojem veškeré státní moci a vykonává ji prostřednictvím orgánů moci zákonodárné, výkonné a soudní. Politický systém je založen na svobodném vzniku a volné soutěži politických stran. Ústava zaručuje ochranu základních práv a svobod a stanovuje, že jsou pod ochranou soudní moci*.“ Ústava je tak nejdůležitějším právním dokumentem v České republice, který zaručuje základní lidská práva a povinnosti a zajišťuje, že budou dostupná a nezrušitelná pro každého. (Zákon č. 1/1993 Sb., Ústava České republiky)

Zákon č. 110/1998 Sb., Ústavní zákon o bezpečnosti

Ústavní zákon o bezpečnosti České republiky, upravuje zajištění bezpečnosti státu prostřednictvím regulace krizových stavů – nouzového stavu, stavu ohrožení státu a válečného stavu. Dále zřizuje Bezpečnostní radu státu a umožňuje zkrácené projednávání opatření v těchto krizových situacích. Zajištění svrchovanosti a územní celistvosti České republiky. Ochrana demokratických základů, životů, zdraví a majetkových hodnot je základní povinností státu. Nouzový stav, stav ohrožení státu a válečný stav mohou být vyhlášeny v závislosti na intenzitě, územním rozsahu a charakteru situace. Ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby jsou zodpovědné za zajištění bezpečnosti České republiky. Státní orgány, územní samosprávné celky a právnické a fyzické osoby jsou povinny se podílet na zajišťování bezpečnosti. Ozbrojené síly jsou doplňovány na základě branné povinnosti. (Zákon č.110/1998 Sb., Ústavní zákon o bezpečnosti České republiky)

Krizový zákon 240/2000 Sb. a zákon 241/2000 o hospodářských opatřeních

„*Zákon, který upravuje působnost a pravomoc státních orgánů a orgánů územních samosprávných celků, práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením. Tento zákon vymezuje několik pojmů, které se vztahují k ochraně obyvatelstva.“* (Zákon č. 240/2000 Sb., o krizovém řízení) Na krizový zákon navazuje zákon č. 241/2000 Sb. o hospodářských opatřeních pro krizové stavy, který upravuje hospodářská opatření pro krizové stavy. To zahrnuje různá opatření, která mohou být přijata

za účelem udržení stability a ochrany občanů. Tyto zákony jsou důležité pro správné fungování státu během krizového stavu a stanovení povinností právnickým a fyzickým osobám. (Zákon 241/2000 Sb., o hospodářských opatření pro krizové stavy)

Zákon č. 273/2008 Sb. o policii České republiky

„*Upravuje postavení, činnost, řízení a organizaci policie jako jednotného ozbrojeného bezpečnostního sboru. úkolem je chránit bezpečnost osob a majetku, udržovat veřejný pořádek, předcházet trestné činnosti a plnit úkoly podle trestního řádu a mezinárodních smluv. Působí na území České republiky, pokud zákon neustanoví jinak. Policisté a zaměstnanci policie vykonávají úkoly spojené s ochranou veřejnosti, vyšetřováním trestných činů a udržováním pořádku*.“ Policie České republiky se podílí na udržování pořádku a dodržování platných právních norem, snižuje tak páchání trestné činnosti a občanům zajišťuje bezpečnost života, zdraví a majetku. Podílí se na pomoci při mimořádných událostech právě i udržováním pořádku a dopravních cest pro evakuaci. (Zákon č. 273/2008 Sb., o policii České republiky)

Zákon č. 320/2015 Sb., o hasičském záchranném sboru České republik

„*Hasičský záchranný sbor je jednotný bezpečnostní sbor, jehož hlavním úkolem je chránit životy a zdraví obyvatel, životní prostředí, zvířata a majetek před požáry a jinými mimořádnými událostmi. Dále se podílí na zajišťování bezpečnosti České republiky plněním úkolů požární ochrany, ochrany obyvatelstva, civilního nouzového plánování, integrovaného záchranného systému, krizového řízení a dalších úkolů stanovených zákonem a dalšími právními předpisy. Hasičský záchranný sbor spolupracuje s Ministerstvem zahraničních věcí při organizaci přijímání humanitární pomoci poskytované České republice ze zahraničí.*“ (Zákon č. 320/2015 Sb., o hasičském záchranném sboru České republik) Hasičský záchranný sbor se podílel na humanitární pomoci v České republice v roce 2021 na jižní Moravě při tornádu, a v roce 2022 v Českém Švýcarsku. (Hasičský záchranný sbor Jihomoravského kraje, 2021) V roce 2002 se podílel hasičský záchranný sbor na záchranných a likvidačních pracích při rozsáhlých povodních. Hasičský záchranný sbor může být i podnikový, kdy je sbor přiřazen k danému podniku, kde se vyskytuje riziko vzniku mimořádné události. Zaměstnanci pracují na plný úvazek jako hasiči, jejich působnost je v místě areálu podniku. (Hasičský záchranný sbor, 2024)

Zákon č. 374/2011 Sb., o zdravotnické záchranné službě v České republice

„*Zákon upravuje podmínky poskytování zdravotnické záchranné služby. Práva a povinnosti poskytovatelů zdravotnické záchranné služby. Povinnosti poskytovatelů akutní lůžkové péče k zajištění návaznosti na zdravotnickou záchrannou službu. Podmínky pro zajištění připravenosti na řešení mimořádných událostí a krizových situací*.“ Záchranná služba se významným způsobem podílí na záchranných pracích při mimořádných událostech. Jsou nepostradatelnou složkou integrovaného záchranného systému. Spolu s policii a hasiči tvoří integrovaný záchranný systém. důležité, aby složky mezi sebou komunikovaly a spolupracovaly, podílí se na společném cvičení při přípravě na mimořádné události. (Zákon č. 374/2011 Sb., o zdravotnické záchranné službě v České republice)

Zákon č. 133/1985 Sb., o požární ochraně

Jedná se o zákon, který je považován za jeden z nejdůležitějších při řešení mimořádných události. Je potřeba plošného pokrytí kraje jednotkami požární ochrany, tento zákon upravuje povinnosti a postavení orgánů, jednotek a osob na úseku požární ochrany. „*Jeho účelem je vytvořit podmínky pro účinnou ochranu života, zdraví občanů a majetku před požáry a poskytování pomoci při živelních pohromách a jiných mimořádných událostech. Zákon stanovuje povinnosti ministerstev, správních úřadů, právnických a fyzických osob, a také postavení a povinnosti jednotek požární ochrany. Zákon také řeší spolupráci mezi různými subjekty v oblasti požární ochrany. Zákon obsahuje ustanovení týkající se čištění, kontroly a revize spalinové cesty. Zákon stanovuje pravidla pro náhradu škody v případě požárů a dalších mimořádných událostí. Byl naposledy aktualizován 22. března 2024 (verze 23). Tato novela zákona přinesla změny ve znění zákona o požární ochraně. Předchozí významnou novelou byl zákon č. 415/2021 Sb., který nabyl účinnosti 26. října 2021 a také upravoval zákon o požární ochraně.*“ (Zákon č. 133/1985 Sb., o požární ochraně)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Pro informační a kybernetickou bezpečnost v české republice je zákon o kybernetické bezpečnosti č.181/2014 sbírky. „*Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.*“ (Zákon č.181/2014 Sb., o kybernetické bezpečnosti)

„*Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zpracovává příslušné předpisy Evropské unie (jedná se o transpozici směrnice NIS) a upravuje zajišťování*

bezpečnosti sítí elektronických komunikací a informačních systémů.“ (Národní úřad pro kybernetickou a informační bezpečnost, 2023)

Zákon jako takový je poměrně stručný a spíše se zabývá definicemi, určení povinností. Subjekt jako takový má podle tohoto zákona incident nahlásit na poskytovatele internetu, který se bude podílet na řešení a o incidentu bude v případě většího rozsahu informovat autority. Tento zákon se zabývá problematikou jen velmi povrchně a neúplně. Proces řešení incidentu ze strany poskytovatele je zdlouhavé a náročné, v mnohých případech se povede filtrovat útok, ale ve většině případu se nepovede pachatele zjistit. (Zákon č.181/2014 Sb., o kybernetické bezpečnosti)

Národní úřad pro kybernetickou bezpečnost zveřejnil v roce 2023 návrh na změnu tohoto zákona. „*Široká veřejnost tak měla unikátní příležitost podílet se na tvorbě zákona, který povede ke zvýšení kybernetické bezpečnosti České republiky.*“ Na tvorbě tohoto dokumentu se mohla podílet široká veřejnost, která měla možnost své připomínky a návrhy anonymně zasílat na webové stránky. Tento zákon by měl reagovat na rychlou změnu vývoje prostředí pro bezpečnost, zákon bude v souladu se směrnicí Evropské unie NIS. (Národní úřad pro kybernetickou a informační bezpečnost, 2023)

Zákon č. 101/2000Sb., o ochraně osobních údajů

„*Zákon se zabývá ochranou osobních údajů, cílem zákona je stanovit práva a povinnosti při zpracování osobních údajů a také podmínky pro předání údajů do jiných států. Byl zrušen k 24. dubnu 2019 a nahrazen zákonem č. 110/2019 Sb., který upravuje zpracování osobních údajů v České republice a navazuje na nařízení Evropské unie 2016/679. Dodržování tohoto zákona má v gesci Úřad pro ochranu osobních údajů. Stanovuje základní principy ochrany osobních údajů, definuje klíčové pojmy a upravuje práva subjektů údajů. Zabývá podmínkami a omezeními při zpracování osobních údajů, včetně povinností správců a zpracovatelů. Práva, která mají jednotlivci v souvislosti se svými osobními údaji, jako je právo na přístup, opravu, výmaz a omezení zpracování. Pravomoc a povinnosti Úřadu pro ochranu osobních údajů, který dohlíží na dodržování zákona. Upravuje postihy za porušení zákona a sankce, které mohou být ukládány.*“ (Zákon č. 101/2000 Sb. o ochraně osobních údajů) Tento zákon je důležitý z hlediska nakládání s osobními údaji, se kterými se setkáváme v každodenním životě, které se uchovávají pro různé účely. Osobní údaje zapisujeme jako zaměstnavatelé nebo zaměstnanci do smluv, veřejná správa osobní údaje zpracovává pro různé dokumentární účely, firmy zpracovávají osobní údaje klientů. Osobní údaje můžeme nalézt i v digitální podobě na webových stránkách, které shromažďuji údaje,

jako jsou příjmení, emailové adresy, telefonní čísla. (Zákon č. 110/2019 Sb. o zpracování osobních údajů)

S nárustem zadávání osobních a citlivých informací v kyberprostoru vzniklo GDPR, Obecné nařízení o ochraně osobních údajů. Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, bylo vyhlášeno dne 27. dubna 2016 a vstoupilo v platnost 25. května 2018. Cílem je výrazně zvýšit ochranu osobních dat občanů. Komentář k GDPR přináší podrobný výklad se zohledněním zkušeností z prvních dvou let jeho účinnosti. Obsahuje relevantní výkladová stanoviska, rozhodnutí a publikované názory Úřadu pro ochranu osobních údajů a také vodítek Evropského sboru pro ochranu osobních údajů. GDPR má za cíl omezení nakládání s osobními údaji, tak aby měl uživatel opět kontrolu nad tím, jak se s daty nakládá. Jedním z největších problému se staly nadnárodní platformy, které díky GDPR musí dodržovat platná pravidla o tom, jak s údaji nakládat. (Uřičař, 2020)

Na webových stránkách nalezneme cookies nástroje, které sbírají informace o tom, co si na webu lidé prohlížejí, kde nakupují a co je předmětem jejich nákupu, mohou to být také sociální sítě a data, která z nich sbírají. Tyto nástroje se tváří neškodně z hlediska, že provozovatelé webových stránek chtějí mít přehled o produktech, aby mohli zacílit svou reklamu na to, o jaký produkt máme zájem. Tyto informace mohou zaznamenávat mnohem více dat, které bychom nechtěli, aby provozovatelé webových stránek měli k dispozici. Úřad pro ochranu osobních údajů definuje několik pravidel, jak na webových stránkách provozovat cookies v rámci platných nařízení. (Portál veřejné správy, 2024)

Zákon č. 412/2005 Sb., o utajovaných informacích

Zákon č. 412/2005 o utajovaných informacích pojednává o tom, co jsou to utajované informace a jak s těmito informacemi nakládat. „*Stanovuje základní definice a principy týkající se utajovaných informací a jejich ochrany. Specifikovány kategorie informací, které mohou být považovány za utajované, a podmínky pro jejich označení. Zabývá podmínkami pro přístup k utajovaným informacím, včetně oprávněných osob a postup. Ustanovení týkající se způsobů ochrany utajovaných informací, včetně fyzických a technických opatření. Věnuje se podmínkám pro výkon citlivých činností ve státní správě. V zákonu jsou uvedeny tresty za porušení zákona o utajovaných informacích*.“ Utajované informace se týkají finančních institucí, které musí chránit informace svých klientů, ale také firmy a organizace chránící důležité informace, například konkurenční výhodu. V ochraně obyvatelstva sehrávají utajované informace důležitou roli. (Zákon č. 412/2005 Sb., o utajovaných informacích)

„*Při zneužití utajované informace by subjektu vznikla újma, proto je subjekt ten, kdo má zájem na utajení těchto informací. Utajení může být trvalé, nebo jen po určitou dobu. Na únik utajované informace může mít vliv lidský faktor, nebo selhání technických systému. Prvky informační bezpečnosti se skládá z jednotlivých prvků personální bezpečnosti, režimové bezpečnosti, bezpečnost dat, bezpečnost komunikačních systému, fyzická bezpečnost, bezpečnost programových prostředků. Platnost osvědčení pro fyzické osoby je na vyhrazené informace 12 let, důvěrné 9 let, tajné 7 let a přísně tajné 5 let*.“ (Tomek, 2018)

Vyhláška č. 317/2014 Sb. o významných informačních systémech

Vyhláška č. 317/2014 Sb. stanovuje pravidla pro významné informační systémy a jejich určující kritéria. Vyhláška je stanovená podle zákona o kybernetické bezpečnosti. Změna vyhlášky 205/2016 Sb., nově vyhláška 360/2020 Sb., s účinností od roku 2021. Významný informační systém je systém, jehož správcem je orgán veřejné moci (např. státní orgán, kraj nebo hlavní město Praha). Toto znění vyhlášky určuje kritéria, které informační systémy spadají do významných informačních systému. Spadají zde elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci, kontrolní nebo inspekční činnosti anebo státního dozoru, výkonu veřejné moci při přípravě na krizové situace a jejich řešení, výkonu spisové služby, vedení úřední desky způsobem umožňujícím dálkový přístup, mezinárodní spolupráce, nebo zadávání veřejných zakázek. (Vyhláška č. 317/2014 Sb. o významných informačních systémech)

„*Tento systém se používá při výkonu veřejné moci a může sloužit například k elektronické poště, kontrolní nebo inspekční činnosti, řešení krizových situací, vedení úřední desky nebo zadávání veřejných zakázek. Informační systém je považován za významný, pokud narušení jeho bezpečnosti by mohlo způsobit omezení poskytování služeb nebo informací orgánem veřejné moci veřejnosti. Omezení hospodaření orgánu veřejné moci. Jiné omezení fungování orgánu veřejné moci. Zásah do osobního života nebo práv fyzických nebo právnických osob postihující nejméně 50 000 osob. Ohrožení veřejného zájmu, které nelze odvrátit bez nepřiměřených nákladů*.“ (Vyhláška č. 317/2014 Sb. o významných informačních systémech)

Vybrané významné systémy obsažené ve vyhlášce č. 317/2014 Sb. Vyhláška stanovuje 153 významných informačních systému, tyto systémy spadají pod stát, nebo kraje.

