Koncepce kybernetické bezpečnosti vybraných složek integrovaného záchranného systému

Ivo Gahura

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

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

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Ivo Gahura**
Osobní číslo:	**L18088**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**Kombinovaná**
Téma práce:	**Koncepce kybernetické bezpečnosti vybraných složek integrovaného záchranného systému**

Zásady pro vypracování

1. V souladu s momentálně platnou legislativou proveďte rešerši dostupných zdrojů v oblasti IZS a kyberntické bezpečnosti.
2. Vhodně prezentujte teoretické poznatky rešerší.
3. Proveďte analýzu rizik kybernetické bezpečnosti u vybraných složek IZS a navrhněte koncept nápravných opatřeních na základě provedené analýzy.

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

Seznam doporučené literatury:

1. KOLOUCH, Jan a kol. *CyberSecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-37-7.
2. ŠULC, Vladimír. *Kybernetická bezpečnost*. ČR: Aleš Čeněk s.r.o., 2019. ISBN 978-80-7380-737-5.
3. DONÁT, Josef. *Právo v síti*. Praha: C. H. Beck, 2016. ISBN 978-80-7400-610-4.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Pavel Valášek**
Ústav krizového řízení

Datum zadání bakalářské práce: **1. prosince 2020**
Termín odevzdání bakalářské práce: **14. května 2021**

L.S.

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

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

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: 6. 8. 2021

Jméno a příjmení studenta: Ivo Gahura

.....
podpis studenta

ABSTRAKT

Bakalářská práce se zabývá kybernetickou bezpečností v rámci IZS. Cílem teoretické části je podrobně popsat tato dvě témata a vysvětlit jejich vzájemné propojení. Součástí teoretické části je také představení metod analýzy použitých v části praktické. Praktická část analyzuje konkrétní složku IZS z perspektivy kybernetické bezpečnosti procesu toku informace od momentu zavolání na tísňovou linku po předání pacienta do nemocničního zařízení. Analýza se zaměřuje na vyhledávání slabých míst v procesu, na která jsou následně aplikována nápravná opatření. Tím vzniká nový koncept procesu, což je hlavním cílem bakalářské práce.

Klíčová slova: kybernetická bezpečnost, integrovaný záchranný systém, zdravotní záchranná služba, informace, analýza

ABSTRACT

This Bachelor thesis deals with cyber security of the IZS (Integrated Rescue System). The aim of theoretical part is to describe these two subjects in great detail and to explain their interconnections. Theoretical part also encompasses introduction of the methods of analysis used in the practical part. The practical part analyzes a specific IZS file from the perspective of cybernetic security regarding the process of flow of information, from the moment of calling the hotline, to the transfer of the patient into medical care. The analysis focuses on the search for weak spots in the process, to which appropriate correcting measures are applied. This way, a new process concept is created, which is the main goal of this Bachelor thesis.

Keywords: cyber security, integrated rescue system, emergency medical services, information, analysis

Rád bych zde vyjádřil poděkování především vedoucímu mé bakalářské práci panu Pavlu Valáškovi, jelikož mě jeho trpělivý a shovívavý přístup dokázal motivovat k psaní dalších a dalších stránek a mohl jsem se na něj spolehnout při řešení jakéhokoliv problému. Velké poděkování patří také Milanu Leškovi a Radimu Kozelskému za spolupráci při zpracovávání praktické části.

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

OBSAH

ÚVOD

Informační doba, ve které se lidstvo v současnosti nachází, naskýtá neskutečné množství příležitostí, ale stejně tak s ní přicházejí i hrozby. Vzhledem k tomu, že umění používat informační a komunikační technologie v dnešní době staví základ úspěchu států, firem i jednotlivců, je nezbytné, aby se lidstvo naučilo využít veškerý jejich potenciál, což znamená i zajištění bezpečnosti těchto technologií a bezpečné práce s internetem. Taková bezpečnost je známá pod názvem kybernetická bezpečnost a v současnosti se dostává do popředí zájmu světového dění, státních politik a podnikatelského prostředí.

Z toho důvodu jsem rád, že moje práce může skloubit tématiku integrovaného záchranného systému s kybernetickou bezpečností, jelikož i v této sféře je zásadní mít tuto dovednost na špičkové úrovni, aby byla občanům zajištěna vysoká úroveň kvality poskytování pomoci při vzniku mimořádných událostí.

V teoretické části práce si především dávám za cíl podrobně vysvětlit problematiku kybernetické bezpečnosti a následně popsat integrovaný záchranný systém s přihlédnutím na skutečnost, jakým způsobem se integrovaný záchranný systém dostává do styku s kybernetickým prostorem, a proč je tedy důležité se o kybernetické bezpečnosti v souvislosti s integrovaným záchranným systémem bavit. Cílem praktické části je analyzovat současnou situaci v integrovaném záchranném systému z pohledu kybernetické bezpečnosti a pomocí příslušných metod vyhledat slabá místa, na která lze aplikovat nápravná opatření.

Výsledkem celé bakalářské práce je tedy nový koncept analyzované sféry vytvořen na základě implementace nápravných opatření tak, aby bylo dosaženo zlepšení stavu kybernetické bezpečnosti, což ve výsledku napomůže efektivnějšímu fungování služeb integrovaného záchranného systému.

V teoretické části práce vycházím především z odborné literatury, přičemž jsem se snažil hledat co možná nejaktuálnější tituly, což vzhledem k povaze vybrané problematiky nebyl problém. Praktická část je založena na informacích poskytnutých přímo z informačního oddělení analyzované složky. K objektivitě všech informací a analýz představených v praktické části mi napomohl i rozhovor s příslušníkem výjezdové skupiny pracující ve strukturách zdravotnické záchranné služby. Použité metody analýzy jsou podrobně vysvětleny v závěru teoretické části práce.

I. TEORETICKÁ ČÁST

1 POJMY V RÁMCI KYBERNETICKÉ BEZPEČNOSTI

Na úvodní řádky bakalářské práce jsem se rozhodl zařadit z mého pohledu důležitou kapitolu, ve které budou vysvětleny základní pojmy související s danou tematikou. V rámci bakalářské práce není prostor k tomu, aby zde byly představeny všechny pojmy, a proto bude následující text průřezem nejpodstatnějších pojmů.

Zprvu se zaměřím na to, jakým způsobem se posunulo vnímání pojmu kybernetika od doby, kdy tento obor vznikal, až po současnost.

1.1 Kybernetika

Kybernetika je vědní obor, který se svým obsahem zaměřuje na studování přenosu informace napříč živými bytostmi a také stroji, přičemž dále studuje i řízení takové informace. (Kybernetika, 2002)

Prameny kybernetiky sahají až do roku 1919, kdy její zakladatel, Norbert Wiener, se dostává do pozice asistenta na katedře matematiky technologického institutu v Massachusetts. Zde se začíná zabývat novým oborem, který pojmenuje „kybernetika“, ten se svým obsahem dotýká matematiky, fyziky, neurologie a ekonomie. (Kapoun, 2004)

Z výše uvedeného je patrné, že kybernetika, ač by se mohl jevit opak, není vůbec novou vědou, ba naopak je to vědní obor přes 100 let starý. V současnosti je ale těžké najít jakoukoliv aktuální literaturu k danému oboru, a proto se mi zdá, že tento obor byl poněkud pohlcen obory ICT a právě onou kybernetickou bezpečností, o které moje bakalářská práce z převážné většiny je.

1.2 Kybernetická bezpečnost

Kybernetickou bezpečností se rozumí systematizovaný proces obrany softwarového a hardwarového vybavení ICT, serverů, mobilních zařízení a informací, jehož cílem je vyloučit jejich zcizení, poškození či neoprávněný zásah. (Kybernetická bezpečnost – definice a právní předpisy, 2020)

1.3 Další pojmy

Nyní již následují další důležité pojmy, se kterými budu v rámci své bakalářské práce dále nakládat.

1.3.1 Kyberprostor

Již několikrát zmíněný kyberprostor představuje prostor v digitální podobě, ve kterém se informace uchovávají, šíří, zpracovávají, ale také tvoří. (Česko, 2014)

Jedná se tedy o prostor tvořený hardwarovým i softwarovým vybavením informačních a komunikačních technologií, které společně propojují veškeré počítače a další koncové prvky ICT prostřednictvím globální počítačové sítě. Je to takzvaná virtuální realita. (Kolouch et al., 2019)

1.3.2 Kybernetická hrozba

Kybernetická hrozba představuje nekalou aktivitu v kyberprostoru, která může ohrozit bezpečnost občanů a celého národa nebo národní ekonomiku. (Cyber crime, 2020)

U kybernetické hrozby je důležité dodat, že tato aktivita může nebo také nemusí být dotažena do konce, ale v každém případě zde hrozí riziko narušení bezpečnosti. (Kolouch et al., 2019)

Takové hrozby můžeme dělit na vnitřní a vnější. Dále se hrozby dělí na základě úmyslu a původu. Do dělení hrozeb podle původu patří hrozby antropogenní a přírodní. Dělení hrozeb se taky uvádí podle toho, jakou konkrétní škodu způsobí, sem například patří hrozba odepření služby. Poslední dělení hrozeb se zabývá motivací útočníka. (Před čím se chránit, 2016)

1.3.3 Bezpečnostní incident a bezpečnostní událost

Bezpečností událostí se rozumí aktivita, která by mohla ohrozit informaci nebo nějaký z prvků kyberprostoru, kdežto bezpečnostní incident už takové konkrétní narušení bezpečnosti přímo představuje. (Česko, 2014)

Z pohledu oboru kybernetické bezpečnosti je třeba tento rozdíl vnímat a nezaměňovat tyto dva pojmy.

1.3.4 Kybernetický útok

U pojmu kybernetický útok se již dostáváme do situace, která představuje úmyslné a vědomé jednání prostřednictvím kyberprostoru s cílem někoho nebo něco poškodit. (Kolouch, 2016)

1.3.5 Internet

Internet je celosvětová síť, která obsahuje neskutečné množství počítačů a počítačových sítí lokalizovaných v různých koutech planety. Ty jsou navzájem propojeny prostřednictvím počítačové infrastruktury, pod níž si můžeme představit například optické kabely či bezdrátové připojení. Díky internetu se můžeme z pohodlí domova připojovat na libovolné servery a vyhledávat potřebné informace. (Jirásek, Novák a Požár, 2015)

1.3.6 Aktiva

Aktivum je výčet všeho majetku, a to jak hmotného, tak nehmotného. Pro potřeby kybernetické bezpečnosti je vhodné vytvořit hodnocení aktiv, které například kvalifikuje dopady na organizaci v případě napadení aktiva. Existují tři základní vlastnosti aktiv, které je potřeba zabezpečit. Jsou jimi důvěrnost, dostupnost a integrita neboli celistvost. (Dostál, Jašek a Kristová, 2013)

1.3.7 Informace

Informace se řadí do nehmotných aktiv. Kvalitní informace zvyšuje znalosti a svému uživateli poskytuje detailní představu o dění v reálném světě. Informace je reprezentována konkrétním obsahem nějaké zprávy. (Lukáš et al., 2011)

Pokud se máme na informaci spoléhat, měla by obsahovat následujících sedm elementárních atributů. První je **důležitost**, u které se je směrodatné, aby informace opravdu obsahovala zprávu ohledně dané problematiky. Druhá **srozumitelnost** reprezentuje jednoznačnost informace, které se dá snadno porozumět. Třetí atribut je **včasnost**, což je u informací mimořádně důležité. Na včasnost navazuje čtvrtá **aktuálnost**, která zaručuje, že informace nejsou zastaralé. Poté následuje pátá **hodnověrnost**, která by měla vyloučit neověřený původ informace. Šestá **úplnost** neboli integrita značí to, že informace je celistvá. Poslední **přiměřenost** zaručuje, že adresát nebude zahlcen zbytečnými informacemi, které jsou příliš detailní. (Lukáš et al., 2011)

1.3.8 Zranitelnost

Zranitelnost leze definovat jako: „*Slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami*“ (Jirásek, Novák a Požár, 2015, 136)

2 KYBERNETICKÁ BEZPEČNOST

Následuje kapitola, která je věnována podrobnému popisu kybernetické bezpečnosti, čehož se snažím dosáhnout využitím co největšího množství relevantních zdrojů v dané problematice.

Kybernetická bezpečnost chrání počítačové sítě a samotné počítače před napadením v rámci kybernetického prostoru. (Šulc, 2018)

Podle dalšího zdroje se kybernetická bezpečnost jednoduše zabývá zajištěním ochrany kybernetického prostoru. I tento zdroj tedy klade důraz na spojitost kybernetické bezpečnosti a kybernetického prostoru. (Doucek, Konečný a Novák, 2019)

Pojem kybernetické bezpečnosti je možné dále chápat jako snahu o předcházení zneužívání elektronických dat nebo dále jako veškerá opatření směřující k ochraně kybernetického prostoru s důrazem na to, že jsou tato opatření směřována jak na veřejný, tak i na soukromý sektor. Komplexní definice kybernetické bezpečnosti by tedy měla zahrnovat ochranu počítačů a dalších prvků komunikační a informační technologie společně se schopností těchto technologií reagovat na útoky v kybernetickém prostoru a zajistit svoji funkčnost po obnovovacím procesu, který následuje po kybernetickém útoku. (Kolouch et al., 2019)

Kybernetická bezpečnost je také úzce spjata s bezpečností informační, která má za úkol ochranu samotných informací před vnějšími přírodními vlivy, před zcizením nebo zneužitím za předpokladu, že uživatel musí být schopen s těmito informacemi nadále pracovat. (Kybernetická bezpečnost, 2011)

Kybernetické bezpečnosti se pozorně věnuje i BIS, která si je vědoma toho, že tato problematika se stává prioritním zájmem pro zpravodajské služby po celém světě a je zde na místě mezinárodní spolupráce k zajištění bezpečnosti v rámci kybernetického prostoru. BIS se převážně zabývá takovými incidenty, které by svou podstatou mohly ohrozit zájmy ČR. (Kybernetická bezpečnost, 2018)

Firma Kasperksy chápe kybernetickou bezpečnost jako obranu serverů, počítačů, mobilních a elektronických zařízení, sítí a dat, přičemž kybernetickou bezpečnost dělí na další prvky, kterými jsou bezpečnost sítí, aplikační bezpečnost, informační bezpečnost, operační bezpečnost, jež zahrnuje procesy pro ochranu dat, a neméně důležitý prvek obnovy a kontinuity. (What is Cyber Security, 2020)

Je patrné, že oblast kybernetické bezpečnosti má před sebou velké výzvy a příležitosti, ale také hrozby, což celkově z tohoto oboru dělá perspektivní oblast zájmu pro širokou škálu lidí, jak ve smyslu pracovních pozicí, tak i ve smyslu různých kybernetických útočníků.

2.1 Prvky kybernetické bezpečnosti

Kybernetická bezpečnost, ostatně jako všechno v životě, není jednoduchý jednolitý prvek, ale je to systém a interakce vícero prvků, které při správném fungování vytvářejí právě onu kýženou kybernetickou bezpečnost. (Kolouch et al., 2019)

2.1.1 Lidé

Prvním prvkem kybernetické bezpečnosti jsou lidé, které je možno vnímat z různých úhlů pohledu. Lidé, kteří vytvářejí kybernetickou bezpečnost. Lidé, jakožto příjemci pravidel. Lidé, které je potřeba chránit před kybernetickými útoky. Lidé, kteří musí být informování a proškoleni v oblasti kybernetické bezpečnosti. A konečně lidé, kteří představují hrozbu. Je potřeba dodat, že lidé jsou vnímáni jako nejslabší článek kybernetické bezpečnosti a většinou je to člověk, kdo nese vinu na selhání systému. (Kolouch et al., 2019)

2.1.2 Technologie

Druhým prvek jsou technologie neboli fyzická bezpečnost. Jedná se o technologie koncové, které jsou obsluhovány uživateli, ale také o technologie, jež dohromady skládají celou informační infrastrukturu firem a také aktivní zabezpečovací prvky, jimiž jsou například detekční systémy. (Kolouch et al., 2019)

2.1.3 Procesy

Posledním prvkem jsou procesy, které lidem určují pravidla používání technologií, a tím celou kybernetickou bezpečnost uvádí do provozu. Tato takzvaná organizační bezpečnost je právem nejsložitější částí kybernetické bezpečnosti, neboť je potřeba procesy kontinuálně udržovat, modifikovat a nastavovat nové tak, aby byla zajištěna co největší míra bezpečnosti. (Kolouch et al., 2019)

2.2 Časová osa

Kybernetická časová osa neboli také životní cyklus se skládá ze tří částí, a to **prevence, detekce** a následná **reakce**. (Kolouch et al., 2019)

Různé zdroje rozšiřují tuto základní časovou osu i o další části, které si uvedeme ve spojitosti se základní časovou osou.

Zde představenou časovou osu, neboli životní cyklus jsem si vypůjčil z odborné literatury společnosti CZ.NIC, která však čerpala z portálu kybez.cz, a záchytnými body zde jsou správa, audit, rizika, opatření a zavedení. Tento cyklus pochopitelně běží neustále dokola. (Kolouch et al., 2019)

Pokud si tuto časovou osu představíme ve spojitosti se základní osou, potom zde **prevenci** reprezentuje správa a audit. Rizika jsou zde **detekcí**, zatímco opatření se zavedením znázorňují **reakci**.

Obrázek 1 - Životní cyklus dle Kybez (Kybernetická bezpečnost životní cyklus, 2021)

Kybernetická bezpečnost je proces, který neustále běží a jeho zastavení by mohlo vést ke vzniku rizika ohrožení kybernetickým útokem, je tedy jasné, že takové zastavení je krajně nežádoucí.

