Bezpečnost informační podpory krizového řízení

Václav Mikl

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:	**Václav Mikl**
Osobní číslo:	**L19486**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**Kombinovaná**
Téma práce:	**Bezpečnost informační podpory krizového řízení**

Zásady pro vypracování

1. Seznamte se s teoretickými základy krizového řízení.
2. Charakterizujte problematiku informační podpory krizového řízení.
3. Proveďte analýzu současného stavu v oblasti informační podpory krizového řízení a navrhněte doporučení ke zlepšení stávajícího stavu.

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

Seznam doporučené literatury:

1.SOCHU, Corey a Steven HERNANDEZ. *Information assurance handbook : effective computer security and risk management strategies*. New York ; McGraw-Hill Education, 2015. ISBN 978-0-07-182165-0.
2. VILÁŠEK, Josef a Emil ANTUŠÁK. *Základy teorie krizového managementu*. Praha: Karolinum, 2016. ISBN 978-80-246-3443-2.
3. PETROWSKI, Thorsten. *Bezpečí na internetu : pro všechny*. Liberec: Dialog, 2014. ISBN 9788074240669.
Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Pavel Tomášek, Ph.D.**
Ústav ochrany obyvatelstva

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

V Uherském Hradišti dne 2. prosince 2020

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: 29.7.2021

Jméno a příjmení studenta: Václav Mikl

.....
podpis studenta

ABSTRAKT

Tato bakalářská práce se zabývá bezpečností informační podpory v oblasti krizového řízení, informačními systémy, které jsou již dnes součástí krizového řízení. V části teoretické budou vymezeny základy krizového řízení, základní pojmy, právní normy, použití daných informačních systémů v oblasti krizového řízení, přístupy do těchto systémům, hierarchie přístupu do informačního systému a rozsah přístupu do těchto systémů. V neposlední řadě je zde řešena bezpečnost těchto systémů. V praktické části je zmíněn systém ukládání hesel jako jsou plain text nebo hashe. Dále je taktéž v praktické části provedena analýza rizik těchto informačních systémů, posouzení těchto rizik a návrh ke zlepšení současného stavu v oblasti bezpečnosti informačních systémů v oblasti krizového řízení.

Klíčová slova: Analýza rizik, krizové řízení, nouzový zákon, krizový zákon, informační systém, informační podpora, bezpečnost, hesla.

ABSTRACT

This bachelor thesis deals with the security of information support in the field of crisis management, information systems that are already part of crisis management. The theoretical part will define the basics of crisis management, basic concepts, legal standards, the use of information systems in the field of crisis management, access to these systems, the hierarchy of access to the information system and the scope of access to these systems. Last but not least, the security of these systems is addressed here. The practical part mentions the system of storing passwords such as plain text or hashes. Furthermore, the practical part also analyzes the risks of these information systems, assesses these risks and a proposal to improve the current state of security of information systems in the field of crisis management.

Keywords: Risk analysis, crisis management, emergency law, crisis law, information system, information support, security, passwords.

Poděkování:

Tímto si dovoluji poděkovat panu Ing. Pavlu Tomáškovi, Ph.D. za odborné vedení a cenné připomínky ke zpracování této bakalářské práce. Děkuji taktéž své rodině za podporu po celou dobu studia.

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

OBSAH

ÚVOD

Informační systémy v oblasti krizového řízení zastávají v dnešní době poměrně zásadní roli, tak jakožto i v jiných oblastech lidského působení. Informační systémy v právě v této oblasti jsou zejména využívány ze strany státní správy a samosprávy a jsou její nedílnou součástí.

Jako stále aktuální příklad lze uvést krizové řízení v období pandemie COVID – 19 sehrálo zásadní roli důležité při jejím zvládnutí, k tomu bylo třeba i využití informačních systémů od nejvyšších instancí až po ty nižší prvky samosprávy (vlády, různé poradní skupiny – které byly nápomocny při rozhodování o opatřeních, krajských úřadů, městských a obecních úřadů), za pomocí informačních systémů byly v době pandemie zpracovány data například od počtu testovaných, infikovaných, později i očkovaných občanů, tato data byla taktéž distribuována za pomocí informačních systémů, na základě jejich propojení mezi sebou.

Nedílným parametrem těchto systémů je v neposlední řadě i bezpečnost. Bezpečnost informační podpory je velmi zásadním prvkem těchto systémů. Každý systém disponuje určitou databází, kde jsou ukládány data se kterými se následně nakládá dle potřeby. V současné době je kladen velký důraz, aby byla daná databáze, kde se nachází data řádně zabezpečena, nikoliv pouze databáze jako taková, ale i přístup do ní by měl být limitován, tj. každá osoba, která s informačním systémem, chceme-li s databází pracuje, by měla mít přidělen přístup pouze k vybraným částem této databáze, které nezbytně potřebuje pro svoji pracovní činnost.

Rozhodně není žádoucí, aby přístup do databáze byl každému přidělen v neomezeném rozsahu, je to z důvodu zamezení ztráty informací, jejich následnému zneužití, popřípadě prodeji nežádoucím osobám, které by k daným informacím rozhodně mít přístup neměly. Informace jsou v dnešní době rozhodně jednou z nejcennějších komodit, a ne nadarmo se říká, že ten, kdo má informaci, tak má i moc, protože s informací může naložit dle svého uvážení, tedy ji může libovolně použít, chceme-li zneužít ve svůj prospěch a poškození ostatních, kteří by v rámci vyzrazení té dané informace mohli přijít k úhoně, ať již morální, finanční, materiální (k úhoně na majetku), či jiné. Informace je třeba vhodným způsobem zabezpečit, tedy je chránit proti zneužití. K tomu se samozřejmě váže i ochrana přístupů k informaci v rámci informačních systémů, obzvláště v informačních systémech, které slouží jako opora již zmiňovaného krizového řízení se mohou nacházet data, která mohou být

citlivá, jako jsou rodná čísla, data narození, jména, jiné souvislosti, například kdo je majitelem poškozené nemovitosti při živelných katastrofách, popřípadě na koho je uvalena exekuce, takové informace by se rozhodně neměly dostat do nepovolaných rukou. Důležité je i samotné zabezpečení databází jako takové proti neoprávněnému přístupu zvenčí, a nikoliv zvnitř organizace, tudíž je vhodné databázi šifrovat, nenechávat ji dostupnou bez daných přihlašovacích údajů, a to ani při přístupu zvnitř organizace. Důležité je taktéž pravidelně provádět zálohy databází na vhodná úložiště, ideálně ne trvale připojená k dalším informačním systémům. Taktéž je vhodné provádět osvětu v rámci uživatelů těchto informačních systémů. Například vhodně zvolené zabezpečení těchto přístupů, nejen případnými hesly, ale i například za pomoci dvoufázového ověřování, že je tento uživatel opravdu oprávněn přistoupit do daného informačního systému, se kterým pracuje v rámci krizového řízení. V dnešní době bývá často například řešen přístup i pouze do počítače, jež slouží k zobrazení daného systému pro krizové řízení za pomocí čipových karet a bezpečnostních certifikátů spojenými s nimi, což je velmi rozumný přístup k bezpečnosti těchto systémů, zpravidla bývá kombinováno i s hesly pro přístup do daných systémů, a to je již relativně dostatečné zabezpečení. Dále je vhodné neustále inovovat a vylepšovat i heslovou politiku, která se váže k těmto přístupům z důvodu stále propracovanějších možností úniku informací. V momentě, když se stále zdokonaluje bezpečnostní strategie v rámci informační podpory krizového řízení, která si klade za cíl zvýšit bezpečnost těchto systémů a snížit riziko úniku informací, popřípadě neoprávněných přístupů. Cílem této práce je navrhnout zlepšení stávajícího stavu.