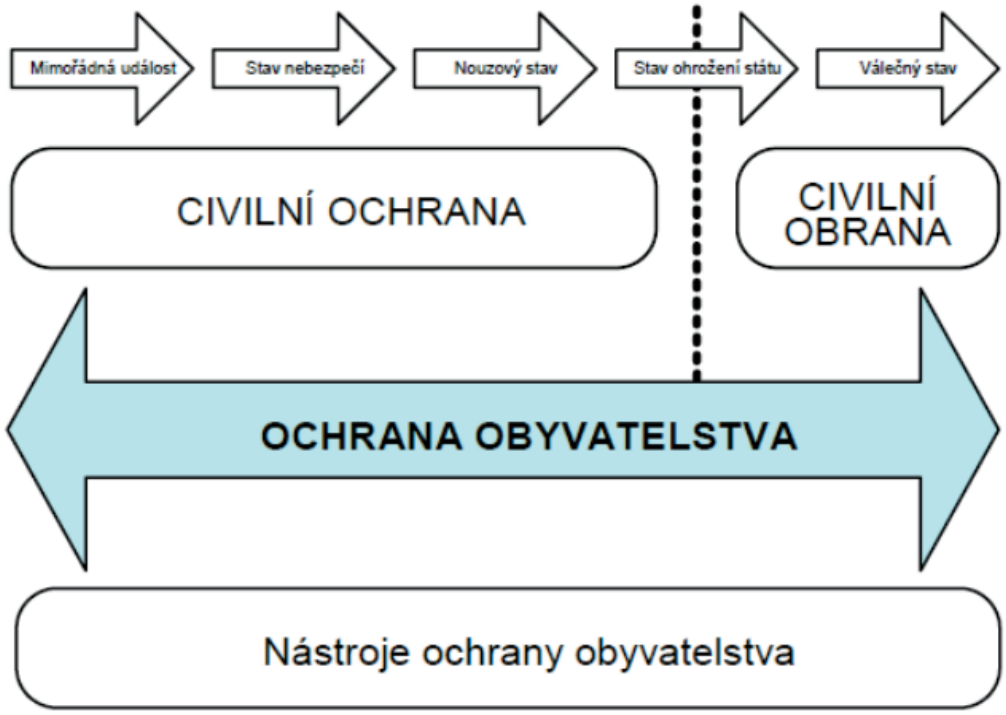
1. Webové stránky kraje.
2. Elektronický poštovní systém kraje.
3. Ekonomický systém a spisová služba kraje.

4. Centrální registr pojišťoven.
5. Vězeňský informační systém.
6. Informační systém majetku státu.
7. Informační systém úřadu pro ochranu osobních údajů.
8. Registr léčivých přípravku s omezením.
9. Registr externích adres pro úřad jaderné bezpečnosti.
10. Krizkom.
11. Agris.
12. Kontrolní informační systém pro kontrolní úřad.
13. Centrální evidence stíhaných osob.

Informační systémy jsou nepostradatelné pro fungování krajů a státu. Narušením významných systému, jako je například Krizkom nebo Agris by mohl v případě mimořádných události významným způsobem narušit fungování celého státu. Účelem systému Krizkom je koordinace a podpora procesů při řešení požadavků na věcné zdroje za krizových stavů. (SSHR Czech Repulic, 2024)

2 OCHRANA OBYVATELSTVA

Ochrana obyvatelstva vznikala již historicky v dávných dobách, kdy se lidé potřebovali ukrývat před nepřáteli. Nejvýznamnějším milníkem ochrany obyvatelstva byla druhá světová válka. Ačkoliv se historicky mluvilo o branné výchově, vycházející z myšlenek doktora Tyrše v 19. století, myšlenka se aplikovala až s příchodem druhé světové války, kdy byl přijat zákon o branné výchově. Ochrana obyvatelstva v té době jako civilní protiletecká ochrana, protože se během druhé světové války využívalo bombardování, proto byly zřizovány úkryty pro civilní obyvatelstvo, nebo improvizované ukrytí ve sklepech nebo jiných staveních. V polovině 20. století se název přetransformoval do Civilní obrany, myšlenka branné výchovy zůstala. Po roce 1993 se název změnil na civilní ochranu a s příchodem nového století a vznik nových zákonů se název změnil na Ochranu obyvatelstva. Vztah mezi civilní ochranou a obranou vysvětluje ministerstvo vnitra v schématu. (Dvořák, 1999)



Obrázek 1 Ochrana obyvatelstva, MV GŘ HZS, 2016.

Ochrana obyvatelstva obsahuje všechny stavy a mimořádné událostí, civilní ochrana je pro stavy, kdy nejsou ohrožené základní demokratické principy státu. V momentě, kdy stát přejde do stavu ohrožení, nebo do válečného stavu začíná civilní obrana. (Ministerstvo vnitra – generální ředitelství Hasičského záchranného sboru, 2015)

Ochrana obyvatelstva je důležitou součástí každodenních životů civilistů, je potřeba je chránit před mimořádnými událostmi a krizovými situacemi různého charakteru, za cíl si primárně klade ochranu životů, zdraví, majetku a životního prostředí. Podle zákona o integrovaném záchranném systému je definice „*plnění úkolů civilní ochrany, zejména varování, evakuace, ukrytí a nouzové přežití obyvatelstva a další opatření k zabezpečení ochrany jeho života, zdraví a majetku.*“

K ochraně obyvatelstva se váže několik základních pojmů, které jsou vymezené zákonem 239/2000 Sb. o integrovaném záchranném systému. Tento zákon definuje nejzákladnější pojmy, se kterými se v této oblasti setkáváme, jejich znalost je nezbytná k definování činností, které se k tématu vztahují. Zákon také stanovuje záchranné složky a jejich působnost, jejich další definice a úkoly jsou rozepsány v jednotlivých zákonech o vybraných složkách integrovaného záchranného systému. Zákon o integrovaném záchranném systému také upravuje práva a povinnosti právnických a fyzických osob při záchranných a likvidačních pracích. Tento zákon také definuje ochranu obyvatelstva, je proto jedním z nejdůležitějších legislativních dokumentů, které se k ochraně obyvatelstva váže. Na zákon o integrovaném záchranném systému, navazuje také krizový zákon, který definuje další pojmy spojené s ochranou obyvatelstva.

Mimořádná událost

„*Škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací.*“ Mimořádnou události je vše, co se vymyká z běžného života. Dopravní nehody, požáry, povodně, jsou události, které jsou nežádoucí, vyvolané podmínkami a ohrožují společnost, vymykají se z běžného stavu. (Zákon 239/2000 Sb. o integrovaném záchranném systému)

Mimořádnou událost můžeme dělit na naturogenní a antropogenní, tedy vzniklou přírodními vlivy, nebo vzniklé lidským chováním. Mimořádná událost může být krátkodobá, střednědobá nebo dlouhodobá, dělíme je také z hlediska místa na lokální, regionální, národní nebo nadnárodní.

Záchranné práce

„*Činnost k odvrácení nebo omezení bezprostředního působení rizik vzniklých mimořádnou událostí, zejména ve vztahu k ohrožení života, zdraví, majetku nebo životního prostředí, a vedoucí k přerušení jejich příčin*.“ Záchranné práce jsou práce, které zabraňují škodám, probíhají během mimořádné události. Například při dopravní nehodě hasičský záchrany sbor

bude provádět vyproštění osob z automobilů. Záchranné práce jsou na místě mimořádné události neodkladné, důležitou roli sehrává čas a správný postup záchranářů a bezodkladnost zraněným osobám poskytnout první předlékařskou pomoc. (Zákon 239/2000 Sb. o integrovaném záchranném systému)

Likvidační práce

„*Činnosti k odstranění následků způsobených mimořádnou událostí*." Likvidační práce se na místě události zahajují v jejím vzniku, oprávnění vykonávat likvidační práce mají především členové integrovaného záchranného systému. Náhrada za likvidační práce většinou přichází od státu, nebo místních úřadů. K ukončení dochází v momentě, kdy je situace stabilizována a dochází k obnovení běžného stavu. (Zákon 239/2000 Sb. o integrovaném záchranném systému)

Věcná pomoc

„*Poskytnutí věcných prostředků při provádění záchranných a likvidačních prací a při cvičení na výzvu velitele zásahu, hejtmana kraje nebo starosty obce; věcnou pomocí se rozumí i pomoc poskytnutá dobrovolně bez výzvy, ale se souhlasem nebo s vědomím velitele zásahu, hejtmana kraje nebo starosty obce*." Osoby mohou pomoci například při povodních tím, že nabídnou lopaty, pytle, a další prostředky. Pomoc by měla být kontrolována a regulována, aby se prostředky nehromadily. (Zákon 239/2000 Sb. o integrovaném záchranném systému)

Osobní pomoc

„*Činnost nebo služba při provádění záchranných a likvidačních prací a při cvičení na výzvu velitele zásahu, hejtmana kraje nebo starosty obce; osobní pomocí se rozumí i pomoc poskytnutá dobrovolně bez výzvy, ale se souhlasem nebo s vědomím velitele zásahu, hejtmana kraje nebo starosty obce*." Osobní pomoci při mimořádné události mohou přispět i občané, například při povodních se mohou podílet na pomoci plnění pytlů, pomoc slabším osobám s evakuací, podmínkou je, že tato pomoc musí být s vědomím pověřených osob, aby se z pomoci, nestala další zachraňovaná osoba. (Zákon 239/2000 Sb. o integrovaném záchranném systému)

Kritická infrastruktura

„*Prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení, jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. Prvkem kritické infrastruktury zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a*

odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury. Ochranou kritické infrastruktury opatření zaměřená na snížení rizika narušení funkce prvku kritické infrastruktury.“ Kritická infrastruktura je klíčová pro chod společnosti a ekonomiky. Její ochrana je důležitá, aby nenastala krizová situace. Evropská kritická infrastruktura (EKI) je infrastruktura, jejíž narušení by mělo závažný dopad na chod států EU. (Zákon 240/2000Sb. o krizovém řízení)

Varování a vyrozumění

Varování probíhá předáním signálu, který probíhá na elektronických koncových prvcích, nebo prostřednictvím sirén. V České republice jsou tři zvukové signály. „*Akustická zkouška provozuschopnosti jednotného systému varování a vyrozumění. Ve 12:00 se sirény rozezní zkušebním nepřerušovaným tónem po dobu 140 sekund. Elektronické koncové prvky upozorní občany před začátkem zkoušky hlasově. „Všeobecná výstraha“. Tento signál je vyhlašován kolísavým tónem sirény po dobu 140 vteřin a může zaznít třikrát po sobě v cca tříminutových intervalech. Po tomto signálu následuje mluvená varovná informace, kterou se sdělují obyvatelstvu prvotní údaje o charakteru hrozícího nebezpečí. „Požární poplach“, který slouží ke svolání jednotek požární ochrany. Tento signál je vyhlašován přerušovaným tónem sirény po dobu 1 minuty.*“ V případě mimořádné události jsou tyto signály nepostradatelné, jedná se o rychlou informaci pro občany, že se něco děje. Každý občan by měl proto signály znát a vědět, kdy se jedná o mimořádnou událost a měl by vyhledat úkryt. Vyrozumění jsou krátké, podstatné informace doprovázející varování. Informace k mimořádné události občané mohou najít v televizním vysílání, ve vysílaní rádia, nebo na webových stránkách měst a obcí, nebo na stránkách, které jsou vytvořeny pro předávání informací mimořádných a krizových situací. (Hasičský záchranný sbor, 2024)

Předávání informací občanům pomocí webových stránek

Pro zjišťování informací veřejností, mohou sloužit webové stránky jako je Záchranný kruh, Hasičský záchranný sbor, Portál krizového řízení, které jsou uzpůsobeny k předávaní informací občanům. Občané naleznou informace také na stránkách obcí a měst, většinou v jejich informačních systémech. Aplikace Záchranka předává informace o první pomoci, pokud se občan ocitne v tíživé situaci. Aplikace i webové stránky jsou vždy uzpůsobený k rychlým instrukcím s krátkými informacemi, aby v případě mimořádných události byly pro občany stručné a věcné.

3 INFORMAČNÍ BEZPEČNOST

V informační bezpečnosti v ochraně obyvatelstva se objevuje několik definic této problematiky. Nejčastěji narazíme na definici informační bezpečnosti, která má poměrně menší počet definic oproti kybernetické bezpečnosti, tyto definice se v posledních několika letech neměnily. Požár se zabývá informační bezpečností, kde definuje „*informační bezpečnost vyžaduje celou řadu organizačních opatření různých technik, přístupů a nových metod, protože informace a data je potřeba chránit před neúmyslným narušením. Informační bezpečnost je disciplína, která se rychle rozvíjí, vznikají nové programy v oblasti ochrany dat, ale i stále nové metody a programy, které vytvářejí útočníci.*“ (Požár, 2005)

Další z definic využívá Doucek, který se zaobírá tématem ve vztahu k řízení bezpečnosti. Doucek ve své knize vychází z myšlenek Požára, tyto myšlenky rozvíjí a zahrnuje do současnějšího pojetí. Z Požára vycházejí i další autoři, ačkoliv jeho kniha Informační bezpečnost je z roku 2005. Pojem kybernetická bezpečnost působí mladším dojmem, pojem prochází víceletým zkoumáním autorů a publikováním nových definic. Mohlo by se zdát, že se staví prioritněji než informační bezpečnost. Doucek ve svých definicích také využívá jako zdroj normu ISO 27000. Informační bezpečnost definuje jako „*ochrana důvěrnosti, integrity a dostupnosti informací. Může zahrnovat také vlastnosti odpovědnosti, autenticitu, spolehlivosti, nepopíratelnosti*“

Po prozkoumání definic a pojmů z informační bezpečnosti zjistíme, že tento pojem je na první dojem nadřazen kybernetické bezpečnosti, která je subjektem v informační bezpečnosti. Informační bezpečnost tedy v sobě zahrnuje kybernetickou bezpečnost a oba tyto pojmy sehrávají důležitou roli, pojmy se bezpochyby vztahují k ochraně obyvatelstva, ale neobjevují se ve znalosti osob, které pracují s informacemi.

Zákon o kybernetické bezpečnosti na první pohled vypadá, že lze podle něj přistupovat k problematice, i když je tento zákon důležitou součástí bezpečnosti, prakticky v této oblasti nezahrnuje podstatné opatření ve vztahu informační a kybernetické bezpečnosti v ochraně obyvatelstva. „*Zákon o kybernetické bezpečnosti ani prováděcí vyhlášky k tomuto zákonu vlastní pojem kybernetické bezpečnosti nevymezují. To, co je v těchto právních předpisech vymezeno, však umožňuje pochopit základy a principy kybernetické bezpečnosti, jakož je i následně aplikovat*.“ (Kolouch, 2019) S touto problematikou se spojují dva nejdůležitější pojmy. Informace a data, jsou neodmyslitelnou součástí informační bezpečnosti, protože se jedná o aktiva, která má chránit. (Požár, 2005)

Kybernetická bezpečnost

Vláda České republiky uvádí definici kybernetické bezpečnosti jako: „*Celkovou ochranu sítí před kybernetickými útoky a hrozbami, tak aby byla zachována bezpečnost informací.“* (Česko, 2023) Kybernetická bezpečnost je důležitou součástí dotýkající se moderních technologií a jejich uživatelů.