2.3 Rozdíl mezi kybernetickou a informační bezpečností

Definice kybernetické bezpečnosti zní: *„Souhrn právních, organizačních, technických a vzdělávacích prostředků, směřujících k zajištění ochrany kybernetického prostoru*“. (Doucek, Konečný a Novák, 2019, 19)

Informační bezpečnost se však zaměřuje přímo na ochranu informace a jejím úkolem je zajistit důvěrnost, celistvost a dostupnost informace. (Doucek, Konečný a Novák, 2019)

Jsou to tedy dva rozdílné pojmy, které se ale mohou navzájem ovlivňovat. Příkladem může být situace, kdy incident z oblasti informační bezpečnosti nastartuje incident v kybernetické bezpečnosti, tedy že tento incident v rámci kybernetické bezpečnosti měl svůj původ v bezpečnosti informační. Je to dáno tím, že veškeré digitální informace, které jsou objektem zájmu informační bezpečnosti, se nacházejí v kybernetickém prostoru, který je zase objektem zájmu kybernetické bezpečnosti. (Doucek, Konečný a Novák, 2019)

Praktickým příkladem informační bezpečnosti je GDPR. Jedná se o legislativní dokument EU, který přesně určuje pravidla pro nakládání s osobními údaji. Jelikož je tento dokument ve formě evropského nařízení, tak zaručuje, že na území celé EU budou kladeny na subjekty stejné nároky a národní politika nebude mít možnost znění tohoto nařízení jakkoliv ovlivňovat. (GDPR, 2020)

Pravidla GDPR musí dodržovat každý, kdo nakládá s osobními informacemi občanů EU, ale vztahují se taky na subjekty se sídlem mimo EU, kteří jsou aktivní na evropském trhu. Pokud nastane případ, že tato pravidla budou porušována, tak aktérům hrozí astronomické pokuty. (Co je GDPR a jak bude aplikováno v Česku, 2017)

2.4 Aplikovaná kybernetická bezpečnost

V následující podkapitole bude vysvětleno, jakým způsobem se kybernetická bezpečnost uvádí do praxe tak, aby byla míra rizika kybernetického útoku snížena na co nejmenší úroveň. V podstatě se toho dosahuje dvěma způsoby, které však musí být ve vzájemné symbióze. Jsou jimi organizační neboli režimová a technická opatření.

Organizační opatření jsou tady od toho, aby nastolovala pravidla a tím vytvářela celkový systém, jenž organizuje celkovou bezpečnost zaměřenou na informace, aktiva, lidské zdroje, kritickou infrastrukturu, ale také na řešení kybernetických událostí a incidentů. (Kolouch et al., 2019)

Technická opatření reprezentují hmotné i nehmotné, v našem kontextu softwarové, prvky, jež se zaměřují na takové oblasti, jimiž jsou fyzická bezpečnost nebo třeba detekce kybernetických událostí a incidentů a mnohé další. (Kolouch et al., 2019)

Následující výčet není ani náhodou kompletní. Jedná se pouze o průřez možných řešení, který je však pro pochopení dané problematiky dostatečný.

2.4.1 Režimová opatření

Organizační struktury obohacené o nové odbory, které jsou předurčeny pro činnost na půdě kybernetické bezpečnosti, jsou prvním zde představeným režimovým opatřením. Těmito odbory jsou rada pro bezpečnost informací, jež se v první řadě orientuje na správu aktiv dané organizace, a druhým odborem tým pro plánování bezpečnosti informací, který je zodpovědný za implementaci konkrétních režimových opatření. (Doucek, Konečný a Novák, 2019)

Bezpečnostní politika představuje dokument, který přesně vymezuje, jakým způsobem je v rámci konkrétní organizace přistupováno k bezpečnosti jako celku. Takový dokument například stanovuje zásady, kterými se musí zaměstnanci organizace řídit pro zajištění celkové bezpečnosti a obsahuje i konceptuální pojetí informační bezpečnosti. Je nezbytné, aby byl dokument snadno k nalezení a přístupný pro veškeré zaměstnance dané organizace. (Šulc, 2018)

Řízení rizik označuje přístup k rizikům. Zde probíhají procesy identifikace, analýzy a hodnocení rizik. Řízení rizik probíhá v několika konkrétních krocích, do nichž řadíme vytvoření postupu pro hodnocení rizik, identifikaci hrozeb a zranitelnosti, samotné hodnocení konkrétního rizika s objektivním posouzením hrozeb a zranitelnosti, z čehož se následně zpracuje zpráva o hodnocení rizik. Po vypracování zprávy se již přistupuje k samotnému zavádění plánu, který stanovuje, jakým způsobem budou rizika řešena. (Kolouch et al., 2019)

Zajímavým a velmi důležitým bodem je jistě **řízení přístupu osob ke KII nebo VIS**. Metoda již podle svého názvu určuje režim přístupu konkrétních osob ke konkrétnímu systému na základě přidělování přístupových práv a identifikátorů. Řízení přístupu osob je základním stavebním kamenem pro vytvoření funkčního kybernetického zabezpečení. (Kolouch et al., 2019)

Dalším zde představeným opatřením je **řízení kontinuity činností**, znám pod zkratkou BCM. Je to metoda, která by prostřednictvím optimálního nastavení procesů a postupů měla zaručit schopnost organizace pokračovat v běhu nebo schopnost celkové obnovy klíčových prvků organizace na stanovené úrovni, která umožňuje základní fungování organizace potom, co bylo takové fungování ohroženo kybernetickým incidentem. (Kolouch et al., 2019)

ISMS představuje velmi důležité organizační opatření, jeho smyslem je organizování komplexní bezpečnosti informací. ISMS se zavádí ve čtyřech krocích, kdy v prvním kroku se s vedením společnosti jedná o odsouhlasení samotného zavedení a řeší se především finanční stránka věci. Krok druhý zahrnuje práci s aktivy firmy, která je třeba identifikovat a ocenit, po čemž následuje celková analýza rizik. Ve třetím kroku se navrhují konkrétní opatření pro všechna zranitelná místa identifikovaná pomocí předchozí analýzy. Krokem čtvrtým se rozumí certifikace vytvořeného ISMS, který je však z pohledu funkčnosti systému nepovinný. (Dostál, Jašek a Kristová, 2013)

2.4.2 Technická opatření

Prvním technickým opatřením zde představeným bude **nástroj pro ochranu před škodlivým kódem**. Takový nástroj je především zodpovědný za automatizovanou ochranu počítačových a mobilních zařízení, serverů, celkového systému komunikačních sítí a ukládání dat, přičemž je nezbytné, aby tato ochrana probíhala v nepřetržitém provozu. Nabízí se zde dělení na ochranu před malwarem, jenž se do cílových zařízení dostává pomocí mailu, a před malwarem, který se naopak šíří v rozhraní webu. (Kolouch et al., 2019)

Pro funkční ochranu před malwarem a dalšími projevy kybernetické kriminality je zapotřebí detekovat takovou činnosti již v jeho počátku, k čemuž slouží **nástroj pro detekci kybernetických bezpečnostních událostí**. Je to sofistikovaný software, za jehož pomoci dochází ke kontrole zpracovávaných dat a k odepření nevyžádané komunikace. Programy jako Logwatch, Epylog nebo OpenVAS představují konkrétní produkty z trhu, které takovou detekci umožňují. (Kolouch et al., 2019)

Autentizace slouží k přesnému identifikování uživatele a spočívá ve třech principech. Prvním se rozumí, že uživatel něco ví, což ve většině případů značí znalost loginu. Pokud se uplatňuje princip uživatele, který něco má, je zde řeč o situaci, kdy se uživatele prokazuje nějakým předmětem, například USB token. Nejnovější metodou je princip toho, že uživatel něčím je, který je založen na biometrice, kam patří otisky prstů, geometrie ruky, skeny obličeje nebo oční duhovky, analýza krve, tvar vnějšího ucha, DNA nebo třeba rozpoznávání hlasu. (Šulc, 2018)

Autorizace je označení pro udělování oprávnění v systému, která jasně stanovují, s čím a jak může uživatel v systému nakládat. Pro zefektivnění celého procesu se uživatelé dělí do různých skupin s konkrétními oprávněními, což je rozhodně lepší řešení, než kdyby se každému uživateli udělovala oprávnění jednotlivě. (Šulc, 2018)

Penetrační testy představují výborný prostředek, kterým je možno podrobit informační systémy důkladnému testování a následné optimalizaci. Penetrační test spočívá v úmyslné snaze dostat se nelegálně všemi možnými prostředky do systému s cílem detekovat v tomto systému mezery, kterými je útočník schopen do systému pronikat. (Dostál, Jašek a Kristová, 2013)

Velmi zajímavým samostatným oborem, jenž lze řadit mezi technická opatření kybernetického zabezpečení je **kryptografie**.

„*Kryptografie je věda, která zkoumá matematické metody utajování obsahu i prokazování původu přenášených zpráv.*“ (Burda, 2019, 19)

Tohoto cíle je dosahováno různými metodami, z nichž některé představím. Začnu utajovacím kryptosystémem, který se stará o věrohodnost zprávy, čehož se dosahuje prostřednictvím utajení přesného znění zprávy, jehož znalost osobami bez oprávnění je nežádoucí. Autentizační kryptosystémy zajišťují proces autentizace, který byl již vysvětlen, avšak z pohledu kryptografie je zde řeč spíše o konkrétním algoritmu, na jehož základě autentizace probíhá. Generátory nepředvídatelných čísel představují další z metod kryptografie a spočívá, jak již název napovídá, v generování číselné řady, která se nezasvěceným osobám zdá být nesmyslná, protože ji chápou jako pouhá náhodná čísla. Generátory v praxi slouží mimo jiné pro vytváření kryptografických klíčů. (Burda, 2019)

Poslední prvek technického opatření, který zde představím, je **fyzická bezpečnost**, která má ovšem charakter zcela odlišný než doposud popsané prvky, neboť se jedná o takové záležitosti, jako je kupříkladu ochrana před přírodními vlivy. Bohužel je nutno dodat, že oblast fyzické bezpečnosti se v mnoha případech podceňuje, avšak je třeba si uvědomit, že veškeré sofistikované softwarové vybavení je v podstatě k ničemu, když není zabráněno tomu, že se útočník dostane přímo do místnosti serverů a odnese si naše citlivá data. (Kolouch et al., 2019)

Do fyzické bezpečnosti v prvé řadě patří **zajištění perimetru**. **Kontrola přístupu** je další součástí fyzické bezpečnosti a dosahuje se jí pomocí sofistikovaných systémů, ale třeba i pomocí obyčejného zámku na dveřích. **Vnitřní bezpečnost** tkví v rozmístění důležitých místností a jejich zabezpečení s přihlédnutím například na takové detaily, jako je nevhodnost sousedství místnosti serverů s místností rozvodu vody. **Ochrana proti krádeži** má svoji podstatu ve specifickém rozmístění serverů do přesně stanovených místností, které jsou odpovídajícím způsobem uzamčeny a zabezpečeny. **Ochrana před rozebráním a úpravou**

počítačových systému představuje další důležitou součást. U serverů je skoro samozřejmostí, že disponují funkcí automatického detekování otevření serveru a informace o takovém otevření automaticky oznamují. **Ochranou před připojením cizích periferií** se rozumí především eliminace možnosti připojit na chráněné zařízení cizí periferii prostřednictvím USB portu. K tomuto účelu může sloužit USB Port Lock, což je zařízení, které fyzicky znemožní do portu cokoliv zapojit. (Kolouch et al., 2019)

3 KYBERNETICKÁ KRIMINALITA

Ve třetí kapitole se dostává do popředí téma kybernetická kriminalita. Je zde vysvětleno, co to kybernetická kriminalita je, jak se obecně projevuje v praxi a pro úplnost je kapitola doplněna o konkrétní příklady z kyberprostoru.

Původně se tato problematika označovala jednoduše jako počítačová kriminalita. Tento název ovšem mylně svádí k myšlence, že taková kriminalita může být vykonána pouze za pomoci počítače a že počítač tady reprezentuje jedinou použitou technologii. V tomto případě je ovšem třeba chápat slovo počítač v širším kontextu a zahrnou do něj i další prvky ICT včetně softwarového vybavení a samotných dat. (Kolouch, 2016)

Po zakomponování ostatních pojmů se již dostáváme k termínu kybernetická kriminalita, pod kterou si lze představit úmyslnou a cílenou trestnou činnost, která si bere za cíl útoku počítač nebo počítačovou síť či data, nebo naopak je prostřednictvím počítače páchána, přičemž prostor, ve kterém je taková trestná činnost páchána se nazývá kyberprostor. (Kolouch, 2016)

Kybernetická kriminalita se neuvěřitelně rychle rozvíjí, přičemž se neustále objevují nové způsoby, jakými je páchána. Útočníci se neustále učí novým věcem a přizpůsobují své útoky novým trendům využíváním nových technologií mnohdy i za spolupráce s ostatními útočníky napříč kyberprostorem. Pro lidi, kteří kybernetickou kriminalitu potírají, tohle představuje velkou výzvu, neboť neustále musí držet krok s útočníky a učit se novým technologiím a metodám. (Cybercrime, 2017)

3.1 Druhy kybernetických útoků

Jelikož se kybernetická kriminalita většinou projevuje kybernetickými útoky, tak si následující kapitola dává za úkol soupis nejčastějších druhů takových útoků s krátkým popisem pro pochopení, jak konkrétní kybernetický útok probíhá.

Sociální inženýrství představuje cílenou manipulaci lidí s úkolem přesvědčit je, aby dobrovolně podnikali nějakou činnost, která je v zájmu útočníka, nebo aby poskytli útočníkovi kýžené informace. (Šulc, 2018)

Malware cíleně poškozuje na napadeném zařízení v podstatě cokoliv. Záleží, k čemu byl určen, a má mnoho podob, kterými se projevuje. Český význam pro slovo malware je škodlivý software. Na základě toho, jakým způsobem se malware na napadeném zařízení

projevuje, rozlišujeme následující typy. Virus, Trojan horse, Spyware, Phishing, Adware, Ransomware, Rootkit a mnoho dalších. (Šulc, 2018)

Vybral jsem dva typy, z nichž jeden je spíše otravný a druhý velmi závažný, které podrobněji popíšu.

- Prostřednictvím **Adware** se koncovému uživateli zobrazují na napadeném zařízení nechtěné reklamy například v podobě vyskakujících okem. Dost často se objevují jako přidružená funkce u freeware, což je bezplatně dostupný software. (What is malware, 2019)
- **Ransomware** je malware, který zašifruje na napadeném zařízení buď to nějaké konkrétní data, nebo přístup do celého zařízení, a následně je oběť vydírána a nucena zaplatit výkupné, po jehož obdržení útočník zařízení dešifruje. (What is malware, 2019)

Spam je další spíše otravnou záležitostí a projevuje se masivním šířením nějaké zprávy, kterou si ovšem nikdo nevyžádal, a dost často má atributy reklamního sdělení. (Kolouch, 2016)

Phishing se již řadí mezi závažnější projevy kybernetické kriminality a jeho cílem je podvodným jednáním vylákat z oběti osobní údaje, například login nebo číslo kreditní karty. Častou formou je podvodný e-mail. (Kolouch, 2016)

Pharming obdobná metoda, jako Phishing, tudíž opět se jedná o snahu získat osobní údaje oběti, avšak tento útok již probíhá daleko promyšleněji a je těžké ho identifikovat, jelikož funguje na principu přesměrování adresy webového serveru, ke které se oběť připojuje. (Kolouch, 2016)

Hacking a Cracking. V podstatě se jedná o velmi podobné jednání lidí, kteří jsou mistři v používání výpočetní technologie a jsou schopni získat přístup do cizího počítače nekonvenčními metodami. Těmto lidem se říká hackeři a dělí se do skupin White Hats, Black Hats a Grey Hats. Na hackingu se podílejí především White Hats, kteří prolamují přístup do počítače s dobrým úmyslem a cílem je odhalit díry v systému, které jsou následně napravovány, zatímco cracking je chápán jako činnost skupiny Black Hats, kteří prolamují přístupy do systému s úmyslem oběť poškodit. (Kolouch, 2016)

Sniffing je velmi nebezpečná metoda, jejímž cílem je krást data, která pocházejí ze vzájemné komunikace mezi uživatelem a poskytovanou službou, přičemž je důležité, že

tento odposlech je prováděn nelegálně, neboť Sniffing se také používá jako běžná metoda pro diagnostiku sítě. (Kolouch, 2016)

Botnet si lze představit jako armádu navzájem propojených počítačů připravených k tomu, aby prováděly koordinované útoky. Botnet je typickým příkladem zlomyslného využití dobré technologie. (What is a Botnet, 2019)

Prostřednictvím botnetu se například provádí takzvaný **DDoS**, což je útok mnoha počítačů s cílem zahltit koncové zařízení odesíláním velkého množství nesmyslných paketů. Tyto počítače jsou rozmístěny na různých místech po celé planetě, což ztěžuje lokalizovat původ útoku. (Kolouch, 2016)

Existuje řada dalších metod, jak provádět kybernetické útoky, avšak pro představu jak kybernetický útok probíhá a jaké může mít podoby, se mi zdá tento teoretický základ dostačující.

3.2 Konkrétní příklady z kyberprostoru

Jelikož považuji za vhodné teorii doplnit i praxí, tak následující podkapitola si dává za úkol seznámit čtenáře s jedním konkrétním příkladem, který byl detekován v roce 2010, a také se světoznámou skupinou hackerů vystupující pod názvem Anonymous.