I. TEORETICKÁ ČÁST

1 ZÁKLADY KRIZOVÉHO ŘÍZENÍ

Krizové řízení je velmi zásadní složkou našich životů. Je třeba si skutečně uvědomit rizika, se kterými se potýkáme denně, tato rizika mohou mít zcela zásadní následky na naše životy.

Uvědomění si rizik je jedním z prvních kroků pro ochranu našich životů a zdraví. Krizové řízení jako takové slouží i k zabezpečení jisté ochrany bezpečnosti státu, tuto skutečnost bylo možno spatřit v době pandemie COVID – 19, ve které jsme se nacházeli a vlastně se stále nacházíme (r. 2021).

V této době bylo možno spatřit opravdu hodně zásadní využití tohoto oboru, obor krizového řízení dává v současné době opravdu veliký smysl, ať již pro řešení zdravotních rizik, či narušení bezpečnosti státu. Bez znalosti krizového řízení bychom nebyli schopni zvládat, byť i jednoduché krizové situace. Opět je zde třeba zmínit pandemii COVID-19, kterou ze začátku mnozí z nás považovali za bezpředmětnou, či vykonstruovanou.

Dnes si i ti největší „odříkači“ pandemie uvědomují, že to určitě zcela banální záležitost opravdu nebyla. Celou touto pandemií nás provázelo krizové řízení, ať chceme nebo ne, bez včasných opatření, která byla vyhlašována a stále vyhlášena jsou, byť nyní už minimální (06/2021) bychom určitě pandemii neustáli se ctí, tak jako se nám ji podařilo ustát v současné podobě. Těchto opatření by nebylo zcela jistě možno využít bez znalosti krizového řízení.

Samozřejmě veškeré záležitosti, které se týkají krizového řízení jako takového musí mít nějakou oporu v zákoně, a to v naší České republice konkrétně v zákoně č. 240/2000Sb. (Zákon o krizovém řízení a o změně některých zákonů - krizový zákon), ale o tom až v nějaké z dalších kapitol.

Důležité je zde zmínit souvislosti s krizovým řízením. Ono lze sebe lépe krizově řídit určitou krizovou situaci, která nastala, resp. případně nastane. Nicméně bez dalších navazujících oborů, které jsou s krizovým řízením úzce spjaty. A to jsou v neposlední řadě zcela určitě zdravotnická zařízení, která jsou v naší České republice na velmi dobré úrovni. Například již mnohokrát zmiňovanou pandemii COVID-19 by bylo zcela určitě nemožné zvládnout bez zdravotnictví ve velmi dobré kondici, tak jako je ku příkladu to naše. Samozřejmě bylo v době nejvyššího vytížení v době pandemie zdravotnictví dobře řídit, aby se nestalo to, že by došlo ke kolapsu. Bylo nutno v rámci nějaké strategie zvládnutí „nakažlivé choroby“ určit co je a není priorita a tak na základě určitých rozhodnutí bylo určeno, že prioritní je se postarat o pacienty nakažené COVIDem v těžkém stavu a tím, se z oddělení, které byly

určené pro jiné případy, než COVID stala oddělení, která byla přebudována-přeorganizována pro péči o pacienty, kteří byli COVID positivní. Dále byly vykonávány pouze nejnutnější zákroky, které by případně mohly ovlivnit zdraví a co hůře životy pacientů. Veškeré zákroky, které nebyly vyhodnoceny jako zdraví a život přímo ohrožující byly odloženy na dobu, až ubude hospitalizovaných v kritickém stavu.

Spousta zásadních a omezujících rozhodnutí v oblasti krizového řízení, ale nelze vykonávat bez nouzového stavu. Nouzový stav lze velmi stručně označit jako krizový stav. Tento stav lze vyhlásit v případě vzniku pandemie, v jakéžto se již více než rok nacházíme nebo jej lze vyhlásit i v případě živelných pohrom jako jsou povodně, vichřice nebo také nedávno nastalé situace u nás téměř nevídané a tou je tornádo, které u nás mělo opravdu velmi ničivý průběh, na jihu Moravy, oblast Hodonínska a Břeclavska – nicméně kvůli této konkrétní situaci nouzový stav vyhlášen nebyl.

V případě, že situace nejsou na tolik vážné, ale nevznikla potřeba nouzového stavu, nicméně potřeba vyhlásit nějaký krizový stav přetrvává z určitých vážných důvodů, je-li třeba vyhlásit nějaká specifická omezení využívají se nižší stupně krizového stavu jako je kupříkladu stav nebezpečí. Tento relativně specifický stupeň onoho krizového stavu je definován českými právními normami.

V nouzovém stavu je možno definovat omezení občanů České republiky na osobní svobodě, je možno kupříkladu omezit svobodu volného pohybu, zavést zákaz vycházení od určité hodiny, popřípadě uzavření předem definovaných provozoven, včetně maloobchodu, zavést pouze prodej nezbytného sortimentu. V tomto stavu je třeba, opravdu řádně vymezit práva, která jsou stanovená v zákoně o krizovém řízení, též krizový zákon (č.240/2000 Sb.).

Taktéž stojí za zmínku, že v oblasti krizového řízení se dnes čím dál častěji setkáváme s informačními systémy tak jako i v jiných oblastech lidského života. Tyto systémy jsou velmi užitečné pro sdílení informací mezi státní správou a samosprávou, ale i případnými jinými organizacemi podílejícími se na krizovém řízení.

S používáním a čím dál vyšším rozšířením informačních systémů úzce souvisí i jejich bezpečnost. V současné době je úroveň bezpečnosti informačních systémů mnohonásobně lepší, než před lety, ale stále jsou zde možnosti napadení jejich databází, vyzrazení hesel samotnými uživateli, případně únik hesel, pokud jsou uložena například v plain textu. Nebo se také častěji vyskytují možnosti prolamování hesel, nicméně pokud je dodržena určitá

složitost hesla a případně i dvoufázové ověření, tak je záležitost prolomení hesla značně ztížena.

1.1 Historie a vývoj krizového řízení

Pojem krizové řízení sahá až do roku 1962, kdy byl vůbec poprvé použit v souvislosti s karibskou krizí. Tato krize byla spojena se skrytě rozmístěnými operačně taktickými raketami, tyto rakety měly možnost nést též jaderné bojové hlavice.