„*Kybernetická bezpečnost představuje soubor opatření, která jsou přijata, aby byl ochráněn počítačový systém před neoprávněným přístupem či útokem.*“ (Kolouch, 2019) Kybernetická bezpečnost sehrává důležitou roli při ochraně dat a informací nacházejících se v kyberprostoru s minimalizovat tak jejich poškození a ztrátu.

„*Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.*“ (Jirásek, 2015) V dnešní době máme k dispozici moderní technologie, zařízení i postupy, které musíme zajišťovat a podílet se na bezpečnosti prostoru, ve kterém jsou důležitá data a informace uloženy.

„*Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou českou veřejnost.*“ (Národní strategie kybernetické bezpečnosti 2015-2020)

Zeman ve své definici z roku 2003 kybernetickou bezpečnost popisuje jako ochranu informačního systému před kybernetickými hrozbami. A bezpečnost jako ochranu před rizikem, hrozbou a nebezpečím. (Zeman, 2003)

Důležitou součástí Evropské kybernetické bezpečnosti je European Union Agency for Cybersecurity. „*Agentura ENISA přispívá ke kybernetické politice EU, zvyšuje důvěryhodnost produktů, služeb a procesů IKT pomocí systémů certifikace kybernetické bezpečnosti, spolupracuje s členskými státy a orgány EU a pomáhá Evropě připravit se na kybernetické výzvy.*“ (ENISA, 2024)

Z již ustálených definic lze kybernetickou bezpečnost definovat jako opatření, nebo souhrn úkolů, které mají zajistit bezpečnost, ochranu systému před různými útoky. Kolouch navíc dodává, že se do kyberprostoru nepočítají jen útoky, které přicházejí z kyberprostoru, ale i neoprávněný přístup osob do systému. Strategie pro kybernetickou bezpečnost definuje, že tato ochrana se musí vztahovat na sektory veřejné i soukromé, aby bezpečnost byla poskytnuta všem občanům. (Národní strategie pro kybernetickou bezpečnost, 2020)

Informační bezpečnost

V problematice bezpečnosti se většinou skloňuje a využívá pojem kybernetická bezpečnost. Informační bezpečnost se skrývá spíše v pozadí a tím je i méně známá pro veřejnost. Informační bezpečnost jako taková by se dala považovat za nadřazený pojem. Tyto dvě definice se prolínají, ale dalo by se říct, že kybernetická bezpečnost je součástí té informační. Informační bezpečnost má za úkol chránit aktiva, tedy i data uložená v kyberprostoru. Data a informace musejí být chráněna od svého vzniku, po celou dobu jejich životnosti až po jejich likvidaci. (Požár, 2005)

Informační bezpečností se také zaobírá Doucek, který pracuje s informacemi ve vztahu k jejich řízení. Proces řízení rizik, který zahrnuje identifikaci informací, hrozeb, vyhodnocení rizik a implementaci opatření k minimalizaci těchto rizik ve vztahu s bezpečností informací. (Doucek, 2019)

Požár se zabývá informační bezpečnosti ve své knize Vybrané aspekty informační bezpečnosti. Tato kniha zpracovává přehledně problematiku a uchopení informační bezpečnosti a její výstižné definice. Definice i problematika jsou aktuální a uchopení pojmů je totožné i dnes. Požár definuje pro informační bezpečnost nejdůležitější prvky, kterými jsou důvěrnost, integrita, dostupnost. (Požár, 2005)

„*Informační bezpečnost a její realizace mají za úkol zejména ochránit důvěrnost, dostupnost, integritu informací. Kybernetická bezpečnost se zaměřuje především na řešení kybernetických incidentů spíš než na pouhou ochranu důvěrnosti, dostupnosti a integrity*.“ (Doucek, 2019)

Andress se zabývá ochranou dat, především klade důraz na šifrování, zálohování, přístupová opatření a fyzickou ochranou. Zdůrazňuje tato pravidla, jak správně manipulovat s daty, aby nedošlo k jejich poškození nebo úniku. Poskytuje tak znalosti, jak efektivně chránit informace před případnými ztráty. (Andress, 2014)

Doucek i Kolouch stavějí do popředí teorii rozdělení dat, které musí zachovávat důvěrnost, integritu a dostupnost a tyto tři prvky nesmí být žádným způsobem porušeny. Tuto teorii ve své knize popisuje také Požár. Doucek ve své knize analyzuje normy a zákony potřebné k ochraně dat a systému, popisuje, jak správně instalovat a chránit informační systémy. Pracuje s informační bezpečnosti, daty a informacemi v systému a zabývá se teorii zaměřenou na praxi, zatímco Kolouch se zabývá pouze definováním pojmů. (Kolouch, 2019)

Data

„*Data jsou jakékoli prvky s informační hodnotou, které jsou zpracovávány počítačovým systémem, přičemž jsou zpracovávány tak, aby následně utvořila informaci.*“ (Kolouch, 2019) Podle této definice můžeme říct, že data mohou být čísla, nebo znaky, díky nímž sestavíme ucelené informace.

„*Jakékoli vyjádření faktů, informací nebo pojmů ve formě vhodné pro zpracování v počítačovém systému, včetně programu způsobilého zapříčinit provedení funkce počítačovým systémem.*“ (Ministerstvo zahraničních věcí, 2013)

„*Data, fakta, čísla, události, grafy, mapy. Data jsou základním materiálem, surovinou informace. Tato data získáváme čtením, pozorováním, výpočtem, měřením, vážením, kreslením. Jedná se o vyjádření skutečností a myšlenek. Jsou vhodné vyjádřené zprávy, které vypovídají o světě. Jako lidský produkt opět určeno lidem*.“ (Požár, 2005)

Informace

Informace pro mnohé firmy, organizace i pro organizace IZS, znamenají podstatné aktivum, které musí zabezpečit. Informace jsou pro organizace zásadní, při jejich ztrátě firmy mohou přijít o konkurenční výhodu, nebo to může znamenat vyzrazení Know-how. (Doucek, 2008)

„*Informace jsou tedy vnímány jako něco „kvalifikovanějšího“, nežli data. Data jsou fakta, která se stávají informacemi tehdy, pokud jsou vnímána či vyjádřena v kontextu a nesou význam, který je pochopitelný pro lidi.*“ (Kolouch, 2019)

„*Informace je název pro obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním.*“ (Weiner, 1960)

„*Každé energetické sdělení, které může mít smysl buď pro toho, kdo je činí, nebo pro toho, kdo je přijímá.*“ (Smejkal, 2022) Po porovnání těchto dvou definic, ze kterých také vychází Kolouch, můžeme vidět proces změny definování informací v minulém století. V dnešní době informaci vnímáme spojenou s digitálním prostředí a moderními technologiemi.

„*Hmota, vědomí, myšlení, poznání, pohyb, čas. Informace je poznatek, který se týká objektů, faktů, události, nebo myšlenek. Pojmy informace a data se v praxi často zaměňují. Pro efektivní řízení jakékoliv činnosti je potřeba, aby obsah informace byl objemný a nějak přínosný. Informace také musí být relevantní a včasná.*“ (Požár, 2005)

Informace jsou jedním z nejdůležitějších prvků pro organizace, firmy a stát. Bez informací a dat se žádná organizace neobejde. Podle profesora R.M. Staira z Florida State University jsou důležitým prvkem vědomosti, které řadí na pozici vedle informací a dat. Ostatní

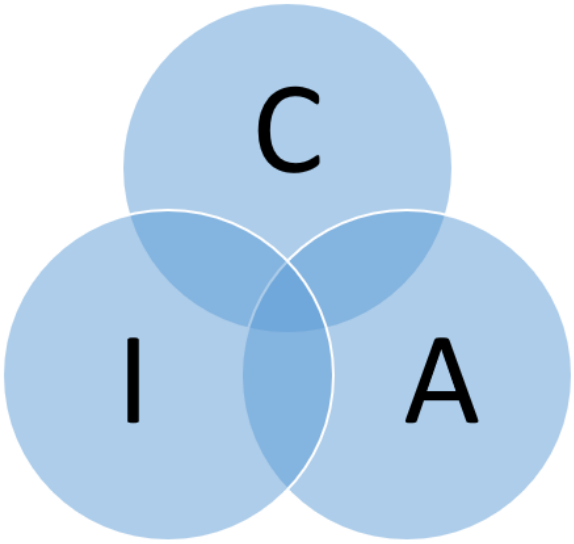
definice, které byly v práci uvedeny řadí vědomosti nebo postup výroby jako část informace, nikoliv jako samostatný pojem stojící na stejné úrovni. (Stair, 2012)

Triáda CIA

Tento pojem je přiřazován v souvislosti s pojmy data a informace. Tento pojem je zkratkou tří slov důvěrnost, integrita, dostupnost, anglický překlad Confidentiality, Integrity, Availability. Pojmy jsou spojovány s informacemi a se zaručením jejich bezpečnosti. Dodržením požadavku pro data, informace, informační systémy, dosáhneme požadovaného zabezpečení. (Kolouch, 2019)

Zaručení důvěrnosti znamená, že data a informace budou v rukou těch, kteří jsou oprávnění s těmito informacemi pracovat. Důvěrnost informací se dále zabývá i norma ISO/IEC 27000. Klasifikace informací nalezneme v zákonu 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti. Vyhláška o kybernetické bezpečnosti 82/2018 se zabývá hodnocením důvěrnosti jako Traffic Light Protocol. (Kolouch, 2019)

Doucek se zabývá definicemi podle normy ISO 27000, kde definuje „*důvěrnost jako vlastnost, že informace není dostupná, tomu, kdo nemá oprávnění. Integrita jako zajištění správnosti a úplnosti. Dostupnost jako přístupnost a použitelnost*.“



Obrázek 2 Triáda CIA, Kolouch, 2019.

Integrita dat a informací představuje jistotu zachování a ujištění, že nebylo s daty manipulováno nikým jiným než osobou, která má oprávněný přístup. Šulc definuje narušení integrity tak, že dojde k neoprávněnému přístupu k datům a informacím osobou, která tato oprávnění nemá. (Šulc, 2019)

Slovník kybernetické bezpečnosti definuje integritu jako „*jistota, že data nebyla změněna. Přeneseně označuje i platnost, konzistenci a přesnost dat, např. databází nebo systémů souborů. Bývá zajišťována kontrolními součty, hašovacími funkcemi, samoopravnými kódy, redundancí, žurnálováním atd. V kryptografii a v zabezpečení informací všeobecně integrita znamená platnost dat*.“ (Jirásek, 2015)

Dostupnost dat a informací klade nárok na dostupnost, kdykoliv je potřeba. „*O zničení (destruction) určitých informací se v informační bezpečnosti hovoří jako o narušení jejich dostupnosti (availability).*“ (Šulc, 2019)

Vyhláška o kybernetické bezpečnosti se zabývá hodnocením důvěrnosti, integrity i dostupnosti dat a informací. (Kolouch, 2019)

Obrázek 3 Parkenian hexad, Pender – Bey, 2016.

Henderson uvádí model Triádu CIA jako klíčový pro pochopení informační bezpečnosti. Ve svém modelu uvádí, že informační bezpečnost je složená z triády CIA, kdy je model sestaven jako trojúhelník a každá strana představuje jednu složku triády a celkově lze říci, že se jedná o informační bezpečnost. (Henderson, 2023)

Aktivum

Definice podle Koloucha pro aktivum je „*Vše, co má jakoukoliv hodnotu, pro jednotlivce, organizaci, nebo stát. Tato aktiva mohou být hmotného i nehmotného charakteru, tedy právě data a informace.*“ Aktivem může být cokoliv, co může osoba považovat za výhodu, může to být i drobný detail, který produkt na trhu práce vyniká před konkurencí, může to být Know-How firmy, nebo také dobré jméno, či vlastnost, které přináší konkurenční výhodu. Práce se zabývá aktivy vybraného subjektu. Tato aktiva budou v praktické části označená

právě jako data a informace, osobní a citlivé údaje, se kterými pracuje personální složka subjektu. Tyto údaje obsahují smlouvy, telefonní čísla a další členů, ale také informace o proběhlých výjezdech, ve kterých se objevují jména, adresy a telefonní čísla volajících. „*Hmotné i nehmotné statky, vše, co má pro majitele informačního systému jistou hodnotu. Peníze, majetek, data a informace, se považují za nejcennější aktiva*.“ (Požár, 2005)

„*Cokoliv, co má v organizaci nějakou cenu.*“ Definice podle ČSN ISO/IEC TR 13335. Doucek dělí aktiva na hmotná a nehmotná, tato definice se objevuje i u Koloucha a Požára. Mezi nehmotná aktiva jsou zařazeny pracovní postupy, data, programové vybavení, služby. (Doucek, 2019)

Zranitelnost

Na pojem aktivum, navazuje zranitelnost aktiva, jedná se o jeho slabé místo. Zranitelnost můžeme dělit na známou, takovou, kterou můžeme předvídat a lépe se připravit prevencí, a na neznámou, která ještě nebyla nikde zveřejněná a nemáme možnost se na ní připravit. Zranitelností může být chyba zařízení, ale i lidská chyba. (Kolouch, 2019)

Vyhláška o kybernetické bezpečnosti ve své příloze č.3 definuje zranitelnosti aktiv.

„*1. Nedostatečná údržba informačního a komunikačního systému,*

2. zastaralost informačního a komunikačního systému,

3. nedostatečná ochrana vnějšího perimetru,

4. nedostatečné bezpečnostní povědomí uživatelů a administrátorů,

5. nedostatečná údržba informačního a komunikačního systému,

6. nevhodné nastavení přístupových oprávnění,

7. nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

8. nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,

9. nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,

10. nedostatečná ochrana aktiv,

11. nevhodná bezpečnostní architektura,

12. nedostatečná míra nezávislé kontroly,

13. neschopnost včasného odhalení pochybení ze strany zaměstnanců.“ (Česko, 2018)

Požár definuje zranitelnost, jako místa v informačním systému, která vlivem prostředí mohou představovat významnou hrozbu. Doucek definuje zranitelnost jako „slabé místo

aktiva, nebo opatření, které může být využito hrozbou. Slabá místa mohou vést k neautorizovanému přístupu ke zdrojům systém. Definice je podobná Požáru, Doucek zde opět vychází z normy ISO 27000.