3.2.1 Stuxnet

Zprávy o šíření škodlivého softwaru, který je schopen napadat řídicí systémy v průmyslovém odvětví se začala šířit v roce 2010, kdy byl později tento malware podroben průzkumu a vešel ve známost jako kód Stuxnet. Byl to neuvěřitelně sofistikovaný malware, který do té doby neměl obdoby. Mnoho infikovaných počítačů se nacházelo na území USA a Indie, ve které byl výskyt nejmasivnější z důvodu nízkého kybernetického zabezpečení řídicích systémů. (Singer a Friedman, 2014)

Stuxnet nebyl typickým malwarem, jehož úkolem je masivní šíření sama sebe do co největšího počtu počítačů. Pokud Stuxnet napadl počítač, jeho mechanismus dovolil šíření na pouhé další tři počítače. Měl v sobě taky sebedestruktivní kód, který způsobil, že v roce 2012 Stuxnet sám sebe zničil. Zajímavostí taky bylo, že neinfikoval počítač nebo operační systém jako celek, ale zaměřoval se pouze na specifické řídící programy používané firmou Siemens. Vážnou se situace stala, když se zjistilo, že Stuxnet se dostal do Iránského atomového programu. (Singer a Friedman, 2014)

3.2.2 Anonymous

Skupina Anonymous byla v podstatě neidentifikovatelným uskupením různých uživatelů z mnoha internetových odvětví, kteří se spojili ve společném úsilí organizovat koordinované protesty a další akce v kyberprostoru. Anonymous fungoval ve vzájemné shodě jejich členů, že budou v anonymitě a budou společně činit takové kroky, které považují za důležité. (Singer a Friedman, 2014)

Členové skupiny komunikovali prostřednictvím různých internetových fór, kde se domlouvali na společném postupu, identifikovali cíle jejich zájmu a debatovali o akcích, které jsou potřeba vykonat. Členové dále přes různé sociální sítě zveřejňovali informace o svých plánovaných krocích, přičemž tímto způsobem taky verbovali dobrovolníky. Skupinu je možno charakterizovat slovy „decentralizovaní, ale koordinovaní“. (Singer a Friedman, 2014)

4 KYBERNETICKÁ BEZPEČNOST V ČR

Česká republika v roce 2014 vytvořila právní dokument, který se kybernetickou bezpečností přímo zabývá, a jeho znění je zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Hlavní záminkou pro vznik tohoto zákona bylo vytvořit státní úřad, který má svoje místo v právní struktuře České republiky a jenž by sloužil k vytvoření systému kybernetické bezpečnosti a patřičným regulacím. V roce 2017 byl takový úřad ustanoven novelizací zákona o kybernetické bezpečnosti a na poli státních institucí tedy vznikl Národní úřad pro kybernetickou a informační bezpečnost. (Doucek, Konečný a Novák, 2019)

4.1 NÚKIB a NCKB

„*Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.*“ (NÚKIB, 2021)

V organizační struktuře NÚKIB je zakotveno Národní centrum kybernetické bezpečnosti, které mimo jiné provozuje Vládní CERT tým, zároveň provádí prevenční činnost v oblasti kybernetické bezpečnosti, koordinuje postup v případě, že nastala bezpečnostní událost, nebo třeba svou činností poskytuje vzdělání a osvětu v rámci kybernetické bezpečnosti. (NCKB, 2021)

4.2 Kybernetická bezpečnost v rámci EU

Evropská směrnice NIS, jež je dalším závazným legislativním dokumentem v rámci kybernetické bezpečnosti, se především týká dvou skupin subjektů, které jsou rozděleny na provozovatele základních služeb a poskytovatele digitálních služeb. Tyto skupiny přesně definuje a ukládá jim povinnosti, které je nezbytné při provozování daných služeb dodržovat. Základní službou se rozumí bankovnictví či energetika. Digitální službou je myšleno především provozování internetového vyhledávače. (Doucek, Konečný a Novák, 2019)

Agentura ENISA, jakožto další prvek zabezpečující kybernetickou bezpečnost mimo jiné i na území ČR, svou činností pomáhá k připravenosti EU čelit budoucím kybernetickým nástrahám prostřednictvím sdílení know-how, rozšiřování svých kapacit a povědomí o dané problematice, spoluprací s klíčovými subjekty, přičemž vše jmenované směruje ke zvýšení odolnosti evropské infrastruktury a zajištění digitální bezpečnosti svým občanům. (About ENISA - The European Union Agency for Cybersecurity, 2020)

4.3 CERT a CSIRT týmy

Smysl týmů typu CERT a CSIRT spočívá v samotném zvládání bezpečnostních incidentů a v další související agendě. Týmy jsou předurčeny k okamžité reakci na incidenty v rámci kyberprostoru a jejich síla činí ve vzájemné spolupráci s podobnými týmy napříč celým světem, které si navzájem mezi sebou předávají zkušenosti a nové poznatky, čímž společně vytvářejí postupy pro řešení kybernetických incidentů. (Doucek, Konečný a Novák, 2019)

4.3.1 Vládní CERT

Zřizovatelem vládního CERT týmu je státní instituce NÚKIB, která již byla v rámci bakalářské práce představena, a nese označení GOVCERT.CZ. Hlavním předmětem zájmu vládního CERT týmu je ochraňování kritické informační infrastruktury na území České republiky, jež je stanovena zákonem o kybernetické bezpečnosti, stejně jako zajišťování ochrany na půdě významné informační infrastruktury. Nedílnou úlohou tohoto týmu je taky poskytování bezpečnostních informací veřejnosti i státním orgánům, s čím souvisí i úloha vzdělávání v rámci internetové bezpečnosti. (GOVCERT.CZ, 2021)

4.3.2 Národní CERT

Národní CERT svůj zájem směřuje na všechny uživatele a sítě, které působí na území České republiky. Z toho vyplývá, že národní CERT se stará o kybernetickou bezpečnost běžného provozu internetu. Zřizovatelem není státní instituce, jako tomu je u týmu vládního, ale soukromé sdružení, které je známo pod názvem CZ.NIC, přičemž samotný tým nese název CSIRT.CZ a je složen z 8 členů, kteří jsou zároveň i zaměstnanci sdružení CZ.NIC. Národní CERT je velmi aktivní na poli mezinárodní spolupráce a od roku 2015 je také členem skupiny FIRST. (O týmu CSIRT.CZ, 2011)

4.4 Odolná společnost

Program odolná společnost 4.0. je jeden ze záměrů Národní strategie kybernetické bezpečnosti, což je dokument vydávaný organizací NÚKIB.

„*Jedná se o stav, kdy je celá společnost schopna naplno využívat výhod moderních technologií a současně je schopna integrovat je do svého každodenního života tak, aby byla minimalizována kybernetická rizika*.“ (Národní strategie kybernetické bezpečnosti České republiky, 2020, 19)

Tohoto stavu by se mělo dosáhnout zabezpečením digitální společnosti a veřejné správy, vzděláním, osvětou a rozšiřováním řad specialistů v kybernetickém prostřední. (Národní strategie kybernetické bezpečnosti České republiky, 2020)

5 INTEGROVANÝ ZÁCHRANNÝ SYSTÉM

Základním atributem integrovaného záchranného systému je společný a především koordinovaný postup, který je reprezentován součinností složek IZS při plnění likvidačních a záchranných prací. (Lukáš et al., 2011)

Záchrannými pracemi se rozumí především činnost, která má za cíl odvrátit rizika bezprostředně hrozící a ohrožující životy a zdraví. Naopak likvidační práce nastupují převážně až po skončení mimořádné události a zaměřující se na odstraňování následků. (Lukáš et al., 2011)

5.1 Složky IZS

„*Základní složky integrovaného záchranného systému zajišťují nepřetržitou pohotovost pro příjem ohlášení vzniku mimořádné události, její vyhodnocení a neodkladný zásah v místě mimořádné události. Za tímto účelem rozmísťují své síly a prostředky po celém území České republiky.*“ (Česko, 2000)

Těmito složkami jsou hasičský záchranný sbor, zdravotní záchranná služba a Policie České republiky. Společným rysem těchto složek je skutečnost, že jsou nasazovány pří každé mimořádné události, která vyžaduje režim nutné spolupráce. (Lukáš et al., 2011)

Ostatní složky IZS jsou předurčeny k tomu, že jsou připraveny na vyžádání podílet se na koordinovaném postupu řešení mimořádné události velkého rozsahu nebo při nutnosti specifické činnosti na místě zásahu. (Lukáš et al., 2011)

Těmito složkami se rozumí vyčleněné síly a prostředky ozbrojených sil, ostatní ozbrojené bezpečnostní sbory, ostatní záchranné sbory, orgány ochrany veřejného zdraví, havarijní, pohotovostní, odborné a jiné služby, zařízení civilní ochrany a neziskové organizace a sdružení občanů, která lze využít k záchranným a likvidačním pracím. (Lukáš et al., 2011)

Dominantní postavení mezi složkami IZS náleží hasičskému záchrannému sboru, který plní roli koordinátora složek při společném postupu a z jeho řad je většinou vyčleněn velitel zásahu. (Integrovaný záchranný systém, 2021)

5.2 IZS v kyberprostoru

Na úvod bych se však rád podělil o aktualitu, která velmi souvisí s mým tématem. ZZS hlavního města Prahy totiž počítá se zavedením elektronického hlášení stavu pacienta

z místa zásahu záchranáře prostřednictvím aplikace v tabletu, které zrychlí a ulehčí práci jak samotného záchranáře, tak i dispečerce, neboť doposud se stav o pacientovi hlásil právě telefonicky přes dispečink. Je to další pozitivní krok směrem k digitalizaci státního sektoru. (Kadlecová, 2021)

5.2.1 Operační a informační střediska IZS

Operační a informační střediska IZS, jak již bylo uvedeno výše, jsou činná na operační úrovni a představují stálý orgán, který je zodpovědný za koordinaci složek IZS. Prostřednictvím tísňových linek přijímají a dále zpracovávají informace o mimořádných událostech, a pokud zůstaneme u úkolů souvisejících s kyberprostorem, tak tato střediska slouží jako prostředník pro nepřetržitý tok informací z místa zásahu IZS do krizového štábu a také mezi samotnými krizovými štáby. (Šenovský, Adamec a Hanuška, 2007)

5.2.2 Komunikace v rámci IZS

Informační tok mezi orgány státu, samosprávou a složkami IZS představuje páteř krizové komunikace, která je pochopitelně nezbytná pro přesnou koordinaci složek IZS při společném zásahu nebo příprav na MÚ. Krizová komunikace slouží pro komunikaci mezi složkami, dále pro komunikaci mezi operačními středisky základních a ostatních složek a pochopitelně pro přenos informací z místa zásahu do samotných operačních středisek. (Šenovský, Adamec a Hanuška, 2007)

- **Krizové telefony PEGAS**

  Od roku 2002 poskytlo MV na základě rozhodnutí vlády vedoucím a dalším vybraným členům základních složek IZS krizové telefony, na kterých je v případě krizového stavu bezplatný provoz. (Šenovský, Adamec a Hanuška, 2007)

  Radiová síť Pegas umožňuje členům jednotlivých složek IZS na celém území ČR vzájemnou komunikaci, což velmi usnadňuje jejich činnost v terénu. Tato síť je v ČR budována již od roku 1994. (Šenovský, Adamec a Hanuška, 2007)

- **Hromadné informační prostředky**

  Pro ještě efektivnější možnost zásahu v nastalé mimořádné události slouží povinnost subjektů provozující hromadné informační prostředky poskytnout bez prodlení na žádost operačního střediska IZS informace tykající se mimořádné události, které jsou potřebné pro záchranné a likvidační práce. (Šenovský, Adamec a Hanuška, 2007)

5.2.3 Informační podpora IZS

„*Informační podpora představuje proces (soubor informačních činností) podporující řídící, rozhodovací a poznávací procesy po informační stránce.*“ (Lukáš et al., 2011, 25)

Souborem informačních činností se rozumí různé nakládání s informací, čímž může být zálohování, distribuce, vyhledávání nebo další zpracování. Další pohled na informační podporu je takový, že informační podpora je výsledkem práce informačního systému. (Lukáš et al., 2011)

- **HZS**

  Hasičský záchranný sbor působí jako dominantní prvek IZS, náleží mu status základní složky IZS a v rámci řešení rozsáhlých MU působí jako hlavní koordinátor záchranných a likvidačních prací. HZS byl zřízen v roce 2000 zákonem č. 238/2000 Sb. (Lukáš et al., 2011)

  Základními prvky informační podpory HZS představuje IS TCTV 112, který slouží pro přijímání tísňových hovorů na lince 112 a IS Výjezd, který koordinuje činnost jednotek požární ochrany na operační úrovni. Velmi významnou roli informační podpory HZS také plní GIS, který především pracuje s prostorovými daty. (Lukáš et al., 2011)

- **PČR**

  Prvek IP v rámci PČR je Dispečer – Maják 158, který slouží především k efektivní koordinaci činnosti PČR a rozdělování dostupných sil při zásahu. Systém je běžnou aplikací v rozhraní Windows, která je ovládána operátorem a poskytuje činnosti jako identifikace volajícího, místo události, druh události, výběr sil a prostředků, o kterém rozhoduje operační důstojník, součinnost, servis pro zásah, průběh a konec akce. (Lukáš et al., 2011)

- **ZZS**

  Pro zajištění informační podpory zdravotnické záchranné služby existuje dispečerská aplikace ZZS, která se stará o veškeré náležitosti spjaté se samotným výjezdem a zásahem ZZS. Tato aplikace funguje v součinnosti se systémem TCTV 112 a geografickým informačním systémem. Jednou ze zajímavostí je, že disponuje funkcí, která umí varovat dispečery před problémovými čísly, která v minulosti bez důvodu volali na tísňové volání ZZS. (Lukáš et al., 2011)

6 VYHODNOCENÍ TEORETICKÉ ČÁSTI A POUŽITÉ METODY

6.1 Teoretická část

Teoretická část bakalářské práce měla za úkol demonstrovat provázanost kybernetické bezpečnosti a IZS s přihlédnutím na jeho fungování v rámci kyberprostoru. Taková prezentace obou problematik by měla vést k názorné ukázce jejich vzájemné provázanosti. Jelikož žijeme v době informační, nemůže být pro nikoho překvapením, že kybernetická bezpečnost se postupně dostává do popředí napříč všemi obory, tudíž i v rámci IZS je tento trend patrný.

Informační tok v rámci IZS by nemohl správně fungovat bez optimálně nastavených procesů, bez adekvátních technologií, které informaci a celou IT infrastrukturu chrání, a také bez dobře proškolených lidí, čímž jsem v podstatě vyjmenoval všechny prvky kybernetické bezpečnosti, tedy procesy, technologie a lidé. Pokud by informační tok nefungoval, jednoznačně by nemohl fungovat ani IZS.

Bylo tedy důležité vysvětlit, co je to kybernetická bezpečnost a jakým způsobem může být kybernetická bezpečnost narušena, stejně tak jako vysvětlit, co je to IZS, jak se svým fungováním do kyberprostoru zapojuje, z čehož vyplývá, proč je tedy nezbytné, se v rámci IZS o kybernetické bezpečnosti bavit. Jelikož teoretická část obsahuje všechny výše zmíněné body, můžu ji považovat za dobrý teoretický základ pro psaní praktické části mojí bakalářské práce.

6.2 Použité metody v praktické části

V praktické části bakalářské práce bude použito několik metod analýzy, které v následující podkapitole stručně popíšu.

6.2.1 Vývojový diagram

Pro popis jakéhokoliv procesu, například pracovního, výrobního nebo také pro popis algoritmu v rámci PC programu se hojně využívá vývojový diagram. Samotný proces by mohl být vyjádřen pouze slovy, ale pro lepší porozumění je dobré proces graficky znázornit pomocí unifikovaných znaků, kterými je jednoznačně uvedený začátek a konec procesu včetně veškerých subjektů zasahujících do procesu. Přesně takovýmto grafickým znázorněním procesu se rozumí vývojový digram neboli anglicky flowchart. (Vývojový diagram, 2017)

6.2.2 SWOT analýza

SWOT analýza je velmi často využívaná metoda a díky její univerzálnosti ji lze aplikovat prakticky na cokoliv. Z manažerského pohledu je možno díky ní analyzovat schopnosti člověka, ale i stav celé organizace a v podstatě všechno mezi tím. Analýza se skládá s vnitřní analýzy, ta bere v úvahu slabé a silné stránky organizace, a z vnější analýzy, která hledá příležitosti a hrozby v okolí analyzovaného subjektu. Na základě toho se určuje další směřování daného subjektu. (SWOT analýza, 2020)

6.2.3 FMEA

FMEA je v češtině Analýza možných vad a jejich následků a její kořeny sahají až do šedesátých let minulého století, kdy ji v rámci vesmírného programu APOLLO vyvinula společnost NASA. Běžně se používá anglická zkratka FMEA a cílem této analýzy je vyhledat slabá místa, u kterých je předpoklad, že zde mohou vznikat poruchy nebo vady, které se projeví v celém systému. Analýzu je možno uplatnit na výrobky, ale i na různé procesy a po vyhledání slabých míst se analýza zaměřuje na eliminaci nebo alespoň redukci zjištěných problému. (FMEA (Failure Mode and Effect Analysis), 2021)

6.2.4 ETA

Analýza ETA, český název Analýza stromu události, ve svém výsledku znázorňuje možné scénáře nehody. K těmto scénářům se dojde na základě uvážení různých sekvencí událostí a činností, přičemž je v analýze přihlédnuto i k reakcím lidí a ke správnému zafungování bezpečnostních prvků v procesu. Celá analýza se větví od jedné iniciační události a je grafický znázorněna jako logické větvení na základě dalších příčin, které mohou iniciovat další vývoj procesu směřující k nehodě. (ETA (Event tree analysis), 2015)

6.2.5 FTA

Metoda analýzy zvaná FTA v překladu do češtiny znamená Analýza stromu poruchových stavů a poprvé byla použita v roce 1962, firma Boeing metodu zdokonalila a následně tato metoda našla široké uplatnění při analyzování složitých systémů především v energetice, vesmírném výzkumu a letectví. Jedná se o rozbor tzv. vrcholové události, která znázorňuje nějaký negativní jev jako třeba poruchu. V rámci tohoto rozboru se hledají příčiny vrcholové události. FTA je možno použít preventivně, ale i pro analýzu problému, který již nastal. (FTA (Fault Tree Analysis), 2015)

II. PRAKTICKÁ ČÁST

7 PŘEDMĚT PRAKTICKÉ ČÁSTI

V následujících kapitolách budu psát praktickou část bakalářské práce. Před tím považuji za důležité vysvětlit samotný předmět praktické části.