Tyto rakety byly rozmístěny v zastoupení SSSR na Kubě v Karibském moři. Z této operace vyvstala konfrontace mezi USA a tehdejším SSSR, dnešním Ruskem. U této konfliktní záležitosti hrozilo vyústění v jadernou válku.

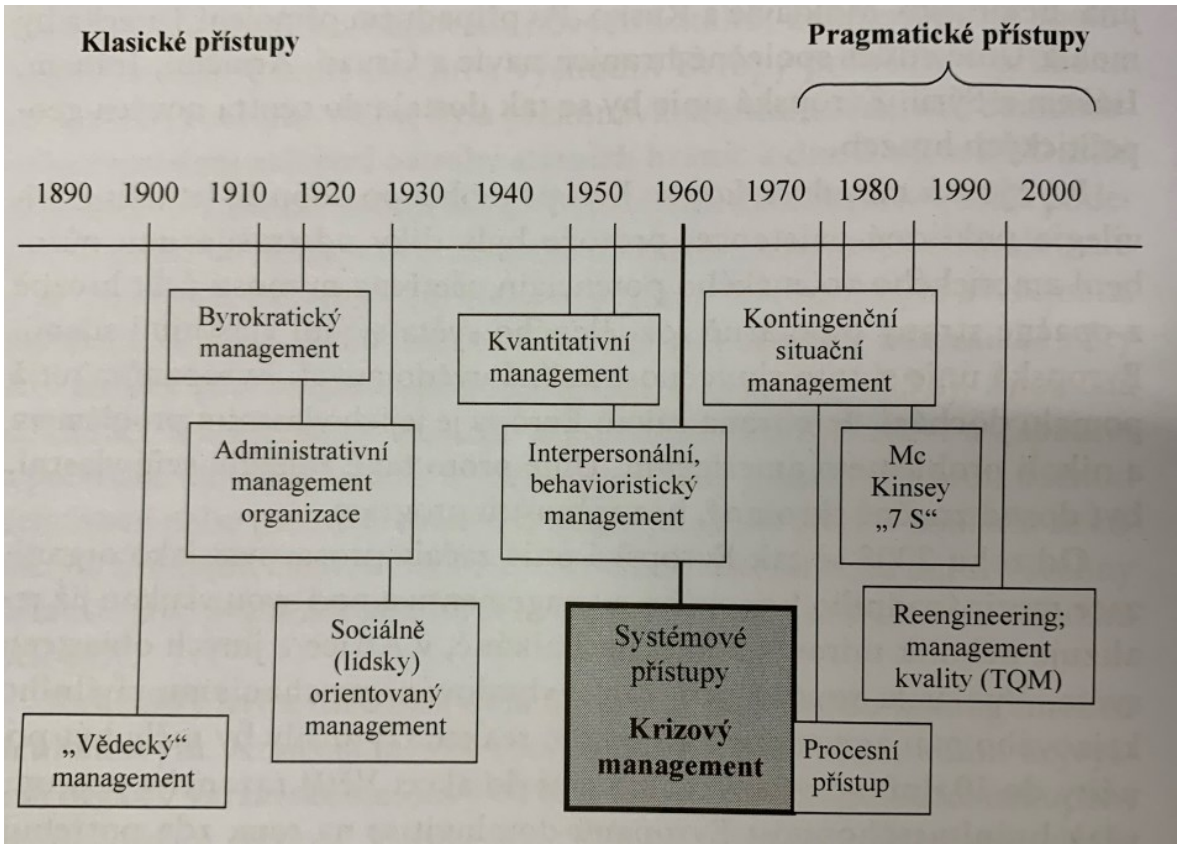
V té době měl J.F. Kennedy zacíleno na omezení rizik, která by mohla vést k případným konfliktním stavům mezi tehdejšími dvěma velmocemi, chceme-li mezi západem a východem. (Antušák a Vilášek, 2016)

Toto omezení rizik bylo tehdy poprvé označeno jako „crisis management“. (Antušák a Vilášek 2016, s. 28). V jedné z následujících etap byla se tato terminologie dokonce ujala i v NATO. Jak zmiňuje Antušák ve své knize základy teorie krizového managementu: *„Po celou dobu studené války byl nástrojem pro řešení (urovnávání) různých krizových situací vojenského charakteru, vzniklých ve vztazích mezi Severoatlantickou aliancí (NATO) a Varšavskou smlouvou.“ (Antušák a Vilášek , 2016, s.28)*

Základ obměny v pojetí krizového řízení se datuje do 60. a 70. let 20. století. Tyto obměny obnášely velké množství hledisek, za ty podstatné lze považovat přijet Harmelovy doktríny, tato měla pilíře zejména na tom, že posilovala obranný charakter aliance a zlepšovala diplomatické vztahy – resp. zmírňovala napětí mezi východní a západní velmocí. Koncem roku 1969 byla vyhlášena ze strany vlády Německé spolkové republiky „Ostpolitik“ – východní politiku, toto vyhlášení tohoto směru proběhlo za kancléře Willyho Brandta. Tato politika směřovala ke zlepšení vztahů na východě Evropy a též s východní velmocí, jíž byl Sovětský svaz. Následně byly přijaty nové normy pro oblast lidských práv a byla následně zavedena opatření pro posílení vzájemné důvěry mezi západem a východem. Tyto normy byly přijaty v srpnu 1975, v Helsinkách, na Konferenci o bezpečnosti a spolupráci v Evropě. Následovaly velké množství shodných událostí, které značně ovlivnily vývoj vztahu mezi západními a východními státy, dále byl těmito událostmi ovlivněn vývoj krizového řízení (v

80. letech minulého století). Určitě lze mezi tato opatření lze zařadit, resp. do tohoto vývoje ku příkladu rozmístění raket středního doletu v Evropě.

Po skončení Studené války a rozkladu vojenských a politických celků začíná NATO s inovovanou strategií Deklaraci o míru a spolupráci. V rámci toho dochází k inovovanému přístupu ke krizovému řízení, které se nyní nezaměřuje pouze na vojenské hrozby, nyní je pojem krizové řízení zaveden téměř do všech oblastí lidského života a zaměřuje se tedy v současnosti na hrozby vojenského i nevojenského charakteru. Krizové řízení jako takové lze tedy případně dělit na dvě podúrovně, tj. krizové řízení v oblasti vojenských krizových situací a civilních krizových situací. (Antušák a Kopecký, 2008).



Obrázek č. 1 – Historie a vývoj krizového managementu (Antušák a Vilášek, 2020, s.32)

Krizové řízení lze v současnosti vymezit jako souhrn řídících činností orgánů krizového řízení. Činnost v oblasti krizového řízení je dnes zaměřena na plánování, realizaci, kontrolu činností souvisejících s přípravou na krizové situace a jejich následným řešením, dále také vyhodnocuje bezpečnostní rizika, kterým se snaží předcházet na základě předchozích zkušeností a případného obecného vývoje v oblasti bezpečnostní situace. Lze tedy s určitostí

říci to, že krizové řízení je relativně efektivní a smyslnou záležitostí pro řešení různých krizových situací a potencionálních hrozeb jak vojenského, tak i nevojenského charakteru. Občas je nutno v případě různých krizových situací i zasáhnout a případně omezit i určitá práva a svobody uvedené v listině základních práv a svobod Ústavy České republiky. K tomu slouží krizová opatření – organizační, technická, která jsou předdefinována pro řešení různých krizových situací. (Kolektiv autorů , 2015).