V informační bezpečnosti je velmi důležité zahrnutou taktické plánování pro ochranu dat a informací, tak aby se v jejich systému nenacházely žádné hrozby a zranitelnosti. Vytvořením plánu tak organizace preventivně zabrání možnému znehodnocení nebo úniku dat a informací. V případě zranitelností nebo hrozeb organizace může vytvořit strategický plán, který v případě poškození nebo odcizení dat, může aktivovat a minimalizovat škody. Po těchto událostech by měly organizace vytvořit report, který bude sloužit jako preventivní opatření, všechny zranitelnosti by měly být opraveny v co nejkratším časovém úseku. (Harold, 2007)

Hrozby

„*Jakýkoli fenomén, který má potenciální schopnost poškodit zájmy a hodnoty chráněné státem. Míra hrozby je dána velikostí možné škody a časovou vzdáleností (vyjádřenou obvykle pravděpodobností čili rizikem) možného uplatnění této hrozby.*“ (Ministerstvo vnitra, 2003) Podle této definice lze říci, že hrozba je negativní jev, který poškodí a naruší systém.

„*Skutečnost, událost, síla, nebo osoby, jejich působení může způsobit poškození, zničení, ztrátu důvěry a aktiv.*“ (Požár, 2005) Hrozba může mít charakter naturogení nebo antropogenní, záleží jen na zabezpečení organizace, či její zaměření, které hrozba může představovat větší riziko. V informační bezpečnosti mohou být hrozby obou původů, nejvíce se však připisuje právě antropogenní. Motivace této hrozby mohou být jakákoliv. Může se jednat o získání konkurenčních výhod, finanční zdroje, nebo se může také jednat o pomstu. (Požár, 2005)

Doucek ve své definici hrozby opět vychází z ISO 27000. „*Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.“* Ve svém rozdělení hrozeb nedělí jen na přírodní a lidské hrozby, přidává i hrozbu technologickou, které jsou poruchy nosičů dat a informací, poruchy sítí, nesprávná funkčnost. Lidské hrozby rozděluje na úmyslné a neúmyslné, uvádí, že více než 50 % je způsobeno neúmyslně.

V kybernetickém slovníku nalezneme definici hrozby jako „*potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace.*“ (Jirásek, 2015)

Jirovský uvádí 4 druhy hrozeb.

„*1) Únik informace je stav, kdy dojde k vyzrazení chráněné informace neautorizovanému subjektu.*

2) Narušení integrity představuje poškození, změnu, či vymazání dat.

3) Potlačení služby znamená úmyslné bránění v přístupu k informacím, aplikacím, či systému.

4) Nelegitimní použití je užití informací neautorizovaným subjektem či neoprávněným způsobem.“ (Jirovský, 2007)

Hrozba může být charakteristická podle různých kritérii, ať už se jedná o metody, dovednosti osoby, která se snaží hrozbu vytvořit, motivací, nebo dostupnými prostředky. Záleží zde také na atraktivnosti cíle. (USA Army, 2010)

Vyhláška o kybernetické bezpečnosti v příloze č.3 definuje hrozby. Vyhláška obsahuje obsáhlejší výčet hrozeb.

„*1. Porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,*

2. poškození nebo selhání technického anebo programového vybavení,

3. zneužití identity,

4. užívání programového vybavení v rozporu s licenčními podmínkami,

5. škodlivý kód (například viry, spyware, trojské koně),

6. narušení fyzické bezpečnosti,

7. přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,

8. zneužití nebo neoprávněná modifikace údajů,

9. ztráta, odcizení nebo poškození aktiva,

10. nedodržení smluvního závazku ze strany dodavatele,

11. pochybení ze strany zaměstnanců,

12. zneužití vnitřních prostředků, sabotáž,

13. dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,

14. nedostatek zaměstnanců s potřebnou odbornou úrovní,

15. cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,

16. zneužití vyměnitelných technických nosičů dat,

17. napadení elektronické komunikace (odposlech, modifikace).“ (Česko, 2018)

Informační systém

„*Jedná se o soubor lidí, technických prostředků a metod, zabezpečující sběr, přenos, uchování, zpracování dat za účelem tvorby a prezentace informací pro potřeby uživatelů*." (Doucek, 2019)

„*Systém komplexních prvků, nacházejících se ve vzájemné interakci."* (Bertalanffy,1956)

Docentka Tvrdíková z VŠB-TU Ostrava využívá ve své knize stejnou definici informačního systému jako Doucek. Informační systém definuje jako umělý, kdy člověk může výrazným způsobem ovlivňovat jeho kvalitu. „*Jedná se o obecně podpůrný systém pro systém řízení. Musíme znát cíle a požadavky na informační systém, abychom jej dokázali vytvořit podle našich potřeb.*" Tvrdíková informační systém skládá z několika komponentů, hardware, software, orgware, peopleware, reálný svět, který zahrnuje informační zdroje, normy a legislativu. „*Má-li být informační systém efektivní, nesmí být při jeho vývoji zanedbána žádná složka*."

Informační systémy se dynamicky vyvíjejí, je potřeba se zaměřovat na aktuální požadavky a hrozby, aby systémy byly vytvořeny v souladu s bezpečnostními požadavky. Díky nestálému a stále vyvíjejícímu se prostředí, by měly systémy procházet aktualizací. Na nové systémy klást bezpečnostní nároky již při jejich komplementaci. Profesor Basl klade důraz na vývoj a rozvoj informačních systému, aby ve změnách byly zahrnuty nové technologie, nové výrobky i nové služby. Při vývoji informačního systému je důležité plánování, dále zdroje, materiál a finance organizace. Při tvorbě systému je také potřeba využít „podnik" zaměření na konkurence schopnost. (Basl, 2012)

Tato část práce se zabývá pojmy z informační a kybernetické bezpečnosti, které zpracovávají teoretický vstup do dané problematiky.

4 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Informační bezpečnost je zásadním prvkem pro ochranu obyvatelstva. Je to oblast, která se zabývá ochranou dat a informací před neoprávněným přístupem, únikem, zneužitím nebo ztrátou. Právní normy v oblasti informační bezpečnosti jsou klíčové pro ochranu dat a informací. Tyto normy stanovují pravidla a postupy, které musí subjekty dodržovat, aby zajistily bezpečnost svých dat. Zákon o ochraně utajovaných informací1 chrání informace, jejichž zneužití by mohlo ohrozit zájmy nebo bezpečnost státu. Zákon o zpracování osobních údajů2 stanovuje pravidla pro zpracování a ochranu osobních údajů, což je klíčové pro ochranu soukromí jednotlivců. Zákon o kybernetické bezpečnosti3 pak upravuje práva a povinnosti v oblasti kybernetické bezpečnosti a zajišťuje bezpečnost sítí elektronických komunikací a informačních systémů. Tyto zákony společně vytvářejí rámec pro ochranu informací a dat v digitálním prostoru. Dodržování těchto zákonů a předpisů je nezbytné pro zajištění bezpečnosti informací. Znalost a dodržování pravidel informační bezpečnosti je klíčové pro ochranu obyvatelstva. Informace a data jsou často cílem osob páchající trestnou činnost, ať už se jedná o kybernetické útoky, krádeže identity nebo jiné formy zneužití. Ztráta dat a informací může mít vážné důsledky, ať už se jedná o finanční ztráty, narušení soukromí nebo dokonce ohrožení bezpečnosti obyvatelstva.

S rozvojem moderních technologií se zvyšuje i riziko spojené s bezpečností informací. Nové technologie přinášejí nové možnosti, ale také nové hrozby. Proto je důležité neustále sledovat vývoj v oblasti informační bezpečnosti a přizpůsobovat se mu. V subjektech ochrany obyvatelstva, jako jsou například veřejné správy nebo státní instituce, je zabezpečení informací na nejvyšších úrovních zásadní. Data a informace, které tyto subjekty spravují, jsou často citlivé a jejich ztráta nebo únik by mohl mít vážné důsledky.

V dnešní době je role informační bezpečnosti stále důležitější. To dokazují i nově vznikající právní normy, které se zabývají ochranou informací a dat, a to nejen v tradičním smyslu, ale i v kontextu kyberprostoru. Informační bezpečnost je tedy klíčová pro ochranu obyvatelstva a její význam bude v budoucnu pravděpodobně ještě narůstat.

II. PRAKTICKÁ ČÁST

5 POPIS VYBRANÉHO SUBJEKTU

Jedná se o subjekt Sboru dobrovolných hasičů nacházejících se ve Zlínském kraji. Umístění v práci nebude specifikováno z důvodu zachování přání subjektu zůstat v anonymitě. Sbor dobrovolných hasičů se nachází na území o rozloze 43 kilometrů čtverečních s přibližnou hodnotou počtu obyvatel 2400. Sbor využívá cisternovou automobilovou stříkačku s výbavou pro dopravní nehody, požáry, technické událostí, živelné události. Dopravní automobil pro technické pomoci, transport osob, výjezdy AED. Sbor disponuje technikou k zásahům u dopravních nehod, hydraulikou pro vyprošťováni osob z osobních automobilů, technikou pro hašení požáru, disponuje také pilami a AED. Hasičská zbrojnice má dvě patra a uzpůsobenou věž pro cvičení. Výjezdová jednotka má dvacet členů.

Tento subjekt plní úkoly podle zákona o Hasičském záchranném sboru 320/2015 Sb. „*ochrana životů, zdraví obyvatel, životního prostředí, zvířat a majetku před požáry a jinými mimořádnými událostmi. Podílí se na plnění úkolů požární ochrany, ochrany obyvatelstva, civilního nouzového plánování, integrovaného záchranného systému, krizového řízení a dalších úkolů.*“ (Zákon č. 320/2015 Sb., o hasičském záchranném sboru)

Tento subjekt je zařazen do příslušné kategorie JPO podle zákona o požární ochraně 133/1985 Sb. Podle tohoto zákona je také vykonávaná činnost subjektu, označení a plošné pokrytí. (Zákon č. 133/1985 Sb., o požární ochraně)

Subjekt také plní povinnosti ochrany obyvatelstva v „*plnění úkolů civilní ochrany, zejména varování, evakuace, ukrytí a nouzové přežití obyvatelstva a další opatření k zabezpečení ochrany jeho života, zdraví a majetku.“* Je zařazen do integrovaného záchranného systému, který se definuje jako „*koordinovaný postup jeho složek při přípravě na mimořádné události a při provádění záchranných a likvidačních prací*.“ (Zákon č.239/2000 Sb., o integrovaném záchranném systému)

Vybraný sbor dobrovolných hasičů se řídí zákonem o Krizovém řízení 240/2000 Sb. „*Tento zákon stanoví působnost a pravomoc státních orgánů a orgánů územních samosprávných celků a práva a povinnosti právnických a fyzických osob při přípravě na krizové situace, které nesouvisejí se zajišťováním obrany České republiky před vnějším napadením, a při jejich řešení a při ochraně kritické infrastruktury a odpovědnost za porušení těchto povinností.*“ (Zákon č. 240/2000 Sb., o krizovém řízení)

Sbor dobrovolných hasičů má zřízenou jednotku, která vyjíždí k mimořádným událostem, které podle zákona o IZS definujeme jako „*mimořádnou událostí škodlivé působení sil a jevů vyvolaných činností člověka, přírodními vlivy, a také havárie, které ohrožují život,*

zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací.“ (Zákon č. 239/2000 Sb., o integrovaném záchranném systému)

Vybraný subjekt se podílí nejčastěji na řešení mimořádných událostí spojených s požáry, povodněmi, záchranou osob pomocí AED, v této souvislosti se podílejí na záchranných a likvidačních pracích. Jeho náplní je také výchova ochrany obyvatelstva dětí.

6 INFORMAČNÍ BEZPEČNOST VYBRANÉHO SUBJEKTU

Modernizace vybavení sboru dobrovolných hasičů jde nezadržitelně kupředu. Jednotky musí být připraveny na hrozby, která pro ně mohou představovat významné riziko v narušení bezpečnosti. Modernizace jednotek se netýká jen jejich vybavení, ale také informačního systému, se kterým pracují, ten může přinášet rizika spojená s jeho využíváním. Sborům z hlediska informační bezpečnosti nejčastěji hrozí hrozby krádeže nebo ztrát informací a dat, k tomu může dojít neznalostí osob, na kterou může navazovat špatné provedení záloh. Využívání informačního systému se nedotýká všech sborů. Sbory si určují pravidla pro modernizaci podle sebe a podle dostupných dotací. (SDH Valašská Bystřice, 2023)

Další reakcí je zabezpečení budov, kde se informace nacházejí. Hlavním prvkem na zabezpečení jsou hesla, používají se při vstupu do zařízení, která se nacházejí na hasičské zbrojnici. V několika minulých letech se hasičské stanice staly atraktivním terčem pro zloděje, kteří ze stanic ukradli vybavení v hodnotě desítek tisíc. Lupiči se dokázali pohybovat po celé stanici, jejich primárním cílem bylo vybavení, ale měli přístup kdykoliv i k zařízením, která se na stanici nacházela. (Kořínek, 2023)

V zařízeních se nacházejí důležité informace, osobní a citlivé informace nejen členů výjezdové jednotky, ale také podrobné informace o výjezdu a průběhu zásahu. V případě krádeže těchto zařízení je neoprávněné osobě přístupný systém, protože neobsahuje hesla. Informace mohou být odcizeny nejen krádeží fyzicky, ale i pomocí hackingu. „*Vlastní prevence zmíněných negativních jevů musí nutně začít u koncových uživatelů, neboť v kyberprostoru jsou to právě oni, kdo je typickou první obětí útočníka.*“ (Kolouch, 2016)

6.1 Fyzická bezpečnost budovy

„*Na zabezpečení budovy má vliv lokace, její funkce a hodnoty, které jsou v budově umístěny. Uživatelé objektu ovlivňují také bezpečnost svým chováním. Je potřeba také pohlížet na pachatele, jaký mohou mít motiv, jeho chování a co bude v budově jeho cílem*.“ Fyzické zabezpečení budovy je důležité z hlediska bezpečnosti informací, především jako prevence před krádeží a zneužitím informací. (Tomek, 2018)

Primární bezpečnost hasičské zbrojnice je tvořen zabezpečeným vstupem do budovy. Tento vstup je vymezen pouze pro členy výjezdové jednotky a výbor daného sboru dobrovolných hasičů. Pokud se koná schůze, nebo akce, školení, je potřeba vstup povolit někým, kdo má přístup a pověření k odemčení zbrojnice. V době mimo výjezd, kdy se členové jednotky potřebují dostat na zbrojnici, slouží ke vstupu hlavní vchod. Dveře jsou uzamčené klasickým

zámkem, po jejich otevření se automaticky spouští alarm, který lze vypnout pouze čipem, který u sebe mají jen pověření členové. Při zamčení dochází k aktivaci alarmu pomocí čipu. Počty osob evidovaných u hasičských sborů je hodně, proto je velmi podstatným bezpečnostním prvkem vymezení řízeného přístupu pro osoby, které opravdu jsou spolehlivé a jejich vchod na zbrojnici je důležitý pro výjezd jednotky ve stanoveném čase. V případě výpadku elektrického proudu je alarm deaktivován, v tomto případě je vstup do budovy omezen na klasické zámky, stejně jako v případě čipu, přístup mají jen vybraní členové jednotky. Tento přístup nahradil klasické odemykaní zámku, které se stalo primárním zabezpečením především před zloději. Modernizace přinesla lepší bezpečnostní prostředky, ale s tím se posunul i o krok dopředu vývoj technik osob, které mohou usilovat o získání informací.