Bude se tedy jednat o analýzu informačního toku v rámci zdravotnické záchranné služby, kdy jako začátek toku informace je považován samotný telefonát z místa události. Následně se budou brát v úvahu všechny možné proměnné na cestě informace k výjezdové skupině zdravotnické záchranné služby, což bude v rámci praktické části stěžejním subjektem, neboť odtud budu čerpat většinu informací pro analýzu daného procesu. Dále budu mapovat cestu informace od výjezdové skupiny do příjmového nemocničního zařízení až po vykazování výjezdu a poskytnuté lékařské péči pojišťovnám.

V rámci procesu toku informace se v jedné kapitole zaměřím na kybernetickou bezpečnost zajišťovanou konkrétními technologiemi, což je jeden prvek kybernetické bezpečnosti, ale především se praktická část a samotné použité metody analýzy budou věnovat lidem a tomu, jak v rámci informačního toku se samotnou informací nakládají, a samotnému procesu toku informace, čímž zanalyzuji zbylé dva prvky kybernetické bezpečnosti, tedy procesy a lidi.

Prioritním cílem analýzy bude vyhledávání slabých míst a hledání nápravných opatření pomocí metody FMEA. Tato opatření by měla vést k optimalizaci celého procesu toku informace s tím, že se bude především jednat o zrychlení toku informace, na což navazuje i zrychlení poskytnutí lékařské péče. Dále bude tato část zaměřena na předcházení tomu, že informace bude na své cestě jakkoliv pozměněna, což je krajně nežádoucí, jelikož na základě informace se poskytuje adekvátní lékařská péče. Pokud je lékařská péče poskytnuta na základě špatné informace, může to mít fatální následky. Optimalizaci procesu budu demonstrovat v metodě SWOT, která bude zpracována před a po zavedení nápravných opatření vycházejících z analýzy FMEA.

Do analýzy zahrnu i metody FTA a ETA, kde budu brát v potaz jednu konkrétní událost, která v metodě FTA bude reprezentovat vrcholovou událost a budu hledat její příčiny, zatímco v metodě ETA bude ta samá událost reprezentovat iniciaci a na základě dalších proměnných budu hledat možné nehodové scénáře.

Nejprve je však potřeba představit samotnou zdravotnickou záchrannou službu, a to konkrétně ZZS Moravskoslezského kraje a uzemní odbor Ostrava, odkud čerpám veškeré informace v praktické části bakalářské práce.

7.1 ZZS Moravskoslezského kraje

Praktickou část práce zahájím stručným popisem Zdravotnické záchranné služby Moravskoslezského kraje a konkrétně ZZS Ostrava, neboť právě odtud budu čerpat většinu informací použitých v následujících kapitolách.

Počátky ZZS Moravskoslezského kraje sahají do roku 2004, kdy se samostatné záchranné služby tehdejších okresů kraje spojily s Územním střediskem služby Ostrava, a vznikl jeden celek. (Humpl, 2021a)

ZZS Moravskoslezského kraje operuje na území táhnoucí se Jeseníky přes Ostravu až po Beskydy, což z ní dělá jednu z největších ZZS v České republice. Více než 60 posádek ZZS je pochopitelně k dispozici 24 hodin denně, 7 dní v týdnu. Do struktur místní ZZS patří rychlá lékařská pomoc, rychlá zdravotnická pomoc, posádky ranez-vous a letecká záchranná služba, které dohromady poskytují širokou paletu odborné zdravotní péče. (Humpl, 2021a)

7.2 Ostrava

Záchranáři jsou v Ostravě poměrně dost vytíženi, neboť se jedná o třetí největší aglomeraci v České republice, tomu také odpovídá struktura, zázemí, materiální vybavení a personální kapacity ZZS i s přihlédnutím na to, že místní ZZS nemá působnost pouze na katastrálním území Ostravy, ale i ve spoustě přilehlých obcí. (Humpl, 2021b)

ZZS Ostrava disponuje šesti výjezdovými stanovišti, konkrétně Ostrava-Zábřeh, Ostrava-Fifejdy, Ostrava-Poruba, Slezská Ostrava, Ostrava-IVC Jih a areál koncernu AcelorMittal. (Humpl, 2021b)

7.3 ISMS ve zdravotnictví

Je zde důležité podotknout, že v rámci zdravotnictví existuje mezinárodní norma ISO/IEC 27002, která se zabývá systémem řízení bezpečnosti informací právě na půdě zdravotnictví. (Ondrák, Sedlák a Mazálek, 2013)

Tato norma určuje postup kontrol v oblasti řízení informační bezpečnosti ve zdravotnictví a její aplikací by se mělo docílit zabezpečení alespoň na minimální odpovídající úrovni na poměry organizace, která zajišťuje důvěrnost, integritu a dostupnost citlivých informací ve zdravotnictví. Norma udává pravidla pro nakládání s informacemi všeho druhu a také vší formy, což znamená, že nerozlišuje, zda se jedná o informace předány ústně, písemně či prostřednictvím ICT. (Ondrák, Sedlák a Mazálek, 2013)

8 ANALÝZA SOUČASNÉHO STAVU

V následující kapitole budu zpracovávat analýzu současného stavu toku informace v rámci integrovaného záchranného systému a konkrétně v jeho složce Zdravotnické záchranné služby v Ostravě za pomoci pěti různých metod analýzy. Celá analýza bude rozčleněna do několika podkapitol, na základě toho, co bude zrovna předmětem analýzy. V první podkapitole pomocí vývojového diagramu graficky znázorním tok informace z místa mimořádné události až po příjmové zdravotnické zařízení a dál k pojišťovnám.

Následovat bude podkapitola, která podrobně popíše, jak je při současné situaci řešena kybernetická bezpečnost konkrétních prvků procesu z technologického hlediska, tedy jaká technická opatření jsou zde aplikována pro zajištění maximální ochrany informace. V rámci zpracování procesu toku informace a popsání kybernetické bezpečnosti budu vycházet z informací poskytnutých Ing. Radimem Kozelským, který pracuje ve strukturách ZZS Moravskoslezského kraje v IT oddělení a Bc. Milanem Leškem, který pracuje jako záchranář ve strukturách ZZS MSK.

Dále pak v podkapitole „Kybernetická bezpečnost procesu“ použiji i odbornou literaturu, za jejíž pomoci popíšu konkrétní technická opatření kybernetické bezpečnosti procesu a také funkci, kterou v procesu plní.

Poté přistoupím k metodě FMEA, kterou již budu konzultovat se členem výjezdové skupiny ZZS Moravskoslezského kraje, konkrétně ZZS v Porubě a na základě vad zjištěných metodou FMEA a procesu toku informace sestavím SWOT analýzu současného stavu, která bude zakončena vyjádřením současného stavu průsečíkem mezi hodnotami na ose X a Y a zasazení stavu do příslušného kvadrantu s vysvětlením.

Jednu konkrétní zjištěnou vadu z metody FMEA dále rozvedu metodou FTA a ETA, přičemž to bude zpracováno opět za spolupráce se členem výjezdové skupiny v Porubě, kdy výjezdovou skupinu, potažmo špatnou informaci pro výjezdovou skupinu, položíme doprostřed mezi metody FTA a ETA budeme hledat příčiny, proč se tak stalo, a následky, které mohou za přispěním vícero proměnných nastat. Tím bych následně ukončil analýzu současného stavu a pokračoval bych dál do kapitoly „Nápravná opatření“, ve které budu opět zpracovávat další analýzy.

8.1 Proces toku informace

Tato podkapitola mapuje tok informace a všechny subjekty, které s informací přicházejí do styku. Samotný vývojový diagram bude přiložen na konci podkapitoly a bude mu předcházet slovní popis procesu a vysvětlení podstatných částí diagramu, což je potřeba pro jeho plné pochopení, neboť je to moje subjektivní grafické vyjádření toku informace v rámci ZZS Moravskoslezského kraje. Všechny informace však pocházejí ze spolupráce mezi mnou a Ing. Radimem Kozelským, což bude uvedeno pod samotným grafem i v seznamu použité literatury, a proto v textu samotném nebude zdroj uveden, neboť veškeré informace uvedené v textu vycházejí z daného grafu, který bude ocitován. Dále také čerpám informace z osobního rozhovoru ze dne 1. 3. 2021 s Bc. Milanem Leškem, který je příslušníkem výjezdové skupiny v rámci ZZS MSK. Na veškeré informace čerpané z toho rozhovoru upozorním předem v textu a v grafickém znázornění je vyjádřen fialovou barvou.

Je potřeba podotknout, že všechny červené šipky znamenají hlavní tok informace, zatímco oranžové šipky znázorňují cestu sdílení informace s potřebnými subjekty. Pak v grafu jsou ještě šipky černé, které vyjadřují příslušnost subjektu zasahujícího do procesu k danému pracovišti nebo zřizovateli. V šedých obdélnících se nacházejí právě tato pracoviště a taky zřizovatelé, u kterých je naznačena příslušnost k danému subjektu. Oranžové obdélníky znázorňují subjekty, se kterými se sdílí informace v rámci celého procesu. A nakonec červené obdélníky znázorňují potenciální slabá místa, kde může nastat zdržení celého toku informace nebo také ovlivnění obsahu informace. Tato potenciální slabá místa budou následně předmětem metody analýzy FMEA.

Vznikem informace se v procesu rozumí telefonický hovor z místa události. Vytočením čísla 112 se hovor spojí s **TCTV**, což znamená „Telefonické centrum tísňového volání“. TCTV se dělí na Centrum tísně a Centrum operačního řízení. V rámci TCTV se volající nejprve dostane do kontaktu s tzv. **Call takerem**, který se snaží volající osobu co nejvíce vytěžit a na základě získaných informací poté v informačním systému **založí událost**, přičemž navrhuje řešení dané události a složení výjezdové skupiny. Tohle všechno se děje v **Centru tísně** a je nezbytné, aby informace byla co nejrychleji postoupena do **Centra operačního řízení**, kde si ji přebírá **Dispečer OŘ**.

Dispečer OŘ už následně pracuje v **aplikaci Dispečer**, která tvoří jeho pracovní prostředí v kyberprostoru. V rámci aplikace se informace promítne i v **GIS**, neboli v Geografickém informačním systému, což je velmi důležité pro přesné identifikování místa

události a pro orientaci výjezdové skupiny. Dispečer OŘ má také k dispozici **panel ovládání technologií**, jehož prostřednictvím je schopný s výjezdovou skupinou udržovat fonetický kontakt za pomoci jakékoliv integrované radiostanice a je tedy možné například aktualizovat informace z místa události přímo výjezdové skupině ještě před jejich příjezdem.

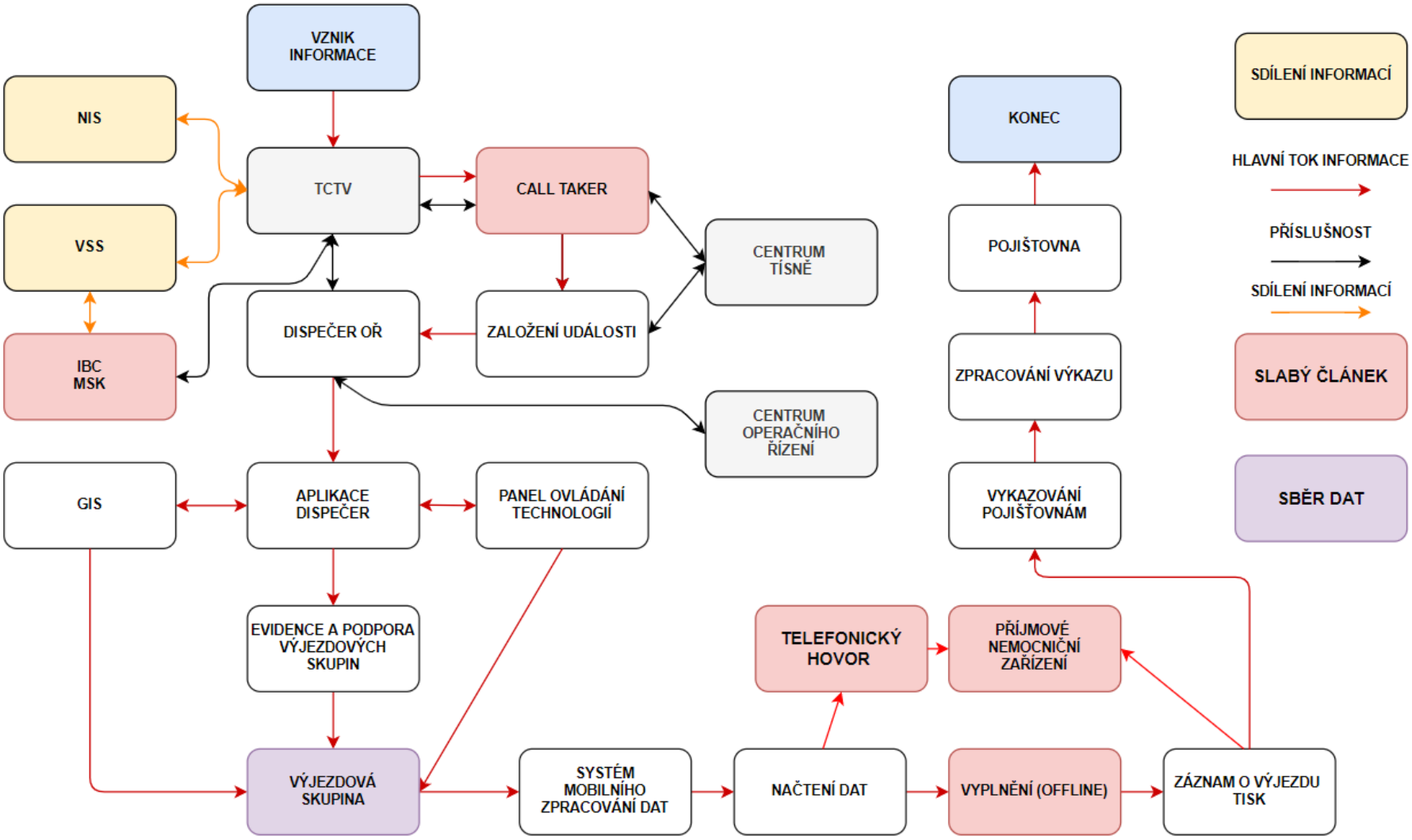
Zatímco se všechno tohle děje v rámci TCTV, tak probíhá i sdílení informací od TCTV do **VSS** (Vrstva společných služeb), což je software zajišťující sdílení informace s **IBC MSK** (Integrované bezpečnostní centrum Moravskoslezského kraje), a to je nesmírně důležité při řešení mimořádné události, na které se podílí více složek IZS, jelikož právě IBC MSK, jehož součástí je i TCTV, koordinuje všechny složky IZS na území Moravskoslezského kraje. Dále se informace z TCTV sdílejí i do NIS (Nemocniční informační systém), prostřednictvím něhož se informace o mimořádné události sdílí se všemi IZS na území ČR.

Dispečer OŘ za pomoci systému **Evidence a podpory výjezdových skupin** sestaví adekvátní posádku, přepošle informace o události na pracoviště výjezdové skupiny a zároveň provede zvukovou signalizaci na pracovišti výjezdové skupiny.

Následující informace jsem již získal z osobního rozhovoru mezi mnou a příslušníkem výjezdové skupiny ve strukturách ZZS MSK, Bc. Milanem Leškem. **Výjezdová skupina** si informace načte do **Systému mobilního zpracování dat** neboli „MobileDoc“, který umožňuje tvorbu zdravotnické dokumentace přímo v terénu. Výjezdová skupina vyplňuje informace **offline** a následně přímo v terénu nebo v příjmovém nemocničním zařízení tiskne **záznam o výjezdu.** Informace o stavu pacienta a nastalé situaci s příjmovým nemocničním zařízením, které vybírá na základě principu nejbližšího vhodného nemocničního zařízení, vyřizuje telefonicky.

Tuto větev toku informace ukončíme u subjektu příjmové nemocniční zařízení, avšak je patrné, že v rámci struktur daného zařízení se s informací pracuje dál až do podání adekvátní lékařské péče.

U posledního odstavce se vrátím k čerpání informací od Ing. Radima Kozelského. Graf zpracovaný v rámci této podkapitoly ještě znázorňuje tok informace, kterým se vykazuje daný výjezd o poskytnutí lékařské péče v rámci výjezdu zdravotním pojišťovnám. Ze záznamu o výjezdu informace putuje do systému **Vykazování pojišťovnám**, kde se provádí **zpracování výkazu**, které se následně předává **pojišťovnám,** a tím bych tento proces toku informace ukončil.