Dle skript Ochrana obyvatelstva a krizové řízení lze klíčové prvky krizového řízení definovat jako: *Orgány krizového řízení:*

- *Vláda České republiky*
- *Ministerstva a jiné správní úřady*
- *Česká národní banka (dále „ČNB“)*
- *Orgány kraje a další orgány s působností na území kraje*
- *Orgány ORP a*
- *orgány obce* (Kolektiv autorů , 2015, s. 19).

V současné době je opora krizového řízení ze strany legislativy dána krizovým zákonem č.240/2000 Sb. (Tento zákon bude rozebrán v jedné z dalších kapitol.) V základě lze říci, že v krizovém zákoně jsou přesně definovány prováděcí pokyny, které umožňují orgánům krizového řízení rozhodnout o řešení krizové situace. Orgány v oblasti krizového řízení mají řádně stanovené povinnosti a oprávnění k zabezpečení plnění těchto povinností zakotvené v legislativě. Ve zkratce lze definovat velmi obecně to, že krizové řízení se zaměřuje přípravou na vzniknutí krizových situací, lze to charakterizovat i tak, že se zejména „připravuje“ na to jak případné krizové situace řešit, ale zaměřuje se i na to, jak řešit vzniklou krizovou situaci. Poměrně značný prostor v oblasti prevence obstarává systém civilního nouzového plánování. Níže na obrázku č. 2 lze spatřit diagram krizí a krizových situací. Krize a krizové situace nelze v základu řešit standartními prostředky a přístupy, protože dané činnosti, které se vyskytují v oblasti krizových situací nelze vyjádřit jakožto činnosti standartní, ale spíše častěji jakožto činnosti nestandartní, které se tedy neřeší na denní bázi, tudíž to určitým způsobem vybočuje ve standartu řešení. Na krizové situace nelze aplikovat obecný způsob řešení, protože vznikají vždy v konkrétním prostředím a každé prostředí je

něčím specifické, například specifičnost prostředí lze uchopit i jako to v jakých podmínkách se daná krizová situace vyskytne.

Chceme-li zaměřme se na autonehodu, můžeme ji vzít jakožto doslova modelovou situaci pro vysvětlení přístupu ke krizové situaci. Ať chceme nebo ne, autonehoda je do jisté míry taktéž krizová situace, něco nestandartního, co se nestává denně, týdně každému z nás, tedy naštěstí. Rozdíl prostředí autonehody lze pojmout i tak, že se stane autonehoda blízko řeky a nešťastnou náhodou jeden z účastníků dopravní nehody, resp. jeho vozidlo prorazí ku příkladu svodidla nebo jinou zábranu a spadne do řeky. Pro příklad počítejme to, že jedno z vozidel zůstane standardně na cestě, ale druhé, jak již bylo zmíněno spadne do řeky, či jiného vodního toku. Uchopme situaci tak, že v obou případech na dané autonehodě dojde k úniku provozních kapalin, ať se již jedná o ropné produkty – jako je palivo, dnes nejčastěji používaných benzín (BA95/BA98 = 95 oktanový/98 oktanový benzín) a nafta (Taktéž značená jako diesel), popřípadě stlačený zemní plyn (označené dnes jako CNG) nebo zkapalněný ropný plyn (značen jako LPG). Nicméně stlačený zemní plyn a zkapalněný ropný plyn není zrovna vhodný pro náš modelový případ. Uvažujme, že dojde k úniku nafty a benzínu. A dalších provozních kapalin typu brzdová a chladící kapalina – většinou založena na metanolu, etylenglykolu nebo propylenglykolu. V případě tohoto úniku je třeba provést určité sanace, tedy odklizení, uniklých kapalin z motorových vozidel. Na silnici jsou zpravidla využívané tuhé sorbenty – resp. sypké a ve vodě se zpravidla užívá norných stěn, díky kterým bývá zabráněno úniku těchto kapalin do toku řeky a podobně. Na toto se specializují zpravidla sanační firmy, které to mají jakožto hlavní předmět podnikání. Někdo samozřejmě musí zajistit propojení sanačních firem, složek IZS a podobně. Takto se dá tedy popsat krizová situace, řešení apod. Nejdůležitější je záchrana lidského zdraví a života, tudíž ve složkách IZS a v případě vážných nehod nesmí chybět záchranná služba, kterou musí samozřejmě tak jako jiné orgány někdo řídit, zabezpečovat po provozní stránce. Tato situace, která byla výše popsána se nestává standardně a bylo názorně popsáno o jakou rozdílnost prostředí se může jednat, voda – asfaltový nebo betonový povrch, i toto lze považovat za prostředí, je to jeho specifičnost. V případě, že uvažujeme tuto metodu jako modelový příklad, tak zcela transparentně zde lze demonstrovat to co je uvažováno v obrázku č. 2 a to sice, že krize nebo krizová situace vzniká v konkrétním prostředí (v našem případě silnice, vodní tok – konkrétní a specifická prostředí obojí), vlastně lze uvažovat to, že krize je následek krizové situace a tou krizovou situací je v našem případě autonehoda, krize je zamoření životního prostředí. Působí na konkrétní objekt, na silnici, popřípadě vodu,

v průběhu této krizové situace prováděné činnosti jakožto sanace a zabezpečení vytažení vozidla z řeky nemá standartní charakter, u každého je nutno zvolit jiný postup. Nelze ani jednu z uvedených situací řešit standardizovanými postupy. Je třeba zvolit individuální přístup. Názorná ukázka, viz obrázek 2. (Slezská univerzita, 2007)

Obrázek č.2 – charakteristika vzniku krizových jevů slu.cz, (Slezká unverzita, 2007, slide č.17)

1.2 Zákon č. 240/2000 Sb. – krizový zákon

Zákon o krizovém řízení a o změně některých zákonů (krizový zákon) je to zákon, který je platný na území České republiky od 1. ledna 2001. Je to zákon, který upravuje soubor krizových stavů. Prvně byl využit při řešení nastalé krizové situace v roce 2002, která měla souvislost s povodněmi. Tento zákon stanovuje pravomoci státních orgánů a orgánů státní samosprávy, dále stanovuje povinnosti a práva pro právnické a fyzické osoby při přípravách pro případ nenadálých krizových situací, které nesouvisí se zajištěním ochrany České republiky před napadením zevně. Dále také definuje odpovědnost za případné porušení povinností za těchto mimořádných situací. Tento zákon také reflektuje předpisy Evropské unie a taktéž upravuje ochranu kritické infrastruktury v EU. Zákonem jsou vymezeny nástroje, kterými lze dosáhnout účelu dané právní regulace. Zásadními nástroji tohoto práva

jsou stanovení povinnosti jednotlivých ministerstev a dalším úřadům, fyzickým a právnickým osobám.