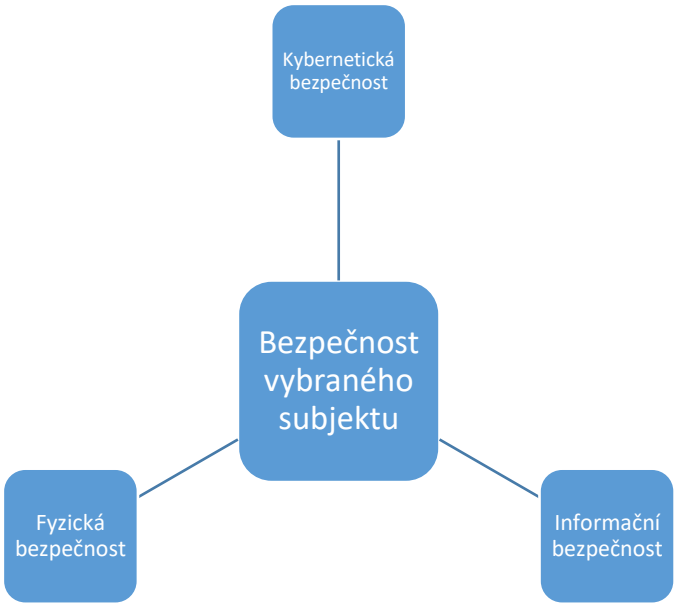
6.1.1 Zabezpečení v době výjezdu

V době vyhlášení výjezdu se nachází zařízení u vrat garáže. První hasič na zbrojnici alarm zruší čipovým zařízením, ještě před tím, než se dostane do garáže. Zařízení je umístěno u garážových vrat, kdy po přiložení čipu dochází k deaktivaci alarmu a automatickému otevření garážových vrat po zadání číselného kódu. Bezpečnostní opatření řízeného vstupu do hasičské zbrojnice je ochranou proti neoprávněnému vniknutí. Alarm zajišťuje bezpečnost před zloději, kteří by měli v úmyslu krást nejen fyzické vybavení, ale také informace. Budova je proto zajištěna proti neoprávněnému vniknutí. Omezený přístup zajišťuje pohyb osob, které jsou oprávněny pracovat s informacemi v systému sboru. Zabezpečit rychlý a bezpečný vstup do budovy při vyhlášení výjezdu je velmi důležité. V případě výjezdu je vyvíjen nátlak a časová tíseň, je potřeba zbrojnici zabezpečit i po odjezdu, aby nedošlo k zapomenutí uzamknutí budovy. V tomto případě zajišťuje kontrolu pověřená osoba po odjezdu vozidel.
Zabezpečení budovy v době výjezdu bylo sledováno ve vybraném subjektu při taktickém cvičení výjezdu k požáru firmy.

6.1.2 Bezpečnost vstupního zařízení

K narušení bezpečnosti může dojít při ztrátě, nebo odcizení klíčů. Čipové zařízení a klíče by neměly být pohromadě v jednom svazku. Tuto zásadu však lidé nedodržují, proto pokud ztratí klíče, nalezneme na nich i čipová zařízení, která se mohou dát zneužít ke vstupu. Ačkoliv čipy nelze tak jednoduše zfalšovat po fyzickém zřízení jako klíče, a je velmi malé riziko, že osoba, která nalezne svazek klíčů i s čipem ví, k čemu tyto zařízení mají přístup a

co odemykají, přesto nelze vyloučit hrozbu, že se zařízení dostane do rukou zkušené osoby se znalostmi, pokud by zařízení obsahovalo informace s přihlašovacími údaji, nebo údaji o síti, útočník by se mohl dostat touto cestou k neoprávněným datům. Na trhu se objevují zařízení, která kopírují signál čipových zařízení. V případě výjezdu by stačilo mít neoprávněné osobě zařízení Flipper Zero. Jedná se o malou krabičku, která kopíruje signál. Stačilo by krabičku umístit do blízkosti zařízení pro odemykání, při výjezdu osoba přiloží čip a krabička zaznamená signál. Dokáže tento signál uchovat. Neoprávněné osobě stačí krabičku následně vzít a signálem otevřít. (Mára, 2023)



Obrázek 4 Rozdělení bezpečnosti, subjekt – upraveno, 2024.

Data k vypracování rozdělení bezpečnosti vytvořené na základě informací poskytnutých subjektem.

6.1.3 Přehled bezpečnostních opatření budovy

Budova nemá mechanické prvky fyzické bezpečnosti, které by zahrnovaly plot, nebo turnikety. V přízemních oknech se nenachází mříže. Dveře jsou vyrobeny z materiálu, který je náročné prolomit a je vybaven bezpečnostními zámky. Bezpečnost budovy a s tím spojena bezpečnost informací, které se v ní nachází, je u vybraného subjektu zabezpečená. Moderní technologie umožňují rychlý vstup do budovy, její otevření i uzamčení v případě výjezdu. Alarm napojený na SMS správci hlásí vstup do budovy neoprávněné osobě a má možnost rychlého zásahu. V posledních letech se začaly objevovat případy vniknutí do budov hasičů.

Sbor na tyto případy reagoval pořízením kamerového systému v prostoru garáží a kanceláře, kamerový systém byl umístěn i na nejfrekventovanější vstupní místa.

1. Alarm.
2. Zamykání na klíč.
3. Zamykání na čipové zařízení.
4. Protipožární zařízení.
5. Protipožární dveře.
6. Bezpečnostní okna.
7. Světla na pohyb.
8. Zásuvky proti přepjetí.
9. Kamerový systém uvnitř i vně budovy.

Seznam bezpečnostních opatření budovy poskytnut subjektem.

6.2 Bezpečnost zařízení

Na hasičské zbrojnici se nacházejí zařízení, která jsou využívána k práci se systémem, který předává důležité informace a urychluje jejich předání v době výjezdu, zaznamenává také důležitá data a údaje. Informace a data jsou v subjektu primárně zpracovávaná v digitální podobě. Smlouvy jsou ukládány také v papírové podobě. Tato zařízení nejsou zvlášť uzamknuta ve speciálních skříních ani trezorech, mohou se proto stát předmětem trestné činnosti krádeže, po odcizení tak mohou být informace a data zneužity, nebo mohou uniknout do veřejného sektoru. Výjezdové mobily se nacházejí v menších výjezdových vozidlech a zastávají funkci tabletu.

Tabulka 1 Přehled zařízení v subjektu, subjekt – upraveno, 2023.

Přehled zařízení nacházejících se v subjektu		
Notebook	Tablet	Mobil
1x	2x	2x

6.2.1 Bezpečnost sdíleného notebooku

Na zbrojnici se nachází notebook. K tomuto zařízení má přístup výjezdová jednotka, která do něj zaznamenává směny. Systém nahradil papírový rozpis, který se nacházel na zbrojnici. Papírová verze nebyla zabezpečená ani chráněna před tím, aby mohla být data neoprávněnou osobou získána, či pozměňována. Systém rozpisu služeb je tvořen souborem v excelu, datumy, rozdělení směn a jak dlouho směna trvá, v případě výjezdu zaznamenané odpracované hodiny. V systému je veden každý člen výjezdové jednotky celým svým jménem. Jméno tak představuje citlivou informaci.

Jméno by se dalo v tomto případě nahradit osobním číslem, které by měl každý člen jednotky přidělen pro práci v systému. Pod tímto číslem by se přihlašoval do systému, systém by zaznamenával i provedené úpravy, v případě neoprávněného přístupu, nebo ztráty dat a informací špatnou manipulací, by se dalo blíže specifikovat, která osoba v té době byla přihlášena a prováděla úpravy.

Notebook je chráněn přístupovým heslem, které mají jen členové, kteří zapisují směny do systému. Heslo však nepodléhá správným bezpečnostním zásadám. Dlouhé, složité a bezpečné heslo se může zdát jako dobrou variantou na ochranu takto citlivých údajů, subjekt aplikuje heslo symbolické, kvůli velkému počtu osob s přístupem do systému a různé věkové kategorie a znalosti.

Do zařízení není zřízen ani přístup, které by jednotlivé osoby strukturovaně omezoval, kam se mohou dostat. Každá osoba by měla mít zřízen svůj vlastní přístup. Na tento problém jednotka nahlíží pohledem spíše lidskosti a jednoduchosti před složitostí. Přístupy nebyly zřízeny, protože se jedná o stálý dokument pro členy výjezdové jednotky, rizikem je přepsání omylem, nebo úmyslně údajů. V ohledu na množství osob různé věkové kategorie s různými technickými dovednostmi, se sbor pokouší ustupovat lidskosti vůči osobám. Starosta sboru pravidelně ukládání směn kontroluje, zda nedochází k záměrným přepisům. Členové v případě zaznamenaných neshod mohou ihned nahlásit neshodná data. Členové tento nepsaný kodex dodržují, v případě zaznamenaní problému bude sbor aplikovat bezpečnostní opatření v podobě složitých hesel a rozdělení přístupu.

Přehled hrozeb sdíleného notebooku

Subjekt byl o hrozbách informován. Některá rizika s tím spojená si uvědomuje, jiné nepředpokládá že vůbec nastanou. Po předání informací subjekt změnil heslo. Heslo je nyní silnější. Kybernetické hrozby se vztahují k připojení zařízení do sítě, kdy může nastat při vyhledávání stažení škodlivého souboru. V případě tohoto zařízení je největší hrozbou manipulace s daty.

1. Neoprávněný přístup.
2. Odcizení dat.
3. Neúmyslné přepsání dokumentu.
4. Úmyslné přepsání dokumentu.
5. Neuložení dokumentu.
6. Neprovedení aktualizace.
7. Nepravidelné zálohování, nebo záloha není provedena vůbec.
8. Krádež zařízení.
9. Připojení zařízení do sítě.

Přehled zabezpečení sdíleného notebooku

Na základě informací, které byly zpracovány v přehledu hrozeb, subjekt reagoval na možnost vzniku rizik informační bezpečnosti a provedl zabezpečení, která mu byla doporučená. Notebook byl umístěn do uzamykatelné místnosti, nyní se na něm nachází silné heslo. Strukturovaný přístup, ani uzamknutí dokumentu nebylo i po doporučení zřízeno. Dokument kontroluje každý týden velitel, pravidelně provádí aktualizaci dokumentů a zálohování na externí softwarové uložiště. Byla provedena kontrola Firewallu se zodpovědnou osobou za systém, a instalován antivirus.

Tabulka 2 Zabezpečení doporučená a provedená, subjekt – upraveno, 2024.

Doporučení zabezpečení	Provedené zabezpečení
Umístění do uzamykatelné místnosti.	ANO
Silné heslo.	ANO
Strukturovaný přístup.	NE
Uzamknout dokument heslem.	NE
Pravidelná aktualizace.	ANO
Provedení zálohování.	ANO
Zvýšená kontrola zápisu dokumentace.	ANO
Zabezpečení sítě.	ANO
Pravidelná antivirová kontrola.	ANO

Tabulka vychází ze zabezpečení subjektu, kde byly navržená opatření. Na pravé straně tabulky je uvedeno, zda subjekt opatření implementoval.

6.2.2 Bezpečnost výjezdových tabletů a mobilů

Dalšími zařízeními jsou tablety, které se nacházejí ve vozidlech. Těchto zařízení je více, v případě menších vozidel je nahrazují mobilní zařízení, určená pouze jako náhrada tabletů pro posádku vozidel. Jedná se o vozidlo DEA, kde by byl tablet nepraktický pro svou velikost. Tablet je určen především pro velitele zásahu, který vyjíždí ve vozidle cisternové automobilové stříkačky. Mobilní zařízení využívají ve vozidlech také strojníci, kteří jsou navigování na místo události. Tato zařízení nejsou chráněna z důvodu rychlé manipulace při výjezdu. Nacházejí se připravená ve vozidlech, čímž se v případě vniknutí na stanici neoprávněnou osobou, mohou stát předmětem trestné činnosti.

Obrázek 5 Aplikace výjezd, Fireport, 2023.

Přehled hrozeb výjezdového tabletu

Tablet není připojen do sítě, využívá datové připojení operátora. Tablet musí fungovat i na místech, kde internetové připojené není zřízeno, proto je potřeba jej zabezpečit touto cestou. Datové připojení není od operátora nijak limitováno z důvodu větší spotřeby dat v případě výjezdu. Na tomto zařízení nesmí být provedené akce, jako je stahování, nebo otevírání nebezpečných souborů z neověřených stránek, smí provádět jen povolené akce v aplikaci, popřípadě vyhledávat informace. Otevřením neověřených nebo nezabezpečených stránek může dojít k infikování zařízení škodlivým programem. Tablet je zabezpečen antivirovou ochranou. Velitel při manipulaci se zařízením dodržuje bezpečnostní pravidla, která má subjekt nastaven. Tablet nemá nastavené zabezpečení, díky čemuž se může stát snadným cílem při odcizení. Aplikace Fireport je pravidelně aktualizována, čímž se zabraňuje vzniku chyb, které by zařízení mohly ohrozit.

1. Krádež zařízení.
2. Získaní dat a informací ze zásahu.
3. Zneužití informací.
4. Zranitelnost aplikací.

Přehled zabezpečení výjezdového tabletu

Subjekt neaktivoval hesla na zařízeních. Zařízení musí být ihned schopná reagovat. V případě výjezdu hraje důležitou roli psychologie, rychlost a stres. V případě dlouhého hesla může velitel zapomenout pod nátlakem heslo. Velitelé se střídají, a v případě krátkého hesla se může stát, že některý z nich přesto zapomene. Subjekt nad biometrickými údaji

uvažuje, avšak zařízení, která mají nyní k dispozici funkce jako otisk prstů, nebo sken obličeje nepodporují. Uzamčením zařízení do skříní na klíč, nebo na čip subjekt zvažoval. Zatím se na zbrojnici nacházejí jen klasické uzamykatelné skříně, kdy při výjezdu pod tlakem není čas zařízení odemykat ze skříně. Pro instalaci nové skříně na čip, která by se nacházela v blízkosti auta sbor nedisponuje financemi.

V zařízení se všechna data a informace ukládají především do aplikací, které jsou využívány při výjezdu jako primární zdroj informací, navigování a pro zápis zprávy. Zařízení podléhá pravidelným kontrolám, zda je v pořádku fyzicky, ale také antivirovou kontrolou po stránce softwarové. Pravidelná aktualizace byla nastavená z ruční na automatickou, aby se pravidelně aktualizovaly aplikace. První den v měsíci dubnu byla provedená velká aktualizace a následně technologický test zařízení.

Tabulka 3 Zabezpečení doporučená a provedená tablet, subjekt – upraveno, 2024.

Doporučené zabezpečení	Provedené zabezpečení
Heslo.	NE
Nastavení biometrických údajů.	NE
Uzavření do uzamykatelné skříně.	NE
Pravidelná aktualizace.	ANO
Pravidelná antivirová kontrola.	ANO

Tabulka vychází z pozorování bezpečnosti u zařízení subjektu. V levé části tabulky doporučení, v pravé, zda subjekt implementoval návrh na bezpečnost.