Obrázek 2 - Tok informace - současný stav (Kozelský, 2020)

8.2 Kybernetická bezpečnost procesu

První z důležitých opatření spadajících do kybernetické bezpečnosti je řešení technologického sálu, ve kterém se nachází IT technologie. Specifikum řešení je takové, že technologický sál existuje ve dvou naprosto stejných provedeních fungujících současně a nezávisle na sobě, což zabezpečuje **zálohování dat** již v průběhu jejich načítání do systému. Duplikace technologického sálu taktéž poskytuje vysokou úroveň **fyzické bezpečnosti** a v podstatě funguje i jako **redundance** technologického vybavení v případě, kdy je jeden ze sálů vyřazen z provozu. (Kozelský, 2020)

Kybernetické bezpečnosti analyzovaného procesu toku informace jistě napomáhá i fakt, že v rámci procesu se využívá systém CUCM, prostřednictvím něhož je možné využívat paketová telefonní síťová zařízení. Tento systém má v sobě zakomponovanou funkci pro **zálohování a obnovení**. Je to tedy další cesta jak zálohovat cenná data, ale především systém poskytuje možnost obnovení dat po havárii. (Kozelský, 2020)

Postupně se dostávám k aplikačním serverům ve struktuře IBC MSK, které zajišťují chod aplikací. Pro ZZS se jedná především o aplikaci Dispečer, ve které pracuje dispečer OŘ. Jedním z dalších opatření spadajících do kybernetické bezpečnosti je nutnost **autentizace a autorizace**, bez čehož aplikační server neumožní uživateli pracovat se softwarem. (Kozelský, 2020)

Využívání klastrového softwaru Oracle Clusterware přispívá k dalšímu zesílení kybernetické bezpečnosti celého systému. Tento software poskytuje **klastrování** na úrovni operačního systému a je vybaven zcela autonomním řízením, zabezpečením a opravami, což vylučuje selhání lidského faktoru. Další užitečnou funkcí je možnost uložení dat na vzdálené servery neboli **cloudy**. (Kozelský, 2020)

Softwarové pracovní prostředí výjezdové skupiny představuje Systém mobilního zpracování dat, který například umožňuje **synchronizaci** dat se serverem, díky čemuž je možné s daty pracovat i v režimu offline. (Kozelský, 2020)

Aby nedocházelo k narušování komunikace uvnitř analyzovaného procesu, je přístup nežádoucích zařízení z vnějšího okolí vyloučen využitím mobilní **VPN**. Pokud je nutné, aby komunikace běžela bez použití VPN přes internet, je bezpečnost řešena za pomoci **hesla** a **klientského certifikátu**. Dále je možné ze systému vzdáleně vyřadit jakékoliv koncové

zařízení, které by mohlo být kompromitováno třetí stranou. Zneužití dat uložených na koncových zařízeních by mělo být vyloučeno použitím **šifrování**. (Kozelský, 2020)

Pro kompletní pochopení komunikace v rámci analyzovaného procesu přikládám definici VPN.

„*VPN je mechanismus (nebo metoda) umožňující propojení počítačových systémů prostřednictvím nedůvěryhodné (např. veřejné) počítačové sítě tak, že propojené počítačové systémy mezi sebou budou moci komunikovat, jako by byly propojeny v rámci důvěryhodné (uzavřené privátní) sítě. Tyto počítačové systémy ověřují svoji totožnost (např. pomocí certifikátů, hesla aj.) a po vzájemné autentizaci je komunikace mezi těmito privátně propojenými počítači šifrována.*“ (Kolouch, 2016, 69)

Pro zajištění maximální ochrany koncových zařízení, jsou tato zařízení vybavena **automatickým aktualizováním** softwaru, což pochopitelně zaručuje i optimální chod zařízení a minimalizuje to manuální zásahy do zařízení. (Kozelský, 2020)

Tímto bych analýzu kybernetické bezpečnosti z pohledu technických opatření ukončil a přistoupím k samotným metodám analýzy, kde předmětem těchto metod jsou především lidé a procesy s cílem najít slabá místa, která již byla naznačena ve vývojovém diagramu, a pokusit se tato slabá místa eliminovat nebo alespoň zmírnit pomocí nápravných opatření.

8.3 FMEA

První z použitých metod představím analýzu FMEA, na základě které jsem hledal slabá místa v procesu a přiřazoval. Prvky procesu, ve kterých jsem našel možné slabé místo, jsou ve vývojovém diagramu zaznačeny červenou barvou.

Metodou FMEA jsem zjistil následující vady, ke kterým může v rámci procesu docházet. Nesdílení dat systému MobileDoc, což je jiný název pro Systém mobilního zpracování dat, který při své práci v terénu využívá výjezdová skupina. Špatná kvalita hovoru, při nutnosti využití telefonického hovoru výjezdovou skupinou. Špatné zpracování informace v rámci MobileDoc výjezdovou skupinou, kde jsem narazil na první možné lidské selhání. Mezi lidské selhání patří i možnost špatné intepretace vytěžených informací od Call-takera. Další vada je absence zajišťování příjmového nemocničního zařízení pro výjezdovou skupinu. K těmto hodnotám jsem přiřadil veličiny významu, výskytu a možnosti odhalení vady. Jednoduchým výpočtem se z těchto veličin dostávám k rizikovému číslu, které se budu snažit prostřednictvím nápravných opatření snížit.

Tabulka 1 – FMEA - současný stav

Současný stav								
Prvek procesu	Možná vada	Možné následky	Význam	Možné příčiny	Výskyt	Stávající opatření k odhalení	Odhalitelnost	Rizikové číslo
MobileDoc	Nesdílení dat	Vyšší riziko zhoršení stavu pacienta	**8**	Nevyužití potenciálu systému	**10**	Žádné	**1**	**80**
Telefonický hovor	Špatná kvalita hovoru	Zkreslení a zpomalení informace	**5**	Špatný signál nebo telefon	**8**	Pokrytí signálem	**1**	**40**
Výjezdová skupina	Špatné zpracování informace	Špatné směřování pacienta	**10**	Neodpovídající znalosti	**4**	Pravidelné školení zaměstnanců	**2**	**80**
Call taker	Špatná interpretace vytěžených informací	Neadekvátní reakce na vzniklou situaci	**8**	Špatné komunikační dovednosti dispečera	**2**	Výběrové řízení	**2**	**32**
IBC MSK	Nezajištění příjmového zařízení pro VS	Komplikace při předávání pacienta	**6**	V MSK tento systém není zaveden	**10**	Žádné	**1**	**60**

- **Nesdílení dat**

  Nesdílení dat ze systému MobileDoc k příjmovému nemocničnímu zařízení je poměrně významná vada, neboť to zpomaluje celý tok informace. Výskyt je tady maximální, protože se tato funkce jednoduše nepoužívá a odhalení je ohodnoceno minimální veličinou, neboť je velmi snadné, funkce se prostě nevyužívá.

- **Špatná kvalita hovoru**

  Špatnou kvalitou hovoru se může zásadně zkreslit informace, ale výjezdová skupina je schopná zajistit, aby i přesto příjmové zařízení dostalo informaci o pacientovi v pořádku, a proto nemá tato vada zásadní význam. Na základě rozhovoru jsem zjistil, že špatná kvalita hovoru je poměrně častý jev, tudíž zde je veličina vysoká. Zjistit skutečnost, že kvalita hovoru je na nízké úrovni nedá moc práce, což vysvětluje nízkou příslušnou veličinu.

- **Špatné zpracování informace**

  Tato vada může mít dost fatální následky pro pacienta, protože se na základě této informace dále postupuje v příjmovém nemocničním zařízení, a tudíž tomu odpovídá i přiřazená veličina. Výskyt tohoto problému není tak častý, ale odhalit tento problém může být trochu obtížnější.

- **Špatná interpretace vytěžených informací**

  Problém, který může zásadně ovlivnit prvotní reakci na nastalou situaci, neboť na základě informací z tísňového centra se sestavuje výjezdová skupina a určuje i naléhavost případu, což je pro výjezdovou skupinu stěžejní informace. Výskyt takového problému naštěstí není moc častý, ale odhalení nastává až při příjezdu výjezdové skupiny a vzniká zde teda značné časové prodlení.

- **Nezajištění příjmového zařízení pro VS**

  Diskutabilní problém, ve kterém vidím spíš možnost, jak věci dělat jinak a možná trochu efektivněji. Každopádně v rámci ZZS MSK taková možnost není a výjezdová skupina si musí příjmové zařízení zajistit sama, proto jsem přiřadil maximální veličinu u výskytu.

Všechny informace implementované do metody analýzy FMEA pocházejí z rozhovoru mezi mnou a Bc. Milanem Leškem ze dne 1. 3. 2021.

8.4 SWOT analýza procesu

V následující podkapitole vyjádřím pomocí SWOT analýzy současný stav procesu toku informace v rámci ZZS MSK. Krátce představím hodnoty, které jsem do analýzy zakomponoval. Výsledkem SWOT analýzy bude grafické vyjádření současné situace, ke kterému opět přiložím slovní vysvětlení.

Všechny zakomponované hodnoty v následující analýze včetně jim přisouzených veličin jsem konzultoval s Bc. Milanem Leškem a pocházejí tedy s již uvedeného rozhovoru mezi mnou a ním ze dne 1. 3. 2021.

8.4.1 SWOT analýza - tabulka

Tabulku mám rozdělenou do čtyř kvadrantů, tedy S (silné stránky), W (slabé stránky), O (příležitosti) a T (hrozby). Kvadranty S a W společně tvoří vnitřní analýzu procesu a kvadranty O a T reprezentují vnější analýzu. Ke každé hodnotě jsem přiřadil body, na základě nichž určuji závažnost/užitečnost, a následně jsem přiřadil i váhy, které definují důležitost dané hodnoty v porovnání s ostatními hodnotami ve stejném kvadrantu. Z toho jsem schopný spočítat výsledek silných a slabých stránek, na základě čehož určím výsledek vnitřní analýzy. Analogicky spočítám i vnější analýzu a veličiny následně zobrazím v grafu.

Tabulka 2 - SWOT analýza - současný stav

SWOT								
	STRENGHTS				WEAKNESSES			
VNITŘNÍ ANALÝZA		Body	Váha	Součin		Body	Váha	Součin
	Dostupnost tísňové linky	5	0.6	3	Nesdílení dat	-5	0.3	-1.5
	GIS	4	0.2	0.8	Telefonický hovor	-4	0.3	-1.2
	Kybernetické zabezpečení	4	0.2	0.8	Nedostatečné zpracování dat VS	-5	0.4	-2
		Součet =		4.6		Součet =		4.7
	Výsledek vnitřní analýzy = 4.6 - 4.7 = -0.1							
	OPPORTUNITIES				THREATS			
VNĚJŠÍ ANALÝZA		Body	Váha	Součin		Body	Váha	Součin
	Silné pokrytí mobilní sítí	4	0.4	1.6	Cílové zařízení	-3	0.2	-0.6
	Komunikační schopnosti dis.	5	0.4	2	Komunikační schopnosti dis.	-5	0.3	-1.5
	Informovanost veřejnosti	4	0.2	0.8	Zneužití/zahlcení tísňové linky	-5	0.5	-2.5
		Součet =		4.4		Součet =		4.6
	Výsledek vnější analýzy = 4.4 - 4.6 = -0.2							

- **Silné stránky**

  Do silných stránek jsem vložil dostupnost tísňové linky, GIS a kybernetickou bezpečnost. Dostupnost tísňové linky je v ČR na velmi vysoké úrovni a je možné se na ni dovolat dokonce bez toho, aniž by telefon byl na místě, kde má od svého operátora k dispozici signál. GIS, myšleno Geografický informační systém, který je zakomponovaný v aplikaci Dispečer, je rozhodně silnou stránkou, neboť napomáhá k rychlé a spolehlivé lokalizaci místa události a jednoznačnému nasměrování výjezdové skupiny. Kybernetickou bezpečnost celého procesu jsem představil v minulé podkapitole a z mého pohledu je velmi kvalitní.

- **Slabé stránky**

  Do slabých stránek jsem musel zakomponovat neschopnost sdílení dat MobileDoc z příjmovým nemocničním zařízením, což jsem zjistil v rámci metody analýzy FMEA. S nesdílením dat souvisí i nadbytečné využívání telefonického hovoru za účelem poskytnutí informací o pacientovi do příjmového zařízení. Veličiny přiřazené k této hodnotě ukazují situaci, kdy telefonický hovor zbytečně zdržuje výjezdovou skupinu od práce, potažmo situaci, kdy se výjezdová skupina kvůli nekvalitnímu vybavení nemůže spojit s cílovým zařízením nebo je kvalita hovoru špatná. To bylo opět zjištěno metodou analýzy FMEA, stejně jako poslední slabá stránka, kterou je nedostatečné zpracování dat výjezdovou skupinou. Veličiny uvedené u poslední slabé stránky odpovídají situaci, kdy se tak opravdu stane, což není úplně častá situace, ale ve SWOT analýze jsem i tohle musel zvážit.

- **Příležitosti**

  Mezi příležitosti řadím rozhodně dobré mobilní sítě, jelikož analyzuji situaci v Ostravě, kde je pokrytí na vysoké úrovni. Napomáhá to k dobré kvalitě hovoru mezi volajícím a dispečerem, díky čemuž by nemělo docházet ke zkreslení informace. Komunikační schopnosti dispečera můžou být pro celý proces jak příležitostí, tak i hrozbou, a proto je tato hodnota přiřazena do obou kvadrantů se stejným bodovým ohodnocením. Informovaností veřejnosti mám zde na mysli povědomí o telefonních číslech a možnosti volat ZZS v situacích, kdy je to potřeba.

- **Hrozby**

  Hrozbou ve smyslu cílového zařízení jsou myšlena nejednotná pravidla o převzetí pacienta od výjezdové skupiny, na základě čehož je vymyšleno jedno z nápravných opatření. Situace, kdy komunikační dovednosti dispečera jsou na špatné úrovni a představují tím hrozbu, může zásadně ovlivnit původní znění informace od volajícího. Je to další ze slabých stránek, na které budu aplikovat nápravné opatření.

  Zneužívání nebo zahlcování tísňových linek je bohužel velmi závažný problém a především hrozba z vnějšího okolí, která zásadním způsobem ohrozí analyzovaný proces, protože se v tu chvíli může stát nedostupným pro kohokoliv, kdo opravdu potřebuje využít pomoci ZZS. Je to problém, který jsem musel do analýzy zakomponovat, neboť existuje v podstatě na denní bázi, ale dále ho rozvádět nebudu, stejně tako jako na něj nebudu aplikovat žádné nápravné opatření. Jedná se o situaci, kdy někdo na tísňovou linku volá s vymyšlenou informací nebo o situaci, která je mnohem častější, kdy si lidé přivolávají výjezdovou skupinu ZZS kvůli naprostým banalitám, se kterými by se do nemocnice na vyšetření mohli dostavit po vlastní ose. V tomto případě nejenže dočasně zahltí tísňovou linku zbytečností, ale především zaměstná výjezdovou skupinu ZZS, která v té chvíli může být potřebná na místě, kde jde o záchranu lidského života, což je jejich prioritní poslání.

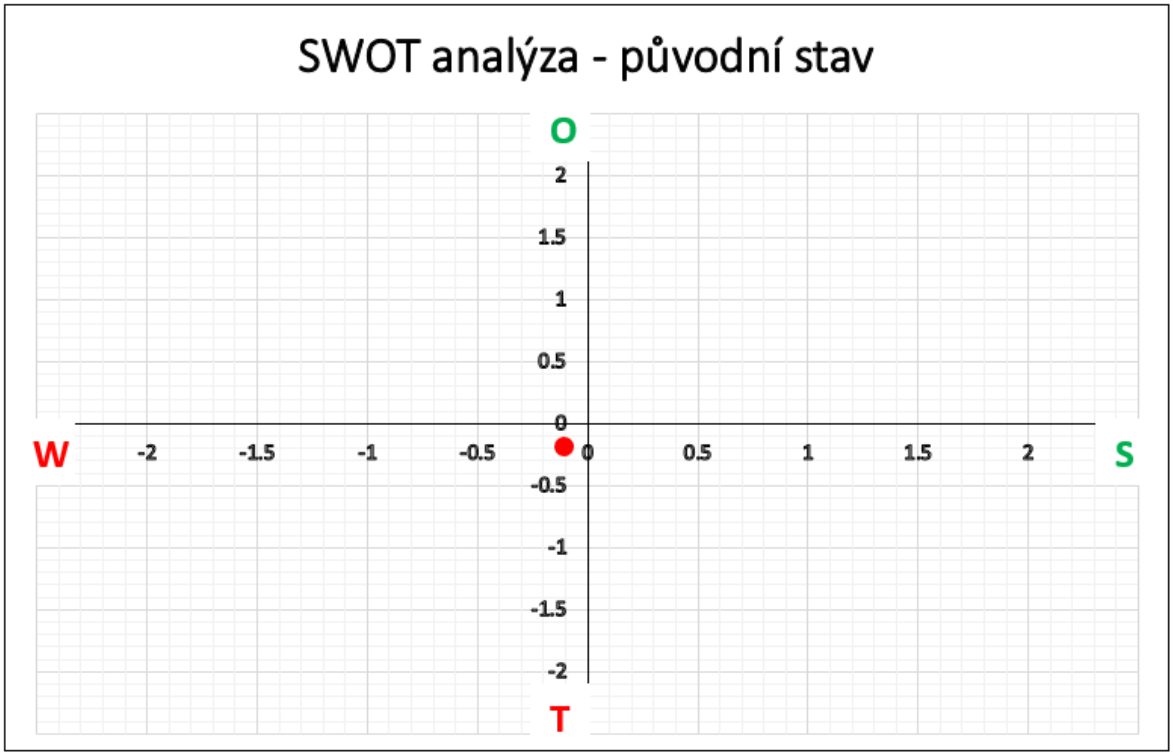
8.4.2 SWOT analýza - graf

Nyní již na základě spočítaných veličin u dodaných hodnot ze SWOT analýzy následuje graf, který ukazuje výsledek současného stavu. Ke grafu je však důležité podotknout, že tento výsledek reprezentuje situaci, kdy se vyskytne řetězec vícera špatných událostí. Je tím myšleno především to, že ve slabých stránkách je při nutnosti telefonického hovoru špatná kvalita hovoru nebo se s příjmovým zařízením nelze spojit vůbec a výjezdová skupina špatně zpracuje data do systému MobileDoc, stejně tak jako v kvadrantu hrozby dochází k situaci, že komunikační schopnosti dispečera nejsou na vysoké úrovni a samotná prvotní informaci je tím pádem již zkreslená. Jedná se tedy o situaci, kdy je všechno špatně, a proto se výsledek nachází v kvadrantu WT, což je v podstatě ta nejhorší možnost.