V první části zákona, tedy HLAVA I. je uvedeno základní ustanovení, § 1 jsou zde uvedeny předměty úpravy, to co zákon stanovuje. Pravomoci státních orgánů, orgánů územních samosprávních celků, dále také jejich působnost, následně taktéž práva a povinnosti fyzických a právnických osob při přípravách na krizové situace.

V § 2 jsou vymezeny pojmy tohoto zákona. Krizové řízení a souhrn řídících činností, která se zaměřují na vyhodnocení bezpečnostních rizik, plánování, organizování, kontrolu v souvislostech s přípravami na krizové situace, popř. jejich řešením nebo se také vážou k ochraně kritické infrastruktury. Je zde například uvedeno, že krizovou situací nebo mimořádnou událostí dle zákona o integrovaném záchranném systému se rozumí narušení kritické infrastruktury případně ostatní nebezpečí, při kterých je vyhlášen stav nebezpečí, nouzový stav, popřípadě stav ohrožení státu.

Krizové opatření je dle definice zákona určeno k řešení krizové situace a případnému odstranění jejich následků, do těchto opatření lze zahrnout taková opatření, která zasahují do právu a povinnosti osob. Dále je zde uvedeno, že pracovní povinnost fyzické osoby se praktikuje na dobu nutnou, určenou práci, která jen nutná pro řešení krizové situace.

Je zde zmíněn i pojem pracovní výpomoci fyzických osob, která obnáší, vykonat jednorázové a mimořádné pracovní úkoly, které jsou nutné pro vyřešení krizové situace. Tyto práce je povinnost konat v místě, které je určeno orgánem krizového řízení.

Je zde také uvedena definice prvku kritické infrastruktury, prvek kritické infrastruktury se rozumí jakožto stavba, zařízení, prostředek nebo veřejná infrastruktura, je určena dle odvětví, pokud je tento prvek součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury. Ochrana kritické infrastruktury znamená dle tohoto zákona č. 240/ 2000 Sb. snížení rizika narušení funkce prvku kritické infrastruktury. Zákon také pamatuje na hledisko pro posouzení závažnosti vlivu prvku kritické infrastruktury v mezních hodnotách, které zahrnují rozsahy ztrát na životech, zdraví osob, vážné ekonomické dopady na veřejnost, v důsledku omezení poskytnutí nezbytných služeb, popřípadě jiného vážného zásahu do každodenního života.

Následně se tento zákon také zabývá pojmem stav nebezpečí. Tento stav může být vyhlášen, pokud jsou bezprostředně ohroženy životy a zdraví, majetek, životní prostředí a v případě, pokud intenzita ohrožení nedosahuje značného rozsahu a není možné odvrátit ohrožení

běžnou činností správních úřadů, orgánů krajů, obcí, složek IZS nebo subjektů kritické infrastruktury.

Tento stav, tedy stav nebezpečí lze vyhlásit pouze s odůvodněním a taktéž jej lze vyhlásit na nezbytně nutnou dobu pro území kraje nebo pouze pro jeho část. Stav nebezpečí vyhlašuje hejtman kraje pro celý kraj nebo jen pro jeho část.

V případě vyhlášení tohoto stavu musí obsahovat vyhlášení obsahovat krizová opatření a jejich případný rozsah, v části rozhodnutí, která obsahuje důvod vyhlášení tohoto stavu se uvádí, zda je tento stav vyhlášen na základě mimořádné události, dle zákona integrovaném záchranném systému.

Pokud hejtman tento stav vyhlásí, v případě hlavního města Prahy toto vyhlašuje primátor hlavního města, musí o této skutečnosti neprodleně informovat vládu.

V případě, že není možno odvrátit ohrožení, které vyvstalo, hejtman požádá vládu o vyhlášení NS. Rozhodnutí o vyhlášení stavu nebezpečí se zveřejňuje na úředních deskách krajského úřadu a na úředních deskách obecního úřadu, kterého se to týká.

Pokud vláda rozhodne o případném zrušení stavu nebezpečí, tak se toto zveřejňuje též na úřední desce krajského úřadu a na deskách OÚ, kterých se toto týká, jak je uvedeno v § 3 a odst. 9.

HLAVA II. tohoto zákona definuje orgány krizového řízení. V prvé řadě je třeba zmínit vládu, vláda při zajišťování připravenosti ČR na krizové situace ukládá úkoly ostatním orgánům činným v oblasti krizového řízení, určuje ministerstvo nebo jiný ústřední správní úřad pro koordinaci přípravy na řešení konkrétních krizových situací, zřizuje ústřední krizový štáb, stanovuje odvětví a kritéria pro určení prvku kritické infrastruktury, rozhoduje na základě seznamu, které předloží ministerstvo vnitra o prvcích KI a prvcích evropské KI, jejíž provozovatel je složka státu.

Je zde taktéž definováno, co lze v případě nouzového stavu nebo stavu ohrožení státu omezit, jsou to zejména vlastnická práva fyzických a právnických osob k majetku, pokud je vlastník nuceně omezen, je za toto poskytnuta odpovídající náhrada. Lze taktéž omezit právo se shromažďovat, svoboda pohybu a pobytu ve vymezeném území, které je případně ohroženo krizovou situací.

Následně je zde definována povinnost pro ministerstva a jiné ústřední správní úřady, že zřizuji pracoviště KŘ, zpracovávají plány, které obsahují souhrn krizových opatření, vedou

přehled možných zdrojů rizik v rámci krizové situace, provádějí jejich analýzu, v rámci prevence odstraňují nedostatky, které by mohly vést ke vzniku krizové situace.

V tomto zákoně je také pamatováno i na orgány kraje a další orgány s působností na území kraje. Zde je zmíněno, že hejtman kontroluje a řídí přípravná opatření činností k řešení KS a zmírnění jejich následků. Zřizuje a řídí také bezpečnostní radu kraje, krizový štáb kraje, schvaluje po projednání krizový plán kraje. (Zákon č. 240/2000 Sb.)

1.2.1 Ústavní zákon č. 110/1998 Sb.

Krizový zákon – 240/2000 Sb. se v základu opírá o ústavní zákon č. 110/1998 Sb., tudíž je popsán v této kapitole 1.2.1. V zákoně č. 110/1998 Sb. je v základním ustanovení poslání pro zajištění svrchovanosti a územní celistvosti České republiky, ochrana demokratických základů, ochrana života, majetkových hodnot jsou základní povinnosti státu.

Ve čl. 2 je definováno, že pokud dojde k ohrožení svrchovanosti, demokratického základu ČR nebo ve značném rozsahu je narušen vnitřní pořádek a bezpečnost, popřípadě jsou ohroženy životy a zdraví (v případě zdraví se lze poohlédnout na stále trvající pandemii COVID-19) lze dle intenzity vyhlásit nouzový stav a stav ohrožení státu, tyto stavy se vyhlašují pro omezené nebo celé území státu.