6.2.3 Osobní mobilní zařízení jednotky

Jedním z největších rizik představují zařízení, která se nacházejí v určité době na stanici a mohou i stanici opouštět. Jedná se o osobní mobilní telefony jednotky. Tato zařízení nejsou nijak kontrolována, bezpečnost stojí jen na jednotlivých osobách, jak svůj telefon mají zabezpečený, jaké využívají hesla, kam se přihlašují a zda využívají veřejné sítě, která představuje jeden z dnešních problémů napadání mobilních zařízení. V mobilních zařízeních mají členové aplikaci, která je napojená na informační systém. V této aplikaci se zobrazují směny, kdo se na směně nachází. V případě výjezdu aplikace upozorňuje na výjezd a pomocí propojení na SMS, dokáže i přečíst text, který hasiči přišel, takže má čas během převlékání

poslechnout, o jaký výjezd se bude jednat a nemusí si tyto informace číst, což by vedlo ke zdržení. Aplikace také umí měnit barvy, které si uživatel nastaví podle výjezdu. Barva na obrazovce tak uživatele upozorní, o jaký zásah se jedná ještě před tím, než začne předčítat text. Rychlé potvrzení výjezdu, či jeho odmítnutí předává veliteli předběžnou zprávu, kdo se dostaví a kdo je naopak mimo území, či nemůže dojet z jiných důvodů, aby nedocházelo k prodlení. Uživatel má také možnost nahlédnout do informací, kdo volal, jaká informace odešla, kde se nachází místo určení. Hasič tak má předběžnou informaci k tomu, na co se má připravit a co bude k zásahu potřebovat.

Mobilní zařízení představují širokou škálu hrozeb, které pokud nebudou hasiči znát, může ohrozit informace, které v tomto zařízení mají uložené a které se vztahují k výjezdům. O tomto problému si je velitel a správce vědom. Jedná se o osobu zabývající se informační bezpečnosti i v civilním životě. Podílí se na chodu informačního systému, na jeho udržování, kontrole a řešení problémů, v případě vzniku incidentu realizuje potřebná opatření. Subjekt využívá dvě osoby, které se podílí na obsluze systému. Tyto osoby mají odpovědné vzdělání i praxi v dané problematice.

Jedná se o předcházení hrozeb, které by se na daný subjekt jednotky mohly vztahovat z hlediska kybernetické a informační úrovně. Správce systému udržuje systém aktuální a bezpečný. V případě podezření, či nahlášení hrozby, které přichází z osobního zařízení členů, má přístup do této aplikace a v případě nutnosti dané zařízení doslova *odřízne* od systému, takže i kdyby bylo zařízení napadené, útočník ztratí možnost nahlížet do aplikace, či jí jiným způsobem zneužít. Správce jakýmkoliv způsobem může zasahovat do systému, udělovat přístupy, či přidávat, nebo ukončit členství v systému. Správce má vše zpřístupněno ze svého osobního mobilního telefonu, který podléhá přísným bezpečnostním kritériím, díky čemuž je hrozbě předcházeno.

Největší riziko, které představuje využívání osobních mobilních zařízení, je hrozba škodlivého programu v zařízení a po přihlášení do sítě hasičské zbrojnice, může program putovat po síti, nebo můžou být odcizeny citlivá data z aplikace. Otevřené Wifi sítě představují přenos a infiltrování nebezpečí do osobních zařízení. V tomto ohledu spočívá riziko nebezpečí pouze na uživateli a jeho znalostech, jak k bezpečnosti u svého osobního zařízení bude přistupovat.

Přehled hrozeb mobilního zařízení

Mobilní zařízení mohou představovat hned několik hrozeb díky tomu, že jsou zapojená do systému FIREPORT. Zařízení obsahují data a informace o výjezdech, která mohou uniknout, nebo být zneužitá. Útok může být veden i záměrně pro konkurenční znevýhodnění sboru. Instituty zabývající se ochranou obyvatelstva mají slabší bezpečnost. Příkladem byly útoky na nemocnici. Hrozby vedené na osobní zařízení jsou spíše hrozby kybernetické.

1. Phishingové útoky na email.
2. DDoS útoky na systém.
3. Škodlivé programy, viry, trojský kůň, červ.
4. Odposlech informací.
5. Únik dat a informací.
6. Záměrné znevýhodnění konkurencí.
7. Ztráta financí z účtu sboru.
8. Přenesení hrozeb do sítě.

Přehled zabezpečení osobních zařízení

Členové výjezdové jednotky byli na zabezpečení svých osobních zařízení upozornění. Znalosti a dovednosti práce s moderními technologiemi se u jednotlivých osob liší, stejně tak mobilní zařízení, které využívají. Na základě rozdílných parametrů byly navrhnuty opatření, které by měla všechna zařízení obsahovat, avšak z hlediska technického se mohla opatření lišit v závislosti aktuálních verzí, výrobci a technických parametrů. Zabezpečení osobních zařízení bylo navrženo a u většiny osob implementováno na jejich osobní zařízení. Tato zabezpečení byla součástí školení, kterého se osoby zúčastnily. Na školení si osoby aplikovaly do svých osobních zařízení doporučená zabezpečení.

Tabulka 4 Zabezpečení doporučená a provedená mobil, subjekt – upraveno, 2024.

Doporučené zabezpečení	Provedení zabezpečení
Aktualizace software.	ANO
Silná hesla a biometrie.	ANO
Vypnutí funkcí automatického připojování.	ANO
Stahování z oficiálních zdrojů.	ANO
Znalost podvodných zpráv.	ANO
Funkce „Najdi telefon“.	ANO
Antivir.	ANO
Nepřipojení k veřejným sítím.	ANO
Zálohování dat.	ANO

Aplikováním doporučených zabezpečení mohou předcházet hrozbám, které by mohly ohrozit data a informace v informačním systému.

6.3 Aktiva vybraného subjektu

Aktiva jsou důležitou součástí vybraného subjektu. Aktiva dělíme na primární a podpůrná. (Doucek, 2019) Jako primární aktiva byly v subjektu označeny data a informace, bez přístupu k nim subjekt nemůže vykonávat plnění povinnosti v ochraně obyvatelstva. Ať už by se jednalo o znepřístupnění informací, které jsou potřebné k lokaci místa zásahu, nebo citlivé informace o členech sboru, informace o jejich odpracovaných hodinách a mzdě, nebo o bližších informacích z místa zásahu. Finanční prostředky a přístup k bankovním účtům je také primárním aktivem, protože bez financování by subjekt nemohl vykonávat svou práci. Podpůrná aktiva na podporu primárních aktiv je hardware, software, mobilní zařízení, díky kterým informační systém funguje v kyberprostoru. Subjekt disponuje s automobily a hasičským vybavením. Dokumentace k automobilům, zařízením, ale také ke smlouvám, dokumentace o financování a dotacích, nebo dokumentace zásahů.

Ztráta důvěrnosti dat může být narušená neoprávněným přístupem do systému subjektu s důsledkem úniku citlivých informací o zásahu, výjezdové skupině. Nedostupnost aktiv například v případě selhání informačního systému, odepření přístupu k důležitým datům.
Zranitelnosti v software a hardware, zastaralý software nebo nedostatečně zabezpečené mobilních zařízení, nebo jiných zařízení subjektu může představovat hrozbu útoku hackerů nebo malware, krádež zařízení. V případě, že se útočníci dostanou k informacím a datům, které obsahují finanční účty, nebo prostředky, může to znamenat omezení provozu, nebo neschopnost financovat aktivity. Chybějící nebo nedostatečná dokumentace k automobilům, zařízením nebo smlouvám, nebo zásahům znamená potíže při řízení a údržbě aktiv. Vybraná aktiva byla spojována s informační bezpečností.
Aktiva vychází z informací poskytnutých subjektem.

7 DOTAZNÍKOVÉ ŠETŘENÍ

Na základě dané problematiky práce, byl vypracován dotazník. Dotazník byl v daném subjektu předán fyzickou podobou. Pro porovnání byl dotazník vytvořen také v online podobě a rozeslán do okolních sboru dobrovolných hasičů pro porovnání výsledku s vybraným subjektem. Z vybraného subjektu se zúčastnilo 20 osob fyzické formy dotazníku, online dotazníku 15 osob z jiných sborů dobrovolných hasičů.

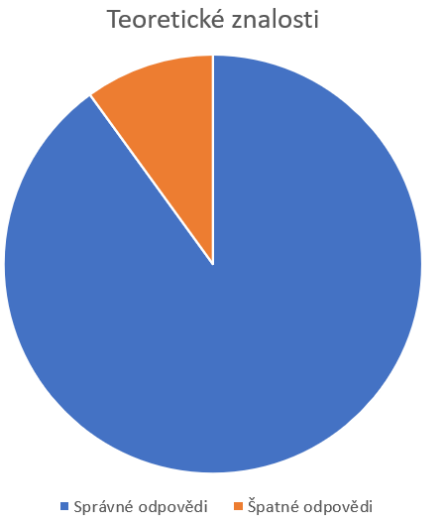
Dotazník se skládal ze 16 otázek na znalost z informační a kybernetické bezpečnosti z nichž 2 praktické otázky. Obsahoval také 5 doplňujících otázek, které se týkaly zájmu a téma školení. Dotazník si kladl za cíl ověřit znalosti a jejich úroveň v informační bezpečnosti. Výsledky dotazníkového šetření jsou zpracovány v grafickém zobrazení v této části práce. Grafy zpracovány na základě výsledků dotazníkového šetření. Zdrojem jsou informace poskytnuté subjektem.

Tato část práce obsahuje metodu srovnání. Primárně se zabývá kvantitativním výzkumem informační bezpečnosti v daném subjektu. Metoda srovnání se v této části zabývá pojetím problematiky, znalostí respondentů a názorů.

7.1 Otázky dotazníkového šetření

Otázky zaměřující se na znalost a definování nejčastějších pojmů: Spam, phishing, informační bezpečnost. Otázky byly pokládány, aby prověřily základní znalost subjektu. Jednalo se především o teoretickou znalost. Vyhodnocené odpovědi ukázaly, že znalost je na dobré úrovni a odpovídá 90 % správných odpovědí. Ve dvou případech byla zaznamenána chyba.

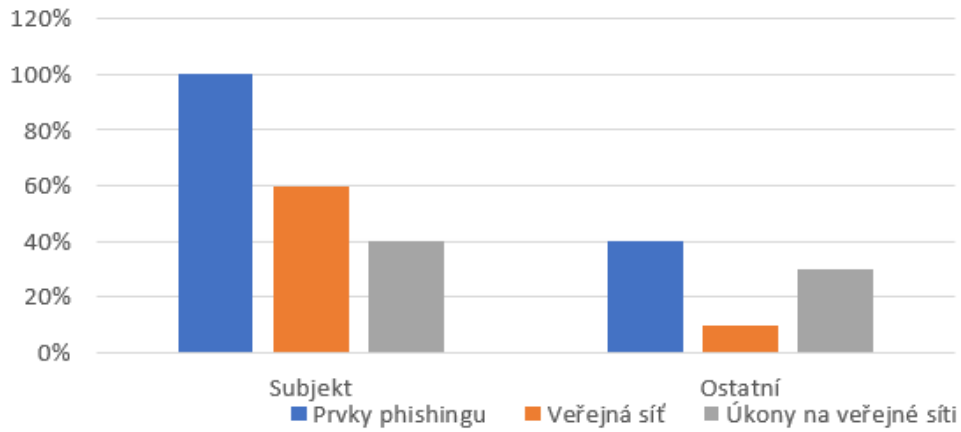
Osoby, které se zúčastnily dotazníkového šetření v rámci vybraného subjektu dokázaly pojmy svými slovy definovat, osoby dokázaly také vypsat varovné prvky, které se v phishingu objevují. V online dotazníku byly otázky vyplněny správně.



Obrázek 6 Graf teoretické znalosti, dotazníkové šetření, 2024.

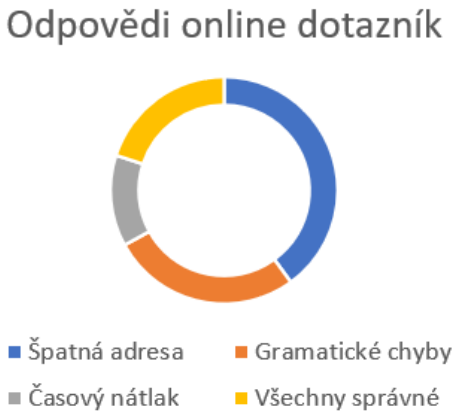
Dotazník obsahoval také praktické ukázky ze stránek Kybertest.cz. Úkolem subjektu bylo označit prvky emailové zprávy, ve které se nacházejí indicie, že se jedná o podvodnou zprávu. Druhým příkladem bylo vybrat ze tří veřejných sítí správnou síť, ke které by bylo možno se připojit. Doplňující otázkou bylo ověření, zda osoby vědí, co v případě připojení k veřejné síti, by neměli provádět za úkony. Cílem bylo zjistit, zda se povede aplikovat znalosti i v praktických otázkách.

Osoby z vybraného subjektu označily všechny viditelné prvky phishingu. Připojování k veřejným sítím se ukázalo jako problémové. V případě veřejných sítí se jednalo pouze o 60 % úspěšnost. Správné odpovědi na doplňující otázku obsahovalo 40 %. Grafické znázornění odpovědi praktické části, vlevo odpovědi vybraného subjektu, vpravo odpovědi z online dotazníku.



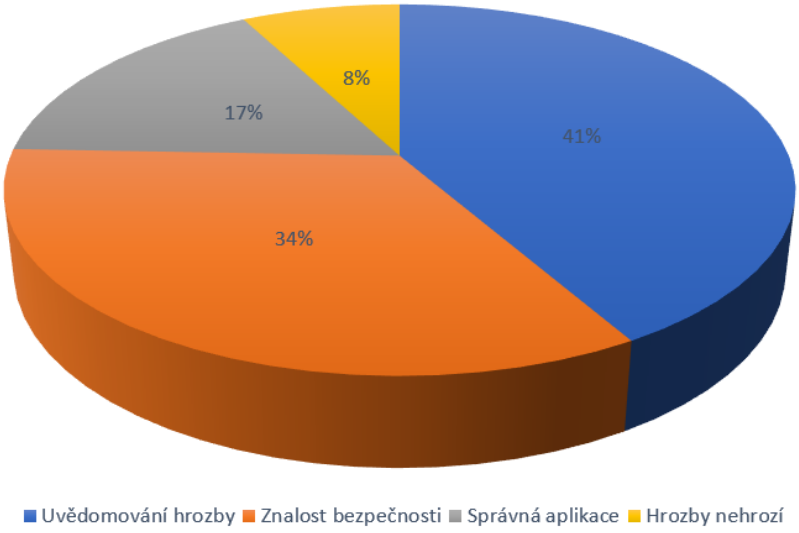
Obrázek 7 Graf praktické znalosti, dotazníkové šetření, 2024.

Subjekty v online dotazníku nedokázaly odhalit všechny prvky. Většinou se jednalo pouze o znalost jednoho prvku, který byl pro ně zásadní a který zaregistrovali jako první. 40 % odpovědí byla označená emailová adresa, 27 % gramatické chyby, 20 % označili vše, 13 % uvedlo časový nátlak. Osoby, které vyplnily otázky prokázaly, že by rozpoznaly podvodný email obsahující phishnig pouze ve 40 %. U otázky na veřejnou síť byly správné dvě odpovědi, ve čtyřech případech byla zaznamenána správná doplňující otázka. Ve třech odpovědích byla zaznamenána odpověď nepřipojování k žádné síti. Graf zobrazuje odpovědi na nalezení prvků phishingu u respondentů online dotazníku.