Nejedná se tedy o každodenní současný stav. Je nezbytné říct, že na základně mnou získaných informací z rozhovoru, který mi poskytl Bc. Milan Leško dne 1. 3. 2021, jsem nabyl dojmu, že fungování výjezdových skupin ZZS MSK na území města Ostravy je na

vysoké úrovni, pacientům je zde poskytována adekvátní lékařská péče a to vše díky profesionálnímu přístupu záchranářů a všeho personálu.

Nyní již následuje samotný graf, kde je výsledek zaznačen červeným bodem v kvadrantu WT.



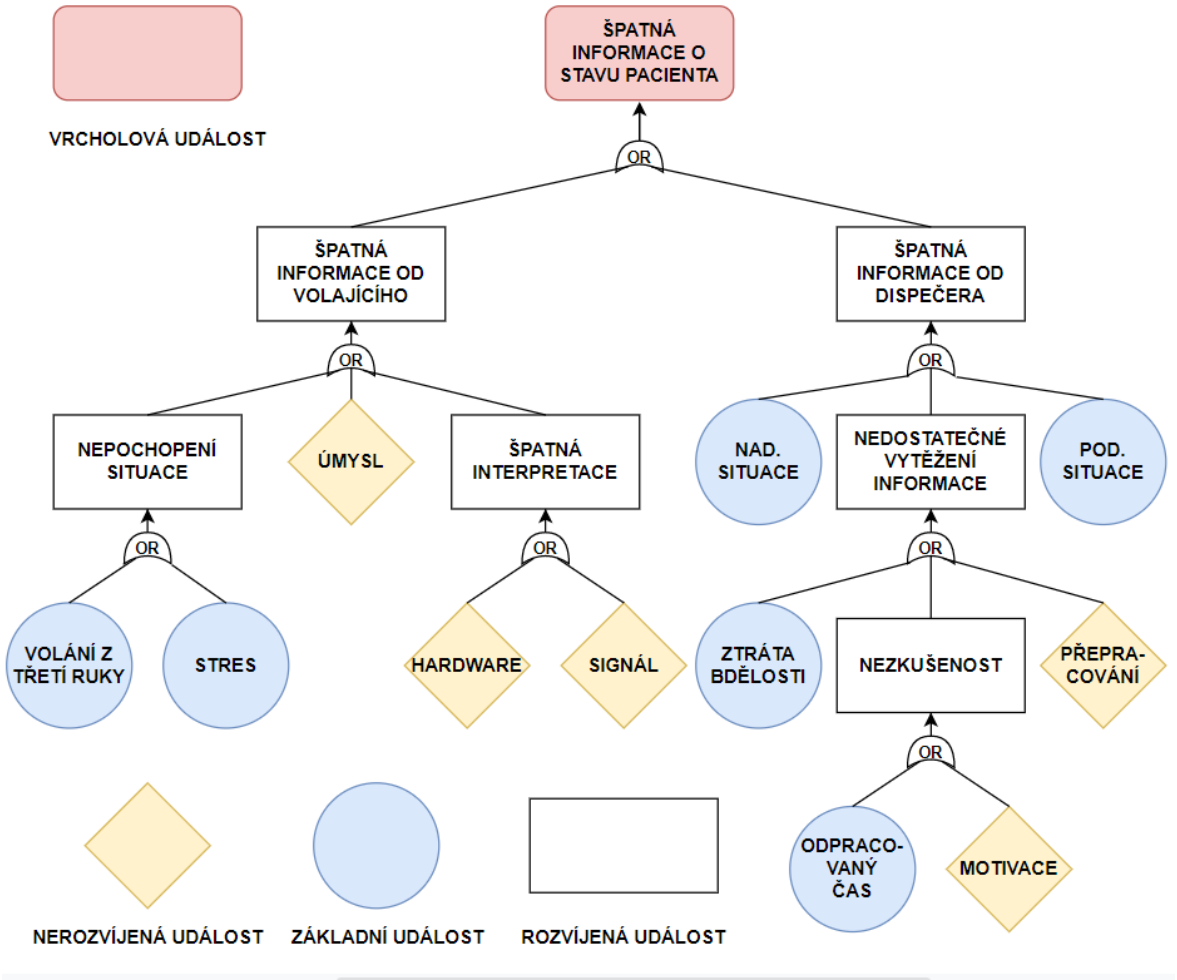
Obrázek 3 - Graf SWOT - současný stav

8.5 FTA

V následujících dvou podkapitolách již přistupuji k analýze konkrétní situace pomocí dvou podobných metod analýzy. V metodě FTA jsem vybral jako vrcholovou událost špatnou informaci o stavu pacienta poskytnutou výjezdové skupině a cílem je zjistit možné příčiny, proč se tomu tak stalo.

Tohle je poměrně závažný problém, který může ovlivnit reakci na vzniklou situaci výjezdovou skupinou, což v krajním případě vede až ke smrti pacienta, a proto jsem situaci vybral jako vrcholovou událost, kterou podrobím důkladnější analýze.

Všechny informace implementované do metody analýzy FTA pocházejí z rozhovoru mezi mnou a Bc. Milanem Leškem ze dne 1. 3. 2021.



Obrázek 4 – FTA

Graf popíšu a vysvětlím uvedené hodnoty v něm. Vrcholovou událostí je tedy špatná informace o stavu pacienta pro výjezdovou skupinu a poté se graf dělí do dvou větví. Každé větvení je krokem o jeden stupeň blíže k základní příčině.

8.5.1 Špatná informace od volajícího

Při hledání příčin špatné informace od volajícího jsem došel k závěru, že se tak může stát nejméně ze tří zde uvedených důvodů. Jeden z důvodů je **nepochopení situace** osobou, která na tísňovou linku volá, což bude dál rozebíráno. **Úmysl** mám v grafu zaznačený jako dále nerozvíjenou událost a je to další z důvodů, proč může dojít ke špatné informaci od volajícího. Posledním zakresleným důvodem je **špatná interpretace**, tím je myšleno, že volající situaci sice správně pochopil a chce tyto informace předat dál, ale kvůli negativnímu přispění vnějších vlivů dochází ke zkreslení informace.

- **Nepochopení situace**

  Nepochopení situace volající osobou může nastat na základě mých úvah nejméně ze dvou důvodů, kterými jsou **volání z třetí ruky** a **stres**. Stres je při mimořádných událostí poměrně častým jevem a může se stát, že kvůli němu člověk situaci ne zcela pochopí, což vede ke zkreslení informace poskytované tísňové lince.

  Zde je třeba podotknout, že existují tři druhy volání na tísňovou linku. **Volání z prvni ruky** znamená, že informaci oznamuje postižená osoba. **Volání z druhé ruky** provádí člověk, který je na místě s postiženou osobou. **Volání z třetí ruky** je situace, kdy informaci oznamuje člověk, který vůbec není přítomen v místě události.

- **Špatná interpretace**

  Špatná interpretace informace z místa události může nastat kvůli tomu, že **hardware**, tedy ve většině případů mobilní telefon, může být rozbitý, což znemožní kvalitní hovor. Druhým zde uvedeným důvodem je **ztráta signálu** na takové úrovni, že není možné se dovolat ani na tísňovou linku.

8.5.2 Špatná informace od dispečera

Další rozvíjenou větví směrem od vrcholové události je špatná informace od dispečera. Zde hledám příčiny v **nadhodnocení** nebo **podhodnocení** situace, což jsem vyobrazil jako základní událost a je možné tyto příčiny schovat pod pojem špatný úsudek. Další příčinou může být **nedostatečné vytěžení informace dispečerem**.

- **Nedostatečné vytěžení informace**

  Nedostatečně vytěžení informace dispečerem jsem si vybral jako příčinu, kterou dále rozvíjím. Zde hledám příčinu ve chvilkové **ztrátě bdělosti**, což může vyústit v opomenutí nějakého důležitého dotazu. Dále hledám příčinu v **přepracování personálu**, což nechávám jako nerozvíjenou událost. Poslední mnou zvažovanou příčinou může být **nezkušenost** dispečera, jež bude dál rozvedena.

- **Nezkušenost**

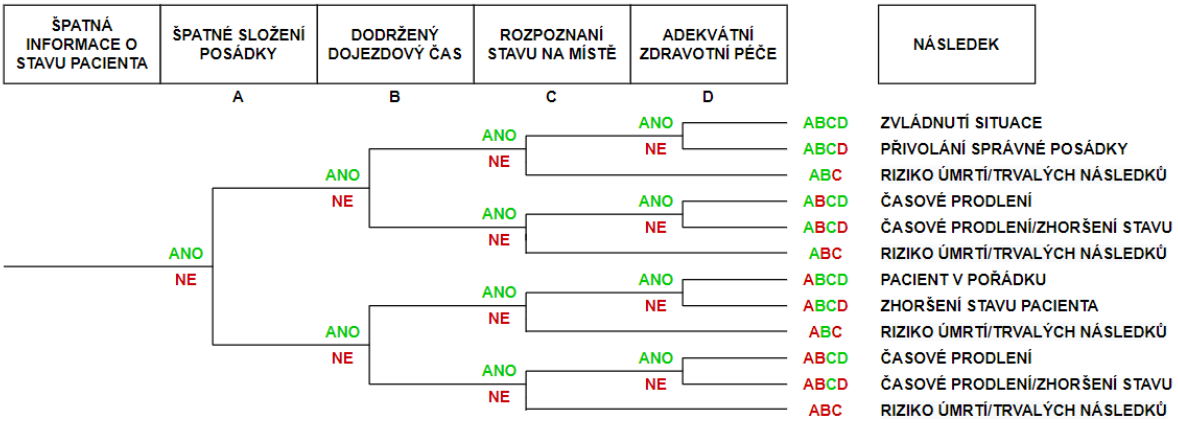
  Nezkušenost může pramenit pochopitelně z nedostatečné **odpracované doby**, ovšem bral jsem v úvahu i ztrátu **motivace** učit se novým věcem a zdokonalovat se v komunikačních dovednostech, což může vyústit v zakrnění a tedy v nezkušenost.

8.6 ETA

V metodě analýzy ETA budu vycházet ze stejné události jako v FTA s tím rozdílem, že nyní mi špatná informace o stavu pacienta bude reprezentovat iniciační událost a mým úkolem je na základě uvážení dalších kroků, ke kterým může dojít, a rozhodovacích procesů v nich, hledat možné následky, potažmo nehodové scénáře, které k těmto následkům vedou.

V mojí metodě se k nehodovému scénáři dostáváme přes čtyři rozhodovací procesy, na základě nichž se graf dál větví. Jsou to následující aspekty: Došlo ke špatnému složení posádky? Byl dodržen dojezdový čas? Byl rozpoznán stav pacienta na místě? Byla poskytnuta adekvátní zdravotní péče?

Všechny informace implementované do metody analýzy ETA pocházejí z rozhovoru mezi mnou a Bc. Milanem Leškem ze dne 1. 3. 2021.



Obrázek 5 – ETA

8.6.1 Špatné složení posádky

Na základě špatné informace o stavu pacienta poskytnuté call takerem může dojít ke složení nedostačující posádky výjezdové skupiny. Tento bod jsem zařadil jako první rozhodovací proces, ale je třeba si uvědomit, že na tohle nemá výjezdová skupina žádný vliv narozdíl od následujících rozhodovacích procesů. Špatné složení posádky může vést k neschopnosti podat adekvátní lékařskou péči, což může mít samozřejmě pro pacienta i fatální následky.

8.6.2 Dojezdový čas

Při poskytnutí špatné informace o stavu pacienta může být vyhodnoceno, že naléhavost případu není na takové úrovni, jakou reálná situace vyžaduje, to může zapříčinit nedodržení dojezdového času. Je to způsobeno tím, že na základě naléhavosti případu se řidič výjezdové skupiny řídí různými pravidly chování v provozu a využívání majáků.

8.6.3 Rozpoznání stavu na místě

V případě, že výjezdové skupině byla poskytnuta špatná informace o stavu pacienta, zůstává pouze na nich, zda jsou schopni na místě události rozpoznat skutečný stav pacienta a tím pádem poskytnou adekvátní péči.

8.6.4 Adekvátní zdravotní péče

Pokud výjezdová skupina není schopna poznat skutečný stav pacienta na místě události, je víceméně jasné, že nedojde ani k poskytnutí adekvátní zdravotní péče, a proto jsem graf tímto směrem již dál nevětvil. V případě, že výjezdová skupina rozpozná stav pacienta v terénu, nastává otázka, zda adekvátní zdravotní péči opravdu poskytla.

8.6.5 Následky

Na základě větvení, které se odvíjí od splnění či nesplnění daných podmínek, se dostáváme k následkům řetězce události. Tyto následky jsou odlišeny barvou písma na základě toho, kterou z podmínek splnil (zelená) či nesplnil (červená), a jedná se o nehodový scénář.

- **Nejlepší scénář**

  Pokud v rámci řetězce událostí po poskytnutí špatné informace výjezdové skupině nedojde ke špatnému složení posádky, je dodržen dojezdový čas na místo události, výjezdová skupina rozpozná skutečný stav pacienta na místě a poskytne adekvátní zdravotní péči, je pacient v pořádku (bereme-li v úvahu, že se nejedná o zranění neslučitelné se životem) a výjezdová skupina může považovat svoji práci za splněnou. Tento scénář značíme: **ABCD**

- **Nejhorší scénář**

  Zcela nejhorší scénář nastává, když je špatně složená výjezdová skupina, není dodržen dojezdový čas, výjezdová skupina nerozpozná skutečný stav pacienta, a tedy ani neposkytne adekvátní zdravotní péči. Nastává scénář: **ABCD**

9 NÁPRAVNÁ OPATŘENÍ

Následující kapitola obsahuje výpis navrhovaných nápravných opatření s bližším vysvětlením toho, kam dané nápravné opatření v rámci celého analyzovaného procesu bude zasazeno a jakým způsobem by mělo fungovat.

Implementaci navrhovaných nápravných opatření do procesu vyjádřím stejně, jako tomu bylo u procesu současného stavu, vývojovým diagramem, který doplním i slovním vysvětlením v podobě textu.

Celý proces následně podrobím opět analýze metodou FMEA, ve které již budou zakomponována navrhovaná nápravná opatření. Metoda FMEA bude na základě dosazených číselných hodnot, z nichž se vypočítá nové rizikové číslo, demonstrovat efektivitu nápravných opatření.

Poté co metodou FMEA zjistím nová riziková čísla, zpracuji novou SWOT analýzu daného procesu. SWOT bude zakončena grafickým vyjádřením budoucího stavu po implementaci nápravných opatřeních, kde bude jasně demonstrováno zlepšení situace.

Celou kapitolu věnující se nápravným opatřením zakončím krátkým shrnutím toho, co se implementací těchto opatření podařilo zlepšit, ale nyní již přistoupím k představení nápravných opatření.

- **Využití plného potenciálu systému MobileDoc**

  Zde narážím na problém, že výjezdová skupina nemá možnost sdílet data s příjmovým nemocničním zařízením. Dochází tedy k prodlení informace, jelikož pokud by se v systému MobileDoc využívaly všechny jeho funkce, příjmové nemocniční zařízení by mělo možnost získávat informace o pacientovi ihned v okamžiku, kdy to příslušník výjezdové skupiny zadává do aplikace.

- **Sdílení dat – redukce používání telefonického hovoru**

  Další opatření úzce souvisí s předchozím bodem, jelikož v okamžiku, kdy se začnou funkce systému MobileDoc využívat naplno, tak pro výjezdovou skupinu padá povinnost využívání telefonického hovoru pro sdělování informací o stavu pacienta příjmovému zařízení. Redukcí používání telefonického hovoru se výjezdová skupina vyhne situacím, kdy se kvůli nekvalitnímu zařízení nebo špatnému pokrytí signálem nemůže s příjmovým nemocničním zařízením spojit, anebo je kvalita hovoru na velmi nízké úrovni.

- **Kvalitní telefony pro VS**

  Pokud ovšem výjezdová skupina bude potřebovat využít telefonického hovoru, je nezbytné, aby měla k dispozici nejlepší možné vybavení, a proto jsem tento bod zahrnul do svých nápravných opatření.

- **Kvalita školení**

  Pro eliminace chybného vyplnění dat do systému MobileDoc výjezdovou skupinou, navrhuji opatření v podobě zlepšení kvality školení ve smyslu zaměření se i na informační dovednosti.