Dále lze taktéž vyhlásit válečný stav – tento se vyhlašuje pro celé území státu. V čl. 3 je definováno, že bezpečnost ČR zajišťují ozbrojené síly, ozbrojené bezpečnostní sbory, záchranné sbory a havarijní služby.

Dále je v tomto článku definována povinnost zapojení státní správy, orgánů územních samosprávných celků, právnických i fyzických osob podílet se na zajištění bezpečnosti ČR. Rozsah a další podrobnosti jsou stanoveny zákonem. V Čl. 4 se tento zákon zaměřuje na to, že ozbrojené síly jsou doplněny na základě branné povinnosti.

Následně je zde popsáno to, že rozsah branné povinnosti a úkoly ozbrojených sil a ozbrojených bezpečnostních sborů, záchranných sborů a havarijních služeb, jejich organizaci doplňování a přípravu definuje zákon, aby byla zajištěna civilní kontrola ozbrojených sil.

Potom je zde zmíněn nouzový stav. Nouzový stav řada z nás velmi dobře poznala za dobu pandemie. Tento nouzový stav byl vyhlášen, poté několikrát prodlužován a s přestávkami trval opravdu dlouhých 256 dnů, poprvé byl v souvislosti s pandemií COVID-19 vyhlášen

dne 12. března 2020 a jeho poslední trvání bylo od 27. února do 11. dubna 2021. Teď již k samotné definici nouzového stavu, která je definována v Č l. 5 a Čl. 6. Vláda má pravomoc přistoupit k vyhlášení nouzového stavu v případech živelných pohrom, ekologických, průmyslových havárií, případně jiných nehod nebo nebezpečí, které jsou ve velkém rozsahu ohrozit životy nebo zdraví, popřípadě majetkové hodnoty, nebo vnitřní pořádek a bezpečnost. Nouzový stav nelze vyhlásit z důvodu stávky vedené na ochranu práv a oprávněných hospodářsky-sociálních zájmů. V případě, že hrozí nebezpečí z prodlení, lze vyhlásit nouzový stav i ze strany předsedy vlády. Toto rozhodnutí může vláda do 24 hodin od vyhlášení schválit nebo zrušit. Vláda má povinnost informovat o vyhlášení nouzového stavu Poslaneckou sněmovnu Parlamentu České republiky, která může toto vyhlášení nouzového stavu anulovat/zrušit. V Čl. 6 je uvedena informace, že nouzový stav lze vyhlásit jen s uvedením určitého důvodu, na dobu určitou, pro určité území. S vyhlášením NS musí vláda vymezit, která práva stanovená ve zvláštním zákoně a v jakém rozsahu, se omezují, samozřejmě vůči listině základních práv a svobod. Jaké a které povinnosti se ukládají, případně v jakém rozsahu. Podrobnosti těchto záležitostí definuje zákon. NS lze vyhlásit nejdéle na dobu 30 dnů. Dobu 30 dnů trvání nouzového stavu lze prodloužit, pouze na základě předchozího souhlasu Poslanecké sněmovny Parlamentu České republiky. Nouzový stav končí v souvislosti s uplynutím lhůty pro, kterou je vyhlášen, ovšem pokud vláda České republiky nebo Poslanecká sněmovna nerozhodne o zrušení NS dříve, než tato doba uplyne.

Taktéž je zde definován stav ohrožení státu (v Čl. 7 – odst. 1 a 2). Tento stav – tedy stav ohrožení státu lze vyhlásit na návrh vlády, pokud je ohrožena svrchovanost státu či územní celistvost státu anebo jeho demokratické základy. Ke schválení, aby byla přijata možnost vyhlášení stavu ohrožení státu je nutnost souhlasu nadpoloviční většiny poslanců a nadpoloviční většiny senátorů.

Následně také zákon č. 110/1998 Sb. pamatuje na možnost zkráceného jednání o návrzích zákonů. Jak je v Čl. 8 uvedeno, v době trvání ohrožení státu popřípadě válečného stavu lze požadovat ze strany vlády, aby byl Parlamentem projednán návrh zákona ve zkráceném jednání.

Určitě stojí za zmínku, že zákon Č.110/1998 Sb. Taktéž obsahuje informaci o bezpečnostní radě státu, tu tvoří předseda vlády, tedy premiér České republiky a následně také další členové vlády. Bezpečnostní rada státu v rozsahu, který je stanoven vládou připravuje návrhy k neustálému zajištění bezpečnosti České republiky. Dále je zde zakotvena informace, že prezident ČR má právo se účastnit schůzí Bezpečnostní rady státu a má právo

vyžadovat jak od Bezpečnostní rady státu, tak i od jejich členů zprávy a projednat s ní nebo s některými členy otázky, které spadají do působnosti tohoto orgánu. Veškerá tato ustanovení se nachází v Čl. 9., odst. 1-3.

V Čl. 10 tohoto ústavního zákona se nachází informace o možnosti prodloužení volebního období. V případě, že v době NS nebo stavu ohrožení státu, případně válečného stavu podmínky na území České republiky nedovolují uskutečnit volby ve stanovených lhůtách, které jsou předurčeny pro pravidelná volební období, lze za pomocí zákona tyto lhůty prodloužit, nejdelší doba, o kterou je možno toto volební období prodloužit je šest měsíců, tedy půl kalendářního roku.

Následně ve Čl. 11, ve společných ustanoveních je uvedeno, že v případě rozpuštění Poslanecké sněmovny Parlamentu České republiky, přísluší horní komoře, tedy Senátu Parlamentu ČR rozhodovat o prodloužení či zrušení nouzového stavu, vyhlašování stavu ohrožení státu, případně válečného stavu, dále taktéž o účasti ČR v obranných systémech mezinárodních organizací, kde má ČR členství.

Dále ve Čl. 12 je uvedeno, že může horní komora rozhodnout o nouzovém stavu, stavu ohrožení státu, válečném stavu, tuto skutečnost sdělují v hromadných sdělovacích prostředcích a vyhlašuje se stejným způsobem jako zákon. Účinnost nabyde okamžikem, který je stanoven v rozhodnutí.

V závěrečném ustanovení tohoto zákona je uvedena informace, že tento ústavní zákon č. 110/1998 Sb. nabyl účinnosti dnem vyhlášení. (Zákon č. 110/1998 Sb.)

1.3 Pojmy v oblasti krizového řízení

Pojmy nejsou v oblasti krizového řízení v České republice sjednocené, přestože ze strany Ministerstva vnitra ČR a jeho odboru bezpečnostní politiky vydán Terminologický slovník pojmů z oblasti krizového řízení, tento slovník byl vydán v roce 2004.

V roce 2009 proběhla novelizace tohoto slovníku, následně prošel schválením Výboru pro obranné plánování, jež je pracovním orgánem Bezpečnostní rady státu.