Obrázek 8 Graf porovnání praktické části, dotazníkové šetření, 2024.

Dalším typem otázek byly otázky týkající se samotné bezpečnosti subjektu. Hrozby, ztráta informací, zálohování dat. Cílem otázek bylo ověření povědomí a aplikované znalosti. Respondenti mají více povědomí o hrozbách dotýkajících se kybernetické bezpečnosti. Bezpečnost informací a její hrozby jsou mezi respondenty méně známe. Výsledky aplikace znalostí respondentů subjektu vidíme uvedené níže v procentech. Jednalo se o aplikaci teoretických znalostí na zabezpečení informací nacházejících se v objektu.



Obrázek 9 Graf aplikace znalostí do praxe, dotazníkové šetření, 2024.

V online dotazníku uvedlo 33 % osob hrozby, které mohou ohrozit SDH z nichž 12 % uvedlo primární důvod odcizení osobních a citlivých údajů. 20 % uvedlo že by se mohlo jednat o nebezpečí, blíže nebylo specifikováno, zbytek byla uvedená odpověď že se hrozby SDH netýkají. V jednom případě byly blíže specifikovány hrozby typu DDoS, malware, spyware a phishing. 47 % osob uvedlo správný způsob zálohování dat. Na otázky bezpečnosti informací osoby odpovídaly subjektivním hodnocením. Ve 27 % bylo uvedeno, že SDH není ohroženo žádnou hrozbou. Ve 13 % byla odpověď na bezpečnost dostačující. 13 % uvedlo, že SDH nejsou ohrožena odcizením údajů.

Poslední typ otázek byl zaměřen na školení. Cílem bylo zjistit zájem a téma školení. Vybraný subjekt projevil zájem o školení a vzdělávání v této oblasti. Upřednostnil spíše fyzickou formu školení před online. Tématem školení by měla být aktualizace, zálohování, zabezpečení dat a informací, ale také hrozby a prevence. Na základě tohoto podnětu se práce dále zabývala návrhem na školení.

Zpětnou vazbou na toto dotazníkové šetření, byla odpověď od sboru dobrovolných hasičů Hrachovec, kterému byl předán dotazník online formou, kdy jako odezvu kontaktoval

členku, která v této oblasti má teoretické i praktické znalosti, se má zabývat sestavením školení pro daný sbor na téma informační bezpečnosti. Tato informace byla předána na základě osobního sdělení. V 53 % byla odpověď na školení Ne. Z 47 %, kteří odpověděli ANO, uvedlo 27 %, upřednostnili fyzickou formu školení před online. Ve dvou případech byla zaznamenána odpověď na téma ochrana dat. Nejčastější odpovědí na otázku negativa školení, byli uvedena pracovní vytíženost.

7.2 Výsledek dotazníkového šetření

Dotazníkovým šetřením bylo zjištěno, že respondenti, kteří vyplňovali online dotazník neprokazují dostatečné znalosti v oboru informační a kybernetické bezpečnosti. Jejich teoretické znalosti se neshodují s aplikováním praktických znalostí. Na otázky bezpečnosti si mnozí neuvědomují rizika, nebo jejich prevenci zanedbávají. Online dotazník poukázal na velmi nízkou úroveň znalostí v této oblasti členů SDH. Respondenti neprokázali ani základní znalosti bezpečného chování, toto chování a neznalost mohou být budoucí hrozbou v modernizačních krocích pro SDH.

Vybraný subjekt prokázal základní znalosti aplikované do praxe. Respondenti si uvědomují hrozby, kterým může být SDH vystaveno. Tyto hrozby dokážou na nejnižší úrovni identifikovat. V subjektu se ukazuje potřeba spíše dovzdělávání se v hrozbách a uvědomění si propojení hrozeb a jejich přenos na sbory dobrovolných hasičů. O školení respondenti projevili také zájem, ve většině případu fyzickou podobou. Respondenti vypověděli, že u školení vidí problém časové náročnosti. U respondentů však převládá vědomí o nových výzvách moderní společnosti a hrozbách, které se jich mohou dotýkat, proto školení neodmítají.

Data do grafického znázornění byla použita z dotazníkového šetření. V této části práce byla využita metoda komparace pro porovnání výsledku sledovaného subjektu a u respondentů z ostatních sborů dobrovolných hasičů. Respondenti byli jednotlivci za sbory.

8 ŠKOLENÍ VE VYBRANÉM SUBJEKTU

Pokud lidé nebudou vzdělávání na odpovídající úrovni, nebudou nastaveny bezpečnostní pravidla, která budou dodržovat. Data jsou v dnešní době méně chráněny v kyberprostoru uložených na nosičích jako jsou telefony nebo tablety. (Awad, 2018) Na základě této myšlenky se vybraný subjekt podílel na experimentálním školení, které pro tuto práci bylo vytvořeno. Školení proběhlo jako návrh na opatření k zamezení významným ztrátám informací a dat především ze strany členů subjektu. Respondenti se školení zúčastnili po dvou měsících od vyplnění dotazníkového šetření. Školení se zúčastnilo pět osob z důvodu pracovní vytíženosti. Školení se skládalo z teoretické a praktické části. Teoretická část měla za cíl představit důležité pojmy informační bezpečnosti a ukázat důležitost bezpečnosti pro subjekt. Kromě základních pojmů, byly představeny a objasněny hrozby, které se subjektu mohou dotýkat v rámci informační bezpečnosti, především s rostoucí trestnou činností vloupání a krádeže na hasičské zbrojnice. V rámci školení proběhla prohlídka hasičské zbrojnice s návrhem na bezpečnostní opatření, která byla zaměřená na bezpečnost zařízení ve vozidlech.

V kapitolách teoretické a praktické části byla využita výzkumná technika školení. Školení bylo experimentální, bylo sestavené na základě bezpečnostních prvků subjektu, pracovalo s praktickými ukázky a zabývalo se dodatečně zabezpečením, které je potřeba do budoucna zahrnout. Opíralo se o subjekt konkrétní a praktická část byla přizpůsobená danému systému a práce s ním. Obsahovalo individuální bezpečnostní prvky zaměřené pro subjekt.

8.1 Návrh školení

Školení bylo navrhnuto pro daný subjekt. Teoretická část se skládala z pojmů, se kterými se respondenti dotazníkového šetření setkali dříve. Teoretická část se jen krátce zabývala právním rámcem, základní hodnoty legislativy byly přiblíženy jen na obecné úrovni. Praktická část měla za cíl ukázat prakticky, jak provádět základní zabezpečení informací, také se snažila o přiblížení hrozeb, které se subjektu dotýkají a jak tyto hrozby předvídat a v jejich případě, jak se zachovat a reagovat.

Teoretická část školení

Teoretická část zahrnovala vybrané pojmy. Tyto pojmy na školení byly vysvětleny, co znamenají a jaký je v nich rozdíl. Cílem teoretické části bylo přiblížení do problematiky, základní vysvětlení pojmů. Kromě pojmů také praktická ukázka, jak tyto úkony provádět k zabezpečení informací. Důraz byl kladen na uvědomování hrozeb, vytvoření představy

rizikového chování a jak preventivně předcházet hrozbám, a jaké mohou mít dopad v případě, že data a informace budou odcizeny a vyzrazeny.

1. Informační bezpečnost. Základní vstup do problematiky. Hrozby a preventivní opatření.
2. Kybernetická bezpečnost. Základní vstup do problematiky. Hrozby a preventivní opatření. Prevence zaměřená především na osobní zařízení.
3. Fyzická bezpečnost. Jaké prvky fyzické bezpečnosti existují a jak je tato bezpečnost důležitá pro ochranu dat. Seznámení s aktuální fyzickou bezpečnosti subjektu a možných budoucích opatření. Příklad zabezpečení jiných budov.
4. Šifrování. Jak šifrování funguje a proč je důležité jej používat pro ochranu dat.
5. Antivirový software. Různé typy antivirových programů, jak fungují. Ukázka, jak program používat.
6. Zálohování dat. Pravidelnost zálohování a aktualizace dat. Ukázka, jak data zálohovat na cloudové uložiště.

Teoretická část byla shrnuta ve vytvořené prezentaci, která sloužila jako primární podklad pro školení. Různé ukázky probíhaly i na vlastním zařízení.

Praktická část školení

Praktická část zahrnovala cvičení, které si respondenti vyzkoušeli na zlepšení svých dovedností. Respondenti si vyzkoušeli správné zabezpečení mobilních zařízení, kde v nastavení naleznou zabezpečení a jak postupovat v případě ztráty zařízení. Rychlý přehled zaměřený na bezpečné chování na internetu, který se zaměřoval především na technickou manipulaci s aplikací FIREPORT. Vytvářeli silná hesla, práce s generátory bezpečných hesel. Prováděli zálohování a aktualizace dat na externích uložištích. Hardwarové uložiště, jejich správná manipulace, také softwarové uložiště na cloudovém uložišti. Vyzkoušeli si také jak pracovat s antivirem, a jak funguje strukturovaný přístup do systému. Po absolvování praktické části školení, účastnici uměli lépe zvládnout bezpečnost informací a zaměřit se na předcházení hrozeb, které subjektu mohou hrozit. Tato část se ukázala přínosnější kvůli zábavnější formě, kdy si účastnici mohli prohlédnout a vyzkoušet úkony k provádění zabezpečení dat a informací. Praktická část má svůj základ v teoretické, bez teoretické části a znalosti pojmů a důležitých názvů a vysvětlení, by nemohla proběhnout. Praktická část staví na základních znalostech, které aplikovala přímo na vybrané zařízení subjektu.

8.2 Realizace školení

Školení bylo realizováno v prostorech subjektu. Subjekt disponuje prostory na zasedání a schůze, kde se koná pravidelně výbor. Jako podklad pro školení byla vytvořená prezentace, která byla promítaná spolu s praktickou ukázkou na vlastních zařízeních. Dotazníkové šetření bylo provedené jako první před dvěma měsíci, jeho cílem bylo posouzení znalostí, na které navazovalo vytvoření a následná realizace školení. Po realizaci školení se uskutečnilo znovu dotazníkové šetření, které respondenti vyplnili po školení. Subjektu byla navržená možnost zavedení MDM technologie implementovat na zařízení sdíleného notebooku a na výjezdových zařízeních. Funkce vypnutí aplikace v případě ztráty, nebo odcizení, nebo odepření do osobního zařízení členů jednotky má správce k dispozici. Návrh se vztahoval na implementaci některých známých aplikací, jako je IBM MaaS360 jedno z populárních řešení na trhu nebo Microsoft Intune jako součást Microsoft 365. V obou případech by správce mohl spravovat zařízení, v případě jejich odcizení ze zbrojnice zařízení na dálku uzamknout, nebo přesunout data na náhradní uložiště a pachatel by se tak nedostal k datům a informacím uložených v zařízení. Realizovala se prohlídka hasičské zbrojnice s ukázkou všech bezpečnostních prvků, aby členové věděli, jaké zabezpečení aktuálně mají a o kterém mohou do budoucna uvažovat.

Obrázek 10 Školení ve vybraném subjektu, vlastní, 2024.

8.3 Posouzení přínosu školení

Po proběhlém školení byl účastníkům rozdán dotazník. Dotazníkové šetření bylo stejné, jako šetření, které již vyplnili respondenti dříve. Tentokrát dotazníkové šetření respondenti vyplnili až po školení. Dotazníky byly v teoretických částech vyplněny správně. Velký

posun respondenti prokázali právě v uvědomování hrozeb, jejich preventivní činnosti. Dokázali správně předcházet hrozbám a v případě jejich výskytu znát postup, jak zamezit poškození nebo ztrátě dat a informací. Školení se ukázalo jako podstatná prevence předcházení ztrát nebo poškození dat a informací. Školení bylo navrženo na bezpečnostní prvky přímo na subjekt a zohledňovalo vybrané aspekty informační bezpečnosti, které se subjektu nejvíce dotýkají. Po měsíci byl proveden osobní rozhovor se subjektem, který poskytl informace o tom, že osoby, které se zúčastnily školení správně zálohují a ukládají dokumenty. Vědí, jak pracovat s externími uložišti a kontrolují data po jejich zapsání. Využívají hesla pro přístup do systému a podílí se na bezpečnosti i zvýšením opatřeních na svých osobních zařízeních. Subjekt vyhodnotil, že provedené školení přineslo ve vzdělání velký posun, který umožní předcházet hrozbám ztráty nebo poškození dat. Školení dokázalo ve vybraném subjektu zvýšit prevenci na předcházení hrozeb v informační bezpečnosti. Prezentace byla vytvořena experimentálně v souladu s vybraným subjektem, práce je možná k nahlédnutí jako příloha. Školení se dá aplikovat i pro jiné sbory dobrovolných hasičů, mohlo by také sloužit jako podklad pro další zpracování a zahrnutí do vzdělávacích programů. Subjektu také byla navržená možnost financování, nebo osoba, která by mohla školení provádět. Na školení byla vyjmenována aktiva, kterými subjekt disponuje a proč jsou data a informace jedním z nejdůležitějších aktiv, které se v subjektu nacházejí.

Obrázek 11 Porovnání dotazníkových šetření, subjekt – upraveno, 2024.

Dotazníkové šetření provedené po školení prokázalo vysoké hodnoty znalostí. Jedná se tak o prevenci a předcházení hrozeb spojených s informacemi.

8.4 Návrh na financování školení

Finanční stránka informační bezpečnosti sehrála svou roli. Subjekt některá svá zařízení nemá chráněn dostatečným zabezpečením, protože zařízení nepodporují některé funkce biometrického zabezpečení. Subjekt nedisponuje financemi, které by mohl investovat do informační bezpečnosti. Financování pomáhá zabezpečit obec, která vyčlení finance z rozpočtu na podporu subjektů. Část financování pochází i od kraje Zlín, primární financování přichází od státu jako podpory nebo dotace, tyto dotace se však nezabývají informační bezpečností, spíše financování techniky. Finanční podpora ve formě dotací by umožnila subjektu zakoupit zařízení podporující bezpečnostní prvky. Také by umožnila rozvoj při koupi externích uložišť.

Kraj je primárním zdrojem financí, které do subjektu putují, proto je v této části označen kraj a krajské HZS jako zdroj financování na podporu informační bezpečnosti. Financování by také mohla zajišťovat obec, nebo příslušná obec s rozšířenou působností a nahrazovat tak kraj. Obce by mohly pomoci i s hledáním osob, které by provedly školení.

Na informační bezpečnost a školení musí mít na starost pověřená osoba s odpovědným vzděláním. Může se jednat o odborníka lokalizovaného v místě určení subjektu, který provede školení a kontrolu informační bezpečnosti. Mohlo by se jednat o osobu poskytovatele internetového připojení, který má ve své správě daný subjekt. Poskytovatel má podle zákona o kybernetické bezpečnosti na starost bezpečnost provozu, proto za subjekt odpovídá, tato pravomoc by se mohla rozšířit i na informační bezpečnost. Mohlo by se jednat také o osobu, která bude sborem vyčleněná, aby podstoupila kurz informační bezpečnosti, a tím by v rámci působnosti ve sboru dohlížela na informační bezpečnost.