- **Automatizace postupu**

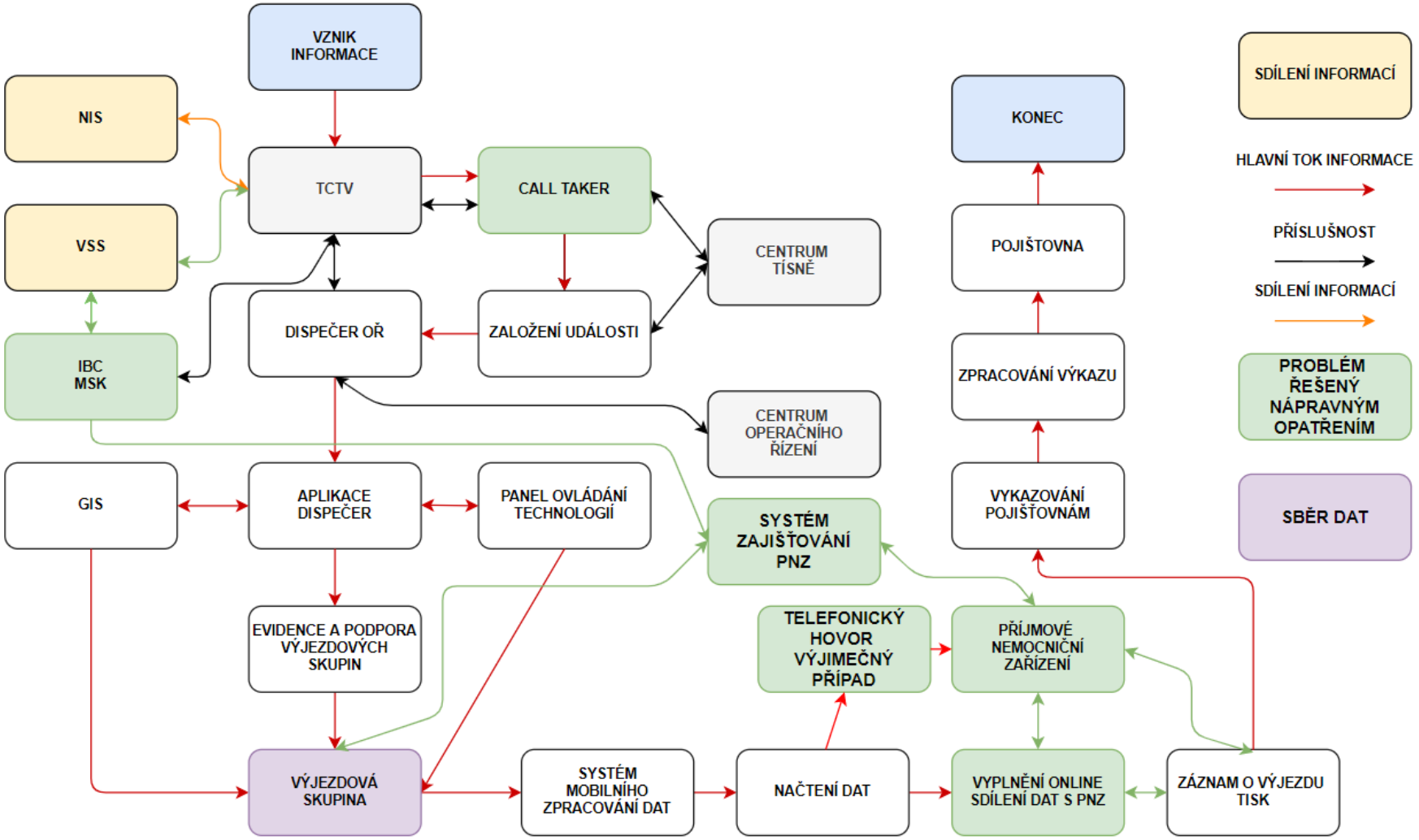
  Dostávám se k problému, kdy dispečer v centru tísně, tedy call taker, z jakéhokoliv důvodu nedostatečně vytěží informace od volajícího a výjezdová skupina následně dostává neúplnou nebo chybnou informaci o stavu pacienta. Tento problém bych řešil školením, které by se zaměřilo na automatizaci postupu při zjišťování všech potřebných informací ve smyslu vštěpování logického řetězce otázek, na které se bude call taker postupně ptát. To může fungovat na bázi pomyslného check listu.

- **Systém automatického určování příjmového nemocničního zařízení**

  Toto nápravné opatření by eliminovalo povinnost příslušníků výjezdové skupiny rozhodovat se, do kterého příjmového zařízení pacienta předají, a fungovalo by ve vzájemné symbióze se systémem MobileDoc. Pomocí informací sdílených do VSS by systém vyhodnotil na základě zásady nejbližšího adekvátního zdravotnického zařízení, které zdravotnické zařízení určí pro výjezdovou skupinu jako příjmové. MobileDoc by na základě vybraného příjmového zařízení začal s daným zařízením sdílet data tak, aby bylo v daném zařízení vše připraveno na převzetí pacienta od výjezdové skupiny.

9.1 Proces toku informace

Všechna nápravná opatření výše uvedená nyní implementuji do procesu toku informace. Při zpracování vycházím z původního diagramu a zásady zpracování vývojového diagramu zůstávají také stejné, avšak jsou zde nově zeleně označeny všechny prvky procesu řešené nápravnými opatřeními a s tím související tok informace.



Obrázek 6 - Tok informace - nápravná opatření

Samotný vývojový diagram procesu toku informace v rámci ZZS MSK byl podrobně popsán v předchozí kapitole. Ve vývojovém diagramu s implementací nápravných opatření tím pádem již pouze vysvětlím, jakým způsobem nápravná opatření činí celý proces efektivnějším a současně i bezpečnějším z pohledu samotné informace a také z pohledu poskytnutí lékařské péče pacientovi.

- **Call taker**

  U call takera bylo pomocí většího počtu školení zaměřených na automatizaci postupu při těžbě informací dosaženo minimalizace případů, kdy je informace vytěžena nedostatečně. Dalším přínosem nápravného opatření může být celkové zefektivnění procesu těžby informace od volajícího.

- **Telefonický hovor**

  Nutnost využití telefonického hovoru se na základě nápravného opatření, které se zaměřuje na sdílení dat s MobileDoc od výjezdové skupiny k příjmovému nemocničnímu zařízení, podařilo zredukovat pouze na výjimečné případy, kdy by třeba z jakéhokoliv důvodu nebyla služba sdílení dat dostupná. Stejně tak se nápravným opatřením v podobě nakoupení kvalitních telefonů pro VS zajistilo to, že při případném využití telefonického hovoru bude kvalita hovoru na vysoké úrovni, čímž se předchází zkreslení informace.

- **Systém automatického zajišťování PNZ pro výjezdovou skupinu**

  Toto nápravné opatření se ve vývojovém diagramu projevilo vznikem zcela nového prvku celého procesu. Systém automatického zajišťování PNZ využívá sdílení dat z TCTV prostřednictvím VSS do IBC, odkud čerpá data pro vyhodnocení nejvhodnějšího příjmového nemocničního zařízení. Jakmile nemocniční zařízení vybere a informuje toto zařízení o nastalé události, poskytne informaci o vybraném příjmovém nemocničním zařízení i výjezdové skupině.

  Na základě této informace začne výjezdová skupina při vyplňování dat do systému MobileDoc sdílet tato data s vybraným příjmovým nemocničním zařízením. V tomto momentě se příjmové nemocniční zařízení již může přichystat na příjem pacienta od výjezdové skupiny, potažmo zajistit operační sál a potřebný zdravotnický personál.

  Pro výjezdovou skupinu se tímhle opatřením ulehčí práce v tom, že se nemusí rozhodovat, do kterého nemocničního zařízení pacienta předají. Nyní již mají

nemocniční zařízení vybráno a především samotné nemocniční zařízení příjezd pacienta očekává, což podle mého názoru značně urychluje celý proces poskytnutí lékařské péče pacientovi.

- **Vyplnění dat online a sdílení dat s PNZ**

  Možnost vyplňování dat do systému MobileDoc a sdílení dat s PNZ pracuje ve vzájemné symbióze se systémem automatického vyhledávání PNZ pro výjezdovou skupinu, jehož funkce byla podrobně popsána v předchozím bodě. Tato možnost je dosažena především využitím plného potenciálu systému MobileDoc a vzájemnou spoluprací nemocničních zařízení se zdravotnickou záchrannou službou. Zde bych tedy pouze zopakoval skutečnost, že užitečnost tohoto nápravného opatření tkví v poskytování nejaktuálnějších informací o stavu pacienta do příjmového nemocničního zařízení, což vede k urychlení celého procesu předávání pacienta.

- **Příjmové nemocniční zařízení**

  Především z předchozích dvou popsaných bodů lze jednoduše dedukovat, že prvek „Příjmové nemocniční zařízení“ se ocitá v zeleném zabarvení proto, jelikož dvě předchozí nápravná opatření vyžadují vzájemnou spolupráci s tímto prvkem procesu a samotný proces poskytování lékařské péče pacientovi se v tomto bodě značně zrychluje. Stejně tak se zrychluje i tok informace, neboť příjmové nemocniční zařízení má k dispozici sdílená data o stavu pacienta od výjezdové skupiny ještě před jejich příjezdem.

9.2 FMEA pro nápravná opatření

Nyní se vracím k metodě analýzy FMEA, ve které budu demonstrovat zmenšení rizikového čísla u nalezených slabých míst pomocí implementace nápravných opatření. Tabulka vychází z původní analýzy, avšak je doplněna o představená nápravná opatření, což zákonitě vedlo i k novým výpočtům vedoucím k rizikovému číslu.

V úvodu podkapitoly bude přiložena samotná tabulka metody analýzy FMEA, načež bude následovat vysvětlení toho, proč se implementací nápravných opatření mění hodnota rizikového čísla a jak jsem se k nové hodnotě dopracoval.

Konkrétní změny hodnot rizikových čísel u nalezených slabých míst jsem konzultoval s Bc. Milanem Leškem v našem vzájemném rozhovoru dne 1. 3. 2021.

Tabulka 3 – FMEA - nápravná opatření

Původní stav									**Stav po implementaci opatření**					
Prvek procesu	Možná vada	Možné následky	**Význam**	Možné příčiny	**Výskyt**	Stávající opatření k odhalení	**Odhalitelnost**	**Rizikové číslo**	Opatření	Zodpovědnost	**Význam**	**Výskyt**	**Odhalitelnost**	**Rizikové číslo**
MobileDoc	Nesdílení dat	Vyšší riziko zhoršení stavu pacienta	**8**	Nevyužití potenciálu systému	**10**	Žádné	**1**	**80**	Využití všech FCÍ systému	Příjmová zařízení a ZZS MSK	**8**	**1**	**1**	**8**
Telefonický hovor	Špatná kvalita hovoru	Zkreslení a zpomalení informace	**5**	Špatný signál nebo telefon	**8**	Pokrytí signálem	**1**	**40**	Kvalitní telefony	ZZS MSK	**5**	**3**	**1**	**15**
Telefonický hovor	Špatná kvalita hovoru	Zkreslení a zpomalení informace	**5**	Špatný signál nebo telefon	**3**	Pokrytí signálem a kvalitní telefon	**1**	**15**	Sdílení dat	Příjmová zařízení a ZZS	**5**	**1**	**1**	**5**
Výjezdová skupina	Špatné zpracování informace	Špatné směřování pacienta	**10**	Neodpovídající znalosti	**4**	Pravidelné školení zaměstnanců	**2**	**80**	Lepší kvalita školení	Zaměstnavatel/ zaměstnanec	**10**	**1**	**2**	**20**
Call taker	Špatná interpretace vytěžených informací	Neadekvátní reakce na vzniklou situaci	**8**	Špatné komunikační dovednosti dispečera	**2**	Výběrové řízení	**2**	**32**	Častější školení automatizace postupu	Zaměstnavatel/ zaměstnanec	**8**	**1**	**1**	**8**
IBC MSK	Nezajištění cílového zařízení pro VS	Komplikace při předávání pacienta	**6**	V MSK tento systém není zaveden	**10**	Žádné	**1**	**60**	Automatický systém	IBC MSK a příjmová zařízení	**6**	**1**	**1**	**6**

- **Nesdílení dat**

  Využitím všech funkcí systému MobileDoc se došlo k plnému sdílení dat od výjezdové skupiny k příjmovému nemocničnímu zařízení, což vedlo ke snížení hodnoty výskytu z 10 na 1. Vada v podobě nesdílení dat může i nadále nastat, avšak jen ve výjimečných případech. Tím jsem se dostal k novému rizikovému číslu **8**.

- **Špatná kvalita hovoru**

  K eliminaci špatné kvality hovoru napomáhá nápravné opatření, které vybavuje výjezdovou skupinu kvalitními telefony. Hodnota výskytu se mění z původních 8 na 3, rizikové číslo je **15**.

- **Špatná kvalita hovoru**

  I přestože je výjezdová skupina již vybavena kvalitními telefony, stále zde existuje velmi častá povinnost využívat telefonního hovoru, u kterého může dojít ke špatné kvalitě hovoru čistě z důvodu nedostatečného pokrytí mobilní sítí. K ještě výraznějšímu snížení rizikového čísla napomáhá implementace opatření v podobě sdílení dat mezi VS a PNZ. Nyní se snížením hodnoty výskytu dostávám ke konečnému rizikovému číslu **5**.

- **Špatné zpracování informace**

  Kvalitnějším školením zaměřeným na práci se systémem MobileDoc se snižuje výskyt této vadu z hodnoty 4 na hodnotu 1, z čehož vypočítám novou hodnotu rizikového čísla, tedy **20**.

- **Špatná interpretace vytěžených informací**

  Vštěpováním automatizace postupu při těžbě informace na pravidelných školeních je dosaženo snížení hodnoty rizikového čísla z původních 32 na **8**.

- **Nezajištění cílového zařízení pro výjezdovou skupinu**

  Jelikož v současném proces neexistuje žádný systém automatického zajišťování PNZ pro výjezdovou skupinu, původní hodnota výskytu byla 10. Zavedením takového systému dochází ke snížení této hodnoty na úroveň 1. Z toho vyplývá i nová hodnota rizikového čísla, která aktuálně je **6**.

9.3 SWOT nového procesu

Po uvedení nápravných opatření a jejich následném zakomponování do vývojového diagramu procesu toku informace, byl tento proces podroben znovu analýze metodou FMEA. Na základě výsledků analýzy FMEA následuje další kompletní SWOT analýza s grafickým vyhodnocením stavu po implementaci nápravných opatření.

Pozměněné bodové veličiny u analyzovaných hodnot jsem opět konzultoval s Bc. Milanem Leškem v našem vzájemném rozhovoru ze dne 1. 3. 2021.

9.3.1 SWOT tabulka – nápravná opatření

Tabulku SWOT analýzy jsem zpracoval za dodržení stejných pravidel jako u tabulky současného stavu. Jedná se tedy o tabulku rozdělenou do čtyř kvadrantů (silné stránky, slabé stránky, příležitosti a hrozby), přičemž vrchní část tabulky se věnuje vnitřní analýze a spodní část tabulky zpracovává analýzu vnější. Analyzovaným hodnotám bylo opět přiřazeno bodové ohodnocení a váha, na základě čehož se počítá výsledek dané hodnoty a konečně i výsledek vnitřní a vnější analýzy.

Tabulka 4 - SWOT analýza - nápravná opatření

SWOT								
	STRENGHTS				WEAKNESSES			
VNITŘNÍ ANALÝZA		Body	Váha	Součin		Body	Váha	Součin
	Dostupnost tísňové linky	5	0.6	3	Nesdílení dat	-3	0.4	-1.2
	GIS	4	0.2	0.8	Telefonický hovor	-1	0.2	-0.2
	Kybernetické zabezpečení	4	0.2	0.8	Nedostatečné zpracování dat VS	-3	0.4	-1.2
		Součet =		4.6		Součet =		-2.6
	Výsledek vnitřní analýzy = 4.6 - 2.6 = 2							
	OPPORTUNITIES				THREATS			
VNĚJŠÍ ANALÝZA		Body	Váha	Součin		Body	Váha	Součin
	Silné pokrytí mobilní sití	4	0.4	1.6	Cílové zařízení	-1	0.2	-0.2
	Komunikační schopnosti dis.	5	0.4	2	Komunikační schopnosti dis.	-2	0.3	-0.6
	Informovanost veřejnosti	4	0.2	0.8	Zneužití/zahlcení tísňové linky	-5	0.5	-2.5
		Součet =		4.4		Součet =		-3.3
	Výsledek vnější analýzy = 4.4 - 3.3 = 1.1							

- **Silné stránky**

  V oblasti silných stránek se oproti SWOT analýze současného stavu nic nezměnilo. Analyzované hodnoty zůstaly stejné, stejně tak jako přiřazené veličiny, a proto se ani výsledek této oblasti nemění.

- **Slabé stránky**

  U slabých stránek již je situace naprosto odlišná, jelikož implementací nápravných opatření se zásadně změnilo bodové ohodnocení u analyzovaných hodnot. Nesdílení dat stále představuje slabé místo v procesu, ovšem už jen v případě, že k tomu dojde z technických důvodů a nikoliv proto, že funkce není zavedena. Na základě dvou nápravných opatření, tedy kvalitní telefony a sdílení dat, se takřka eliminovala potřeba využívat při výjezdu telefonický hovor, čímž se se znatelně snížila závažnost tohoto slabého místa. Nedostatečně zpracování dat do systému MobileDoc výjezdovou skupinou zůstává i nadále významným problémem, avšak zakomponováním častějších školení zaměřených na práci s tímto systémem se podařilo význam tohoto problému značně snížit.

- **Příležitosti**

  Stejná situace jako v oblasti silných stránek nastává také u příležitostí, což znamená, že analyzované hodnoty zůstaly stejné, přiřazené veličiny k nim rovněž a tedy i výsledek analýzy v oblasti příležitostí je neměnný.