Cílem vydání tohoto slovníku bylo to, aby byl výklad termínů odborné terminologie sjednocen, cílem také byla efektivní pomoc při tvorbě dokumentace pro plány případné

obrany státu. Je taky namístě zmínit to, že tento slovník uvádí i ekvivalenty k českým pojmům v jazycích cizích, tyto cizí pojmy jsou uvedeny jak v angličtině, tak i ve francouzském jazyce, je zde vhodno také zmínit, že ne všechny pojmy tento ekvivalent obsahují, nicméně je jich valná většina.

Dobré je zde, ale podotknout, že toto vydání slovníku neobsáhlo všechny oblasti, tudíž si někteří akademičtí pracovníci, případně úředníci jak ve veřejné správě, tak i případně krizoví manažeři si pořád ještě tvoří své výrazové prostředky, které jsou k jejich práci a specializaci nutné. (Antušák a Vilášek, 2016)

Je nutné si v této kapitole uvědomit, že jedním ze zásadních pojmů v oblasti krizového řízení jsou fáze vývoje krizového řízení, tento pojem vyjadřuje jak časový postup, událostí, tak i jejich samotný obsah. Dle Antušáka a jeho knihy Základy teorie krizového managementu jde dle definice zejména o fázi: *„prevence, korekce, protikrizové intervence, redukce a obnovy. Někdy také hovoříme o funkcích krizového řízení". (Antušák a Vilášek, 2016, s.40)*

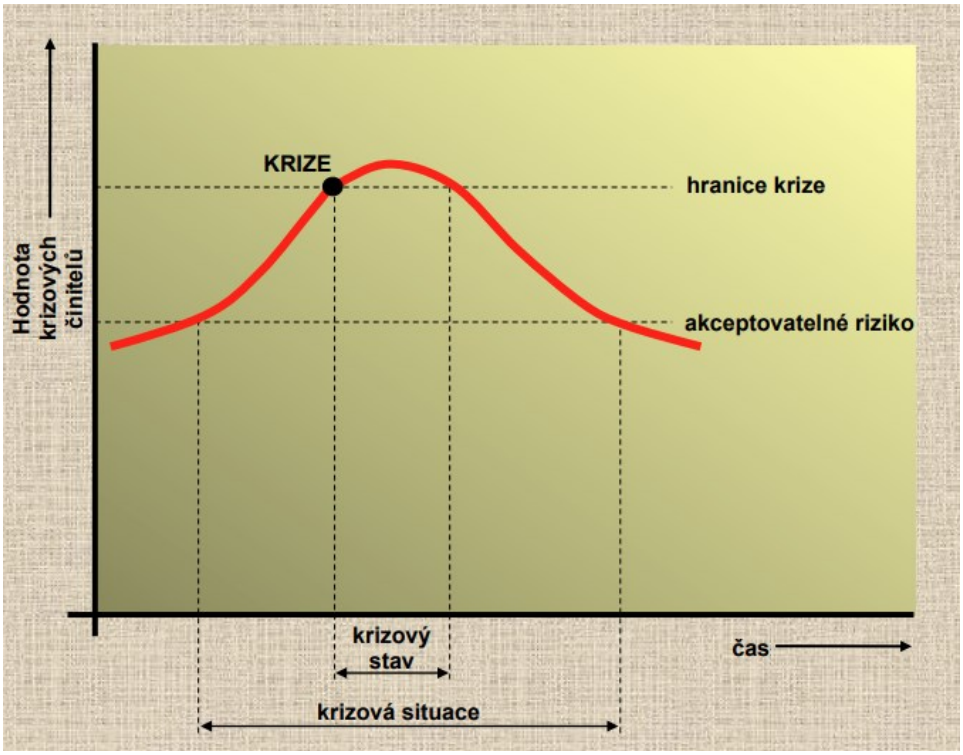
Dále je důležité zmínit pojem fáze vývoje krize. V této problematice lze říci, že se bavíme o postupu narušení systému, jeho rovnováhy, dle Antušáka lze definovat jako: „*studium symptomů, akutní stádium, chronické stádium, stádium vyřešení krize" (Antušák a Vilášek ,2016, s.40).*

Délka samotných fází je relativní, je to odvislé od typu krize, složitosti dané situace. Jako zlomové body lze označit přijatelné úrovně rizika, mez sladěnosti, na těchto veličinách je závislá disharmonie systému, který je narušen.

Toto je únosné pouze pro určité časové období, nikoliv trvale. Jedním ze zlomových bodů je práh katastrofy, nebo také mez únosnosti, při kterých je disharmonie tak velmi vyostřená, že je v podstatě nezbytným vyústěním konfrontace, případně boj. I přesto lze z praxe říci to, že veškeré krizové situace je nejvhodnější řešit s ledovým klidem, protože při zbytečném vyostření je velmi nepravděpodobné to, že jedna, či druhá strana dosáhne kýženého výsledku. (Antušák a Vilášek, 2016)

Dále je vhodné zmínit to, že je zde i pojem jako jsou krizové jevy. Do těchto krizových jevů spadají krize, krizové situace, krizové stavy. Tyto lze charakterizovat obecně jako činnosti ve stresu, popřípadě v časové tísni, při těchto jevech může vzniknou panika, šíření případných poplašných zpráv – zpravidla nepravdivých a nikde nepodložených. Nelze ovšem vyloučit ani předávání falešných informací, které na rozdíl od poplašných zpráv jsou opravdu lživé a mohou více uškodit než pomoci.

V těchto situacích a jevech, tedy krizových jevech zpravidla dochází i k narušení pracovních procesů, které jsou již zažité, vyzkoušené, ověřené celkově i v praxi a v minulosti mohly přinášet opravdu kýžené výsledky, tak v době kdy se člověk, či prostředí nachází v působnosti krizového jevu, je možné ze strany člověka chyba lidského faktoru, tudíž i zkratovité jednání, nelogické jednání, třeba i jen z toho důvodu, že se nachází pod tlakem. V těchto jevech je možné se setkat i s tím, že je rozhodováno bez podrobných analýz daných situací, jak již bylo zmíněno, je zde i šance, že jsou tato rozhodnutí přijímaná pod jistým tlakem, který ne každému vyhovuje, nicméně se ve společnosti nachází stále velké množství lidí, kteří pracují lépe pod tlakem, tedy podávají lepší výkony. V těchto krizových jevech by měla být na pomyslném žebříčku hodnot na prvním místě snaha chránit lidské životy, případně tedy zabránit maření lidských životů v případě nějakých krizových jevů, jako jsou i přírodní katastrofy, a jiné MU. (Slezská univerzita, 2007)



Obrázek č.3 – Grafické znázornění vzniku krizové situace, slu.cz, (2007, slide č.8)

Dále lze tyto krizové jevy dělit dle příčin, které tyto krizové stavy vyvolaly. Lze je dělit tedy na dvě kategorie a těmi jsou: činitele přírodní a činitele lidské. Přírodní činitele jsou tedy ty, které nebyly vyvolané člověkem, tj. jsou to například přírodní katastrofy, jako jsou sesuvy půdu, zemětřesení, sopečná činnost, případně sesuvy půdy, povodně.