Školení nebo kurz by mohlo organizovat HZS kraje. Hasičský záchranný sbor má své oddělení zabývající se bezpečnosti, tito lidé by mohli v rámci své působnosti vykonávat i školení v krajském působišti. Národní kybernetický úřad má ve své gesci spoustu kurzů zabývající se bezpečností. Jedním z nich je i kurz pro pracovníky nemocničních zařízení. Mohlo by se jednat o kurz, který by byl vytvořen pro sbory dobrovolných hasičů přímo Národním kybernetickým úřadem.

ZÁVĚR

Cílem práce bylo posouzení informační bezpečnosti vybraného subjektu. Práce nastínila problematiku informační bezpečnosti v ochraně obyvatelstva spojených s poškozením nebo ztrátou informací, a možnost trestné činnosti a s tím spojený únik informací.

Práce je rozdělená na dvě části, teoretickou, která obsahuje teoretický vstup do dané problematiky. Jsou zde popsány dostupné zdroje a poznatky o dané problematice. Práce obsahuje také popis informačního systému, který subjekt využívá.

Praktická část se zabývá samotnou informační bezpečnosti subjektu. Tato část se zabývá zabezpečením, kterým disponuje subjekt. Subjektu byly navrhnuty opatření na zabezpečení, práce zpracovala přehled o implementaci zabezpečení formou tabulky. Praktická část práce označila primární hrozbu spojenou s lidskou činností. Právě znalosti osob mohou sehrávat klíčovou roli při bezpečnosti informací. Praktická část zpracovala dotazníkové šetření zaměřené na znalost dané problematiky, protože lidé byli odhaleni jako nejslabší článek systému spojených s hrozbou ztráty nebo poškození dat a informací.

Návrhem na opatření je školení zabývající se informační bezpečností. Do práce bylo navrhnuto školení rozdělené na teoretickou a praktickou část. Školení bylo sestavené pro daný subjekt, zahrnovalo praktické ukázky, jak správně pracovat s daným systémem. Po osobním rozhovoru se ukázalo, že školení bylo přínosné především v praktické části, protože členové subjektu dokážou pracovat se systémem efektivněji a bránit se před hrozbou ztrát a poškození dat. V návrhu je také zahrnut návrh na financování.

Hlavní i dílčí cíle byly splněny. Práce naplňuje posouzení informační bezpečnosti ve vybraném subjektu. Zpracování teoretického vstupu do dané problematiky, provedení zhodnocení informační bezpečnosti subjektu pomocí aktuálních zabezpečení a návrhu na zlepšení opatření, dotazníkové šetření pro zjištění současného stavu znalostí informační bezpečnosti subjektu, návrh opatření pro zvýšení informační bezpečnosti vybraného subjektu. Navrhnuté opatření je školení, které by zvýšilo znalost informační bezpečnosti v subjektech zabývající se ochranou obyvatelstva.

Přínosem této práce je odhalení nedostatečné informační bezpečnosti v subjektu. Nedostatečnost spočívá v lidském vědění a znalostech, jak pracovat se systémem a s tím spojenou bezpečnosti dat a informací. Kromě toho také nedostatečné financování subjektu na pořízení vyšší bezpečnostních opatření. Nedostatečná informační bezpečnost v subjektech ochrany obyvatelstva přináší hrozby, které mohou vést nejen ke ztrátě a

poškození důležitých dat konkrétního subjektu, ale také únik a vyzrazení kritických dat ochrany obyvatelstva.

Závěrem lze říct, že hrozby informační bezpečnosti jsou pro subjekt aktuální a je potřeba pracovat s předpokladem a připravit se na ně. Je proto potřeba zvyšovat informační bezpečnost v subjektech ochrany obyvatelstva na předcházení hrozeb. Ať už se může jednat o hrozby osob pohybující se v subjektu, které svou neznalostí mohou data poškodit, nebo špatným provedením znehodnotit, tak i osob, které přicházejí zvenčí a informace chtějí získat neoprávněným přístupem, jejich odcizením nebo vyzrazením. Vyzrazení kritických informací v ochraně obyvatelstva může znamenat velké riziko. Na základě zjištěných informací, které poskytla práce, lze říct, že pomocí provedeného školení, subjekt dosáhl vyšších znalostí bezpečnosti a s tím spojenou prevenci před těmito hrozbami a znalost zabezpečení informací. Hrozby se mohou měnit a lišit, proto je potřeba jejich znalost hodnocení a pochopení jejich chování, aby lidé byli schopni hrozbám předcházet.

„*Právě jednoduchost útoku zacíleného na nejslabší článek celého systému z něj zpravidla činí tu nejúčinnější formu.*“ (Kolouch, 2016)

SEZNAM POUŽITÉ LITERATURY

AFCEA. Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf. [cit. 2024-03-01].

ANDERSON, Ross, 2008. *Security engineering : a guide to building dependable Strategies.* Birmingham: Mumbai. ISBN 9781788475297.

ANDRESS, Jason, 2014. *The Basics of Information Security. Syngress.* ISBN 978-0-12-800744-0.

AVAST, 2021. *Nemocnice pod náporem hackerů: Jak proběhly nejznámější kyberútoky na české nemocnice?* Online. Dostupné z: https://blog.avast.com/cs/nemocnice-pod-naporemhackeru-jak-probihaji-kyberutoky-na-ceske-nemocnice. [cit. 2024-03-01].

AWAD, Ali Ismail, FAIRHURTS, Michael, 2018. Information Security: Foundations, Technologies and Applications. London: The Institution of Engineering and Technology. ISBN 9781849199742.

BASL, Josef a Roman BLAŽÍČEK, 2012. *Podnikové informační systémy Podnik v informační společnosti - 3., aktualizované a doplněné vydání*. Grada. ISBN 978-80-247-7595-1.

Cybersecurity, 2024. Online. Merriam-Webster. Dostupné z: https://www.merriam-webster.com/dictionary/cybersecurity. [cit. 2024-04-03].

DIOGENES, Yuri a OZKAYA, Erdal, 2018. *Cybersecurity - Attack and Defense distributed systems*. Druhé vydání. Indianapolis: Wiley Publishing. ISBN 9780470068526.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2008. *Řízení bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk, 2019. *Řízení kybernetické informací*. Praha: Professional Publishing. ISBN 9788086946887.

DVOŘÁK, Josef a Ladislav SVRČINA,1999. *Teorie a historie civilní ochrany II*. 1. vyd. Vyškov: VVŠ PV. ISBN 80-7231-034-8.

Hasičský záchranný sbor České republiky, 2024. *Varování obyvatelstva v České republice*. [Online]. Dostupné z: https://www.hzscr.cz/clanek/varovani-obyvatelstva-v-ceske-republice.aspx

Hasičský záchranný sbor, 2021. *Novela zákona o požární ochraně*. [online]. [cit. 29. dubna 2024]. Dostupné z: https://www.hzscr.cz/clanek/novela-zakona-o-pozarni-ochrane.aspx

Hasičský záchranný sbor, 2024. *Jednotky PO – Hasičský záchranný sbor České republiky*. [online]. [cit. 29. dubna 2024]. Dostupné z: https://www.hzscr.cz/clanek/jednotky-po-961839.aspx

HASSANIEN, Aboul a Mohamed ELHOSENY, ed., 2019. Cybersecurity and secure information systems: challenges and solutions in smart environments. Cham: Springer. Advanced sciences and technologies for security applications. ISBN 978-3-030-16839-1

HENDERSON, Anthony, 2023. *The CIA Triad: Confidentiality, Integrity, Availability.* Online. HENDERSON. Dostupné z: https://panmore.com/the-cia-triad-confidentiality-integrity-availability. [cit. 2024-04-03].

IDNES, 2022. *Zloději ukradli hasičům v Praze a okolí techniku za stovky tisíc.* Online. Dostupné z: https://www.idnes.cz/praha/zpravy/policie-hasici-kradez-hasicske-stanice-hydraulicke rozpinaky. A220406_111026_praha-zpravy_baky. [cit. 2024-03-01].

JEDNOTKA HASIČSKÉHO ZÁCHRANNÉHO SBORU podniku, 2024. GENERÁLNÍ ŘEDITELSTVÍ HASIČSKÉHO ZÁCHRANNÉHO SBORU ČR. *Hasičský záchranný sbor ČR* [online]. [cit. 2024-05-01]. Dostupné z: https://www.hzscr.cz/clanek/vykon-sluzby.aspx?q=Y2hudW09Mg%3D%3D

JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef, 2015. *Výkladový slovník Kybernetické bezpečnosti.* Online. Třetí vydání. Praha: Policejní akademie ČR v Praze Česká pobočka

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

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. Praha:CZ.NIC. ISBN 978-80-88168-31-7.

KOLOUCH, Jan, 2016. *CyberCrime*. Praha: CZ.NIC, z.s.p.o. ISBN 9788088168157.

KOŘÍNEK, Ondřej, 2023. *Zloději sebrali hasičům vybavení na vyprošťování a vypáčili s ním bankomaty*. Online. Dostupné z: https://www.novinky.cz/clanek/krimi-zlodeji-sebrali hasicum-vybaveni-na-vyprostovani-a-vypacili-s-nim-bankomaty-40430666. [cit. 2024-03-01].

MÁRA, Petr, 2023. *Jsi v bezpečí před Flipper Zero? Co všechno lze "ukrást" pomocí hračky za pár tisíc?* Online, video. 11.1.2023. Dostupné z YouTube: https://www.youtube.com/watch?v=LSjCmx5T9w8.

Národní bezpečnostní úřad, 2024. *Kdo a kdy může mít přístup k utajovaným informacím*. [online]. [cit. 29. dubna 2024]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-

informaci/personalni-bezpecnost-oznameni-pro-v-osvedceni-d-t-pt-certifikaty/1041-kdo-a-kdy-ma-pristup/

Národní strategie kybernetické bezpečnosti, 2020. Online. Dostupné z: narodni_strategie_kb_2020-2025_ cr.pdf (gov.cz). [cit. 2024-03-01].

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, 2021. *Kybernetická bezpečnost.* Online. Dostupné z: Národní úřad pro kybernetickou a informační bezpečnost – Kybernetická bezpečnost (gov.cz). [cit. 2024-03-01].

Nezávislý kontrolní úřad pro ochranu osobních údajů, 2014. *317/2014 Sb*. [online]. [cit. 29. dubna 2024]. Dostupné z: https://nukib.gov.cz/download/publikace/legislativa/vvis_317-2014sb.pdf.

NOVÁK, Luděk a Josef POŽÁR. *Systém řízení informační bezpečnosti* [online]. 10 [cit. 2024-04-29]. Dostupné z: https://www.cybersecurity.cz/data/SRIB.pdf

Parkerian Hexad, 2009. Online. InfoSecMinds. Dostupné z: https://vputhuseeri.wordpress.com/2009/08/16/149/. [cit. 2024-04-03].

Portál veřejné správy, 2024. *Zpracování osobních údajů a cookies*. [online]. [cit. 29. dubna 2024]. Dostupné z: https://www.gov.cz/zpracovani-osobnich-udaju-a-cookies

POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 8086898385.

SMEJKAL, Vladimír, 2022. *Kybernetická kriminalita. 3. rozšířené a aktualizované vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-849-5.

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o. ISBN 9788073807658.

Správa státních hmotných rezerv (SSHR), 2024. *Aktuality – Informační web systému Krizkom*. [online]. [cit. 29. dubna 2024]. Dostupné z: https://www.krizkom.cz/aktuality/.

STAIR, Ralph a George REYNOLDS, 2012. *Principles of information systems*. 10. vydání. Boston: Course Technology Cengage Learning. ISBN 9780538478298 0-538-47829-2.

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-737-5.

TIPTON, Harold F. a Micki KRAUSE, 2008. *Information security management handbook*. 6. vydání. Boca Raton; New York: Auerbach. ISBN 0849374952.

TOMEK, Miroslav, 2018. *Bezpečnost a ochrana objektů a osob*. Uherské Hradiště. Skripta. Univerzita Tomáše Bati.

Tornádo na Moravě, 2021. In: GENERÁLNÍ ŘEDITELSTVÍ HASIČSKÉHO ZÁCHRANNÉHO SBORU ČR. *HZS Jihomoravského kraje* [online]. [cit. 2024-05-01]. Dostupné z: https://www.hzscr.cz/script/docDetail.aspx?docid=22307850&doctype=ART&prev=true&lang=cs

Traffic Light Protocol (TLP) Definitions and Usage, 2022. Online. *Cybersecurity & infrastructure security agency.* Dostupné z: https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage. [cit. 2024-04-03].

TVRDÍKOVÁ, Milena, 2008. *Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů*. Praha: Grada. ISBN 9788024727288.

UŘIČAŘ, Miroslav a Vladan RÁMIŠ, 2020. *Obecné nařízení o ochraně osobních údajů*. Komentář. C. H. Beck. ISBN 978-80-7400-815-3.

Ústavní zákon č. 1/1993 sb. Ústava České republiky, 1992. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/1993-1

Ústavní zákon č. 110/1998 Sb. o bezpečnosti České republiky, 1998. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/1998-110

VLÁDA ČESKÉ REPUBLIKY, 2021. *Kybernetická bezpečnost*. Online. Dostupné z: https://vlada.gov.cz/cz/evropske-zalezitosti/umela inteligence/kyberneticka_bezpecnost/kyberneticka-bezpecnost-192766/. [cit. 2024-03-01].

VRANÝ, Jan, 2021. KRIMI: *Dačičtí policisté vyšetřují krádež v hasičské zbrojnici SDH ve Starém Hobzí.* Online. Dostupné z: https://jvpress.cz/2021/10/03/krimi-dacicti-policiste vysetruji-kradez-v-hasicske-zbrojnici-sdh-ve-starem-hobzi/. [cit. 2024-03-01].

Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích, 2014. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-317

WIENER, Norbert, 1960. *Kybernetika: neboli řízení a sdělování v živých organismech a strojích*. Praha: Státní nakladatelství technické literatury.

Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů, 2000. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-101/zneni-20170701

Zákon č. 110/2019 Sb. o zpracování osobních údajů, 2019. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110/zneni-20190424#p67_p67-1-1

Zákon č. 239/2000 Sb. o integrovaném záchranném systému a o změně některých zákonů, 2000. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-239

Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon), 2000. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240

Zákon č. 241/2000 Sb. o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů, 2000. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-241

Zákon č. 273/2008 Sb. o Policii České republiky, 2008. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-273

Zákon č. 320/2015 Sb. o Hasičském záchranném sboru České republiky a o změně některých zákonů (zákon o hasičském záchranném sboru), 2015. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2015-320

Zákon č. 374/2011 Sb. o zdravotnické záchranné službě, 2011. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2011-374

Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, 2005. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

Zákon České národní rady č. 133/1985 Sb. o požární ochraně, 1985. In: *Zákony pro lidi* [online]. AION CS, 2010–2024 [cit. 2024-05-01]. Dostupné z: https://www.zakonyprolidi.cz/cs/1985-133/zneni-20240322

ZEMAN, Petr (ed.), 2002. *Česká bezpečnostní terminologie: výklad základních pojmů.* Brno: Masarykova univerzita, Mezinárodní politologický ústav. ISBN 80-210-3037-2.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

HZS Hasičský záchranný sbor

MDM Mobile device management

SDH Sbor dobrovolných hasičů

SMS Krátká textová zpráva

SEZNAM OBRÁZKŮ

SEZNAM TABULEK