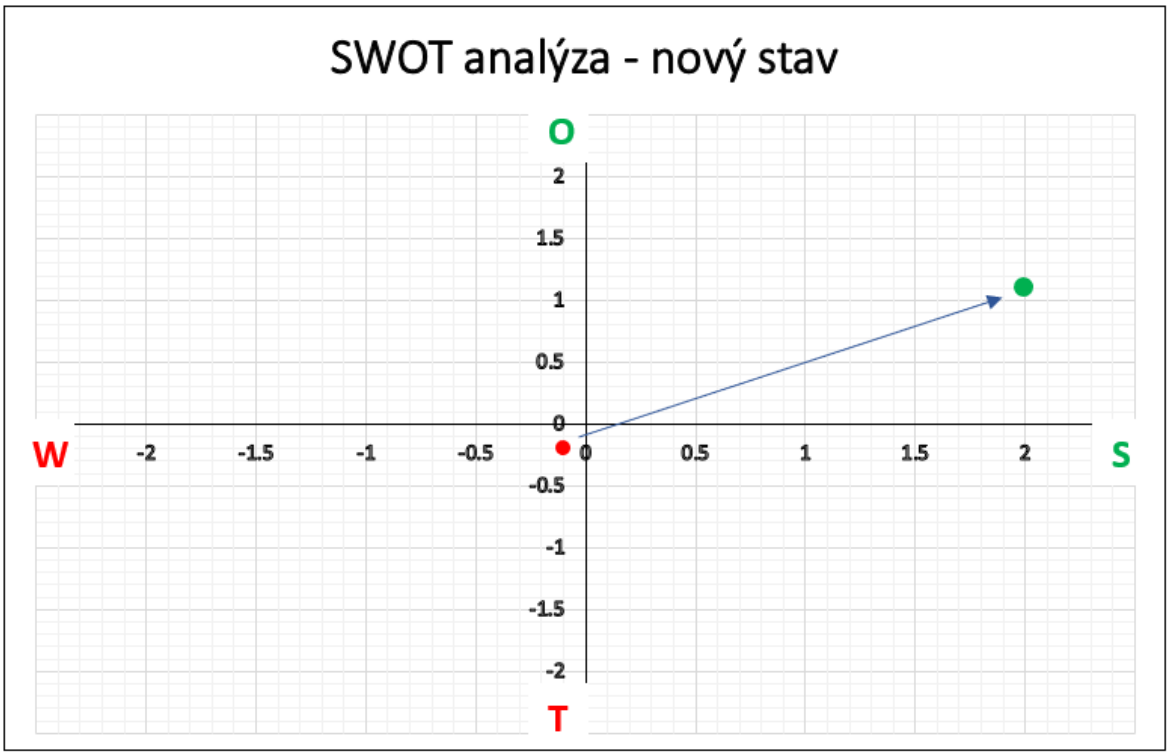
- **Hrozby**

  Po zavedení sdílení dat od výjezdové skupiny k příjmovému nemocničnímu zařízení a především vybudování systému automatického určování příjmového nemocničního zařízení bylo v analýze SWOT dosaženo snížení významu hrozby v podobě cílového zařízení. Následně se i u druhé analyzované hrozby, tedy Komunikační schopnosti dispečera, podařilo snížit její význam, a to zavedením častějších školení zaměřených na automatizaci postupu při těžbě informace od volajícího. Bohužel hrozba zahlcení či zneužití tísňové linky zůstává vážným problémem, což v rámci vypracované SWOT analýzy znamená, že se bodové ohodnocení nemění. Na základě těchto změn se citelně snížila číselná hodnota vyjadřující výsledek v oblasti hrozeb.

9.3.2 SWOT graf – nápravná opatření

Grafické vyjádření analýzy SWOT, které bude vloženo do následující podkapitoly, jasně demonstruje zlepšení stavu procesu. Na základě výsledných hodnot v kvadrantech silných a slabých stránek jsem vypočítal výsledek vnitřní analýzy. Stejně jsem na základě hodnot ve zbylých dvou kvadrantech spočítal výsledek vnější analýzy. Tyto hodnoty jsem následně vnesl na graf osy X a Y, čímž jsem získal výslednou hodnotu analýzy. V grafu je

zakomponováno i znázornění samotného zlepšení směrem od původního stavu k situaci po implementaci opatření. S



Obrázek 7 - Graf SWOT - nápravná opatření

Stejně jako u původního grafu SWOT analýzy je potřeba podotknout, že daný výsledek je hodnotou, která vyjadřuje stav, kdy stále existuje možnost, že proces ovlivní všechny slabé stránky a v praxi se projeví i zmiňované hrozby. Pravděpodobnost toho, že se tak stane, se ale podařila snížit na základě implementací nápravných opatření, a proto je zde značný posun z kvadrantu WT do kvadrantu OS, což je rozhodně žádoucí výsledek, jelikož výsledek nacházející se v kvadrantu OS, je ta nejlepší možná varianta, která může nastat při zpracování analýzy SWOT.

10 VYHODNOCENÍ PRAKTICKÉ ČÁSTI

Rád bych připomenul, že s vypracováním praktické části mně velmi pomohl Bc. Milan Leško, jakožto člen výjezdové skupiny ZZS MSK, a Ing. Radim Kozelský, který mně poskytl materiály. Tyto materiály mi velmi pomohly při zpracování praktické části.

Praktická část si dávala za cíl zmapovat tok informace v rámci ZZS od momentu přijatého hovoru tísňovou linkou od volajícího z místa události až po předání pacienta výjezdovou skupinou do nemocničního zařízení a vykázání výjezdu zdravotním pojišťovnám.

V rámci mapování toku informace jsem se zaměřil na vyhledávání potenciálních slabých míst, na které bych mohl reagovat nápravnými opatřeními. Vzhledem ke spolupráci se členem výjezdové skupiny se snad podařilo objektivně vystihnout možná slabá místa, pak už zůstalo na mně, abych tyto skutečnosti podrobil analýze. Před přistoupením k samotným metodám analýzy jsem v samostatné podkapitole popsal způsob kybernetické bezpečnosti, která je v rámci daného procesu toku informace aplikována.

V rámci analýzy jsem využil metod FMEA a SWOT. Metoda FMEA byla použita za účelem identifikace slabých míst, zatímco metoda SWOT analyzovala stav toku informace jako celku. Následně jsem si vybral jednu konkrétní vadu, kterou jsem dále podrobil analýze pomocí metod ETA a FTA.

Následovala kapitola pojednávající o nápravných opatřeních. Tato opatření jsem po zakomponování do procesu opět podrobil analýze FMEA s cílem demonstrovat zlepšení u konkrétních nalezených vad. Posléze byl celý proces znovu podroben analýze SWOT, která jasně ukázala zlepšení, kterého bylo dosaženo pomocí nápravných opaření.

Je potřeba podotknout, že analýza se zaměřovala na hledání takových slabých míst v rámci kybernetického prostoru, která by mohla ohrozit kybernetickou bezpečnost celého procesu. Díky vzájemné provázanosti jsem však dospěl k závěru, že samotné ohrožení kybernetické bezpečnosti ve smyslu ovlivnění informace má značný vliv i na samotnou práci výjezdové skupiny a fungování celého procesu poskytnutí lékařské péče pacientovi. Z toho důvodu se praktická část zaměřuje mimo kyberprostor i na zefektivnění procesu odbavení pacienta.

ZÁVĚR

Na kybernetické bezpečnosti se mi líbí skutečnost, že se jedná o obor, se kterým je možné se prosadit napříč mnoha dalšími odvětvími. Proto jsem vděčný za příležitost, že jsem mohl psát bakalářskou práci, jejíž téma převážně vychází právě z tohoto oboru. Nyní jsem se již zdárně dopracoval ke konci a už přede mnou leží pouze shrnutí a zhodnocení mé bakalářské práce.

V teoretické části jsem zprvu v samostatné kapitole vysvětlil základní pojmy v rámci kybernetické bezpečnosti. Následně jsem podrobně popsal kybernetickou bezpečnost jako takovou a třetí kapitolu jsem věnoval tématu kybernetické kriminality, což mělo napomoci podrobnému popisu problematiky kybernetické bezpečnosti z obou perspektiv. Ve čtvrté kapitole jsem pro úplnost popsané problematiky zpracoval přehled toho, jakým způsobem je kybernetická bezpečnost řešena na území České republiky. V páté kapitole dostal prostor integrovaný záchranný systém, což završilo teoretickou část, načež následovalo už jen vyhodnocení teoretické části a popis použitých metod v části praktické. Tímto byl naplněn jeden z dílčích cílů, tedy podrobný popis probírané tematiky a vysvětlení provázanosti integrovaného záchranného systému a kybernetické bezpečnosti.

Praktická část se věnovala analýze procesu toku informace v rámci zdravotnické záchranné služby s přihlédnutím na kybernetickou bezpečnost daného procesu. Na začátku praktické části jsem vysvětlit předmět zájmu a představil konkrétní složku IZS, kterou jsem analyzoval. Následovala analýza současného stavu, ve které jsem hledal slabá místa v procesu tak, abych v další kapitole, nápravná opatření, mohl tato opatření zakomponovat do procesu a podrobit další analýze. Následovalo již pouze vyhodnocení praktické části

Na základě splnění dílčích cílů se mi podařilo představit nový koncept toku informace, který původní proces zlepšuje v rámci kybernetické bezpečnosti, jelikož obsahuje nápravná opatření, jež zabraňují ovlivňování informace a automatizací tuto informaci zrychlují, což následně vede i k rychlejšímu procesu poskytnutí zdravotní péče pacientovi.

Musím uznat, že jsem byl překvapen, jak velká je provázanost kybernetické bezpečnosti a fungování integrovaného záchranného systému jako celku. Stále mám však pocit, že v mnoha oblastech státní nebo soukromé sféry je oblast kybernetické bezpečnosti opomíjena. Zde vidím velký prostor pro zlepšení a dle mého názoru by měla kybernetická bezpečnost mít svoje místo v organizační struktuře každého státu i firmy.

SEZNAM POUŽITÉ LITERATURY

About ENISA - The European Union Agency for Cybersecurity: Towards a Trusted and Cyber Secure Europe, 2020. *ENISA* [online]. [cit. 2021-03-02]. Dostupné z: https://www.enisa.europa.eu/about-enisa

BURDA, Karel, 2019. *Kryptografie okolo nás*. Praha: CZ.NIC. ISBN 978-80-88168-49-2.

Co je GDPR a jak bude aplikováno v Česku, 2017. *Obecné nařízení o ochraně osobních údajů* [online]. [cit. 2021-03-02]. Dostupné z: https://www.gdpr.cz/gdpr/co-je-gdpr/

Cybercrime, 2017. *Interpol* [online]. [cit. 2021-03-02]. Dostupné z: https://www.interpol.int/en/Crimes/Cybercrime

Cyber crime, 2020. *FBI: Federal bureau of investigation* [online]. [cit. 2021-03-02]. Dostupné z: https://www.fbi.gov/investigate/cyber

ČESKO, 2000. Zákon č. 239/2000 Sb. Zákon o integrovaném záchranném systému a o změně některých zákonů. In: *Sbírka zákonů*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-239

ČESKO, 2014. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti. In: *Sbírka zákonů*. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

DOSTÁL, Otto, Roman JAŠEK a Gabriela KRISTOVÁ, 2013. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM. ISBN 978-80-7204-872-4.

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.3.

ETA (Event tree analysis), 2015. *Management Mania* [online]. ManagementMania.com [cit. 2021-7-20]. Dostupné z: https://managementmania.com/cs/eta-event-tree-analysis-analyza-stromu-udalosti

FMEA (Failure Mode and Effect Analysis), 2021. *Management Mania* [online]. ManagementMania.com [cit. 2021-7-20].
Dostupné z: https://managementmania.com/cs/failure-mode-and-effect-analysis

FTA (Fault Tree Analysis), 2015. *Management Mania* [online]. ManagementMania.com [cit. 2021-7-20]. Dostupné z: https://managementmania.com/cs/fault-tree-analysis

GDPR, 2020. *Kybez: Platforma kybernetické bezpečnosti* [online]. [cit. 2021-03-02]. Dostupné z: https://www.kybez.cz/gdpr

GOVCERT.CZ, 2021. *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2021-03-02]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/vladni-cert/

HUMPL, Lukáš, 2021a. Kdo jsme. *Zdravotnická záchranná služba* [online]. Zdravotnická záchranná služba Moravskoslezského kraje [cit. 2021-6-23]. Dostupné z: https://www.zzsmsk.cz/Default.aspx?mainhref=informace

HUMPL, Lukáš, 2021b. Organizační struktura. *Zdravotnická záchranná služba* [online]. Zdravotnická záchranná služba Moravskoslezského kraje [cit. 2021-6-23]. Dostupné z: https://www.zzsmsk.cz/Default.aspx?mainhref=oNas

Integrovaný záchranný systém, 2021. *Hasičský záchranný sbor* [online]. Generální ředitelství Hasičského záchranného sboru ČR [cit. 2021-5-4]. Dostupné z: https://www.hzscr.cz/clanek/integrovany-zachranny-system.aspx

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2015. Výkladový slovník Kybernetické bezpečnosti. In: *CyberSecurity.cz* [online]. [cit. 2021-03-02]. Dostupné z: https://www.cybersecurity.cz/data/slovnik_v310.pdf

KADLECOVÁ, Michaela, 2021. Pražská záchranka začne informace o pacientech předávat elektronicky. *Svět chytře* [online]. SocialBooster [cit. 2021-5-4]. Dostupné z: https://svetchytre.cz/a/puk3U/prazska-zachranka-zacne-informace-o-pacientech-predavat-elektronicky?fbclid=IwAR2y-ujGTgNsHchgu5IzFmPldZ5XMa_gUMiNps4EJ18mXL20Y1sGB6-3TjA

KAPOUN, Jan, 2004. Norbert Wiener: otec kybernetiky. *CIO* [online]. [cit. 2021-6-22]. Dostupné z: https://businessworld.cz/veda-a-historie/norbert-wiener-otec-kybernetiky-3947

KOLOUCH, Jan, 2016. *Cybercrime*. Praha: CZ.NIC. ISBN 978-80-88168-15-7.

KOLOUCH, Jan et al., 2019. *Cybersecurity*. Praha: CZ.NIC. ISBN 978-80-88168-31-7.

KOZELSKÝ, Radim, 2020. *Analýza způsobu hodnocení stavu pacienta v přednemocniční péči z dat výjezdů zdravotnické záchranné služby*. Ostrava. Diplomová práce. Vysoká škola báňská – Technická univerzita Ostrava. Fakulta elektrotechniky a informatiky.

Kybernetická bezpečnost, 2011. *CyberSecurity.cz* [online]. [cit. 2021-03-02]. Dostupné z: https://cybersecurity.cz/basic.html

Kybernetická bezpečnost, 2018. *Bezpečnostní informační služba* [online]. [cit. 2021-03-02]. Dostupné z: https://www.bis.cz/kyberneticka-bezpecnost/

Kybernetická bezpečnost – definice a právní předpisy, 2020. *Be safe on the internet* [online]. BE-SAFE [cit. 2021-6-22]. Dostupné z: https://lms.project-bsafe.eu/cs/unit/kyberneticka-bezpecnost-definice-a-pravni

Kybernetická bezpečnost životní cyklus, 2021. *KYBEZ* [online]. GORDIC spol.s r.o. [cit. 2021-7-20]. Dostupné z: https://www.kybez.cz/zakladni-pojmy/

Kybernetika, 2002. *Katedra kybernetiky* [online]. [cit. 2021-03-02]. Dostupné z: http://www.kky.zcu.cz/cs/definition-of-cybernetics

LUKÁŠ, Luděk et al., 2011. *Informační podpora integrovaného záchranného systému*. Ostrava: Sdružení požárního a bezpečnostního inženýrství. ISBN 978-80-7385-105-7.

Národní strategie kybernetické bezpečnosti České republiky, 2020. In: *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2021-03-02]. Dostupné z: https://www.nukib.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf

NCKB, 2021. *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2021-03-02]. Dostupné z: https://nukib.cz/cs/kyberneticka-bezpecnost/

NÚKIB, 2021. *NÚKIB: Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2021-03-02]. Dostupné z: https://nukib.cz/cs/o-nukib/

O týmu CSIRT.CZ, 2011. *CSIRT.CZ* [online]. [cit. 2021-03-02]. Dostupné z: https://csirt.cz/cs/o-nas/

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK, 2013. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM. ISBN 978-80-7204-872-4.

Před čím se chránit, 2016. *Kybez: Platforma kybernetické bezpečnosti* [online]. [cit. 2021-03-02]. Dostupné z: https://www.kybez.cz/bezpecnost/pred-cim-chranit

SINGER, Peter a Allan FRIEDMAN, 2014. *Cybersecurity and cyberwar*. USA: Oxford university press. ISBN 978-0-19-991811-9.

SWOT analýza, 2020. *Management Mania* [online]. ManagementMania.com [cit. 2021-7-20]. Dostupné z: https://managementmania.com/cs/swot-analyza

ŠENOVSKÝ, Michal, Vilém ADAMEC a Zdeněk HANUŠKA, 2007. *Integrovaný záchranný systém*. 2. Ostrava: Sdružení požárního a bezpečnostního inženýrství. ISBN 978-80-7385-007-4.

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

Vývojový diagram, 2017. *Management Mania* [online]. ManagementMania.com [cit. 2021-7-20]. Dostupné z: https://managementmania.com/cs/vyvojovy-diagram-flow-chart

What is a Botnet, 2019. *Norton* [online]. [cit. 2021-03-02]. Dostupné z: https://us.norton.com/internetsecurity-malware-what-is-a-botnet.html

What is Cyber Security, 2020. *Kaspersky* [online]. [cit. 2021-03-02]. Dostupné z: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

What is malware, 2019. *McAfee* [online]. [cit. 2021-03-02]. Dostupné z: https://www.mcafee.com/en-us/antivirus/malware.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BIS	Bezpečnostní informační služba
CERT	Skupina pro reakce na počítačové hrozby
CSIRT	Skupina pro reakce na počítačové bezpečnostní incidenty
DDoS	Distribuované odepření služby
DNA	Deoxyribonukleová kyselina
ETA	Analýza stromu událostí
FMEA	Analýza možných vad a jejich následků
FTA	Analýza stromu poruchových stavů
GDPR	Obecné nařízení o ochraně osobních údajů
GIS	Geografický informační systém
HZS	Hasičský záchranný sbor
IBC	Integrované bezpečnostní centrum
ICT	Informační a komunikační technologie
ISMS	Systém řízení bezpečnosti informací
IT	Informační technologie
IZS	Integrovaný záchranný systém
KII	Kritická informační infrastruktura
MSK	Moravskoslezský kraj
MU	Mimořádná událost
MV	Ministerstvo vnitra
NIS	Nemocniční informační systém
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OŘ	Operační řízení
PC	Osobní počítač
PČR	Policie České republiky

TCTV	Telefonní centrum tísňového volání
USB	Univerzální sériová sběrnice
VIS	Významný informační systém
VPN	Virtuální soukromá síť
VS	Výjezdová skupina
VSS	Vrstva společných služeb
ZZS	Zdravotní záchranná služba

SEZNAM OBRÁZKŮ

SEZNAM TABULEK