Dále je vhodné dle předchozího dělení zmínit taktéž lidské činitele a těmi jsou zejména sociální krize, průmyslové havárie, terorizmus – případně válečné konflikty, ale ty mohou vplývat i z terorizmu.

Následkem těchto dvou příčin mohou také nastat sekundární krize, které mají často velmi vážný dopad, tím může být chaos – který následně může vyústit v hladomor, který je taktéž prvkem sekundární krize, případně i epidemie, a ta může následně vyvolat ekonomickou nestabilitu, v případě omezení podnikání, dále může v populaci rozvinout i psychické choroby a další. Toto je vše znázorněno přehledně v obrázku č. 4. (Slezská univerzita, 2007)

Obrázek č.4 – Rozdělení krizových jevů, slu.cz, (2007, slide č.11)

Následně lze krizové jevy a následné katastrofy kategorizovat jako přírodně klimatické, a do těch lze zařadit tektonické – voda, telurické – oheň, topologické, meteorologické – vzduch a také kosmické – vesmír. Dále je možné kategorizovat i katastrofy antropogenní, těmi mohou být civilní katastrofy, do kterých lze také zahrnout dopravní nehody, průmyslové havárie, působení toxického odpadu, jaderné havárie. V neposlední řadě lze to této kategorie, tedy antropogenní zařadit i válečné konflikty. Lze také krize dělit dle prostoru výskytu, resp. krizové jevy, také dle úrovně ohrožení, rychlosti vzniku, počtu lidí, na které tato krize, či krizový jev působí, v neposlední řadě i dle objektu, účinku faktorů. Krize má i několik stádií a její průběh lze popsat asi tak, že v prvé řadě se krize nachází ve stádiu symptomů, dále i v akutním stádiu, může se také nacházet i v chronickém stádiu, dále při případném vyřešení této krize se dostane do stádia vyřešení. (Slezská univerzita, 2007)

V předcházejících několika odstavcích byly popsány krizové jevy, kde se nacházejí, jak mohou vznikat, případně na koho a jaké prostředí mají – či nemají vliv, kolik mají stádií a jiné. Nicméně zde by bylo vhodné si osvětlit pojem krizový plán. Tento pojem je velmi důležitý pro určitý postup při řešení krizové situace. Lze o něm prohlásit zodpovědně to, že je to plánovací dokument, tedy návod, který je zpracován ze strany orgánů krizového řízení. Tento dokument slouží k vytvoření toho, aby byly jednotlivé krizové stavy zmapovány a byl vytvořen návod pro jejich řešení. Dle definice HZS ČR lze říci: *„ Krizový plán je základním plánovacím dokumentem obsahujícím souhrn krizových opatření a postupů k řešení krizových situací. Jeho účelem je vytvořit podmínky pro zajištění připravenosti na krizové situace a jejich řešení pro orgány krizového řízení a další dotčené subjekty.“* (HZS ČR, 2021)

Tyto plány jsou zpracovávány následujícími orgány: ministerstva, ČNB, státní orgány, které tuto povinnost mají uloženou ze zákona, kraje, obce, které mají statut obce s rozšířenou působností. (HZS ČR, 2021)

Určitě je zde na místě definovat co je krizový štáb, protože je to určitě velmi zásadní složkou krizového řízení. Lze jej definovat, tak, že je to orgán, který spolupracuje se složkami integrovaného záchranného systému, pomáhá koordinovat to jak se provádějí záchranné a likvidační práce, případně další úkoly ochrany obyvatelstva. Následně se podílí i na obnovení postiženého území dané obce. Mají povinnost jej zřídit pouze obce s rozšířenou působností, které jej zpravidla zařazují jako poradní orgán starosty, dále je dobré zde zmínit, že jej řídí starosta. Členové těchto krizových štábů obcí jsou členové určité bezpečnostní rady. Lze určitě prohlásit to, že čím má tým větší odbornost, tím je to lepší pro řízení daných vzniklých krizových situací. (Svaz měst a obcí České republiky, web, 2020)

Postupně je třeba si definovat hrozby a rizika, resp. jejich rozdíly. Poměrně často se stává, že ve společnosti panuje názor takový, že tyto dva pojmy je možno zcela bezchybně zaměnit, bohužel není tomu tak.

Ku příkladu v případě, že definujeme hrozbu, je třeba si přiznat, že je to fenomén, který disponuje schopností potenciálně poškodit zájmy, hodnoty, a jiné užitné záležitosti, které jsou chráněny ze strany státu. Výše tohoto fenoménu, chceme – li zopakujme název, hrozba nebo spíše míra je definována šíří škody a určitou časovou osou, je to čssto vyjádřeno pravděpodobností, chceme-li rizikem možného výskytu hrozby. Hrozby mohou být přírodního charakteru nebo může být hrozba i dána působením lidského faktoru – určité

činnosti, může být, popřípadě i státem a jinou organizací. (Ministerstvo vnitra České republiky, web)

Riziko, lze definovat, jako určitou pravděpodobnost vzniku události, která je všeobecně z bezpečnostního hlediska požadováno jakožto ne zcela žádoucí. Riziko lze za každých okolností odvodit z určité přesné hrozby.

Pravděpodobnost následků, tedy nepříznivých následků, které plynou z hrozby a případné zranitelnosti zájmu je zpravidla posuzováno za pomocí analýzy rizik, která zpravidla kalkuluje i z daného posouzení připravenosti daným hrozbám vzdorovat. (Ministerstvo vnitra České republiky, 2003)

Závěrem této kapitoly by bylo vhodné poznamenat, že před případnými hrozbami a z toho plynoucí mírou rizika, se lze chránit, a to sice za pomocí stálých tlakově odolných úkrytů, případně improvizovaných úkrytů.

V dnešní době je trendem nebýt příliš nakloněn stálým tlakově odolným úkrytům, z důvodu jejich poměrně dost vysoké finanční náročnosti jak na jejich výstavbu, tak i na jejich následnou údržbu.

Tento přístup není zcela určitě správný, protože poohlídneme-li se do minulosti, lze zde zmínit Chráněné zdravotnické pracoviště – Fakultní Thomayerova Nemocnice, Praha 4 – Krč (Objekt KO 17). Tento objekt lze charakterizovat jako podzemní nemocnici, která se nachází celkově pod úrovní okolního terénu. Konstrukce tohoto objektu sestává z monolitického železobetonu, je stále tlakově odolný. Z hlediska historie tohoto objektu lze jen okrajově poznamenat, že jeho výstavba byla zahájena v roce 1952, a šlo v tomto případě o zcela přirozenou reakci na zahájení studené války, stavba byla dokončena v prosinci roku 1961, až do roku 1990 byl tento objekt zařazen do kategorie přísně tajné. Výhodou tohoto objektu je to, že může fungovat dokonce v několika režimech, a to sice jako kryt civilní ochrany, ale také jako chráněné zdravotnické pracoviště, což je obzvláště v dnešní době určitě velkou výhodou. Tudíž je i v dnešní době velmi dobře využitelný pro tyto účely, objekt je stále plně funkční, stále tlakově odolný, vybavený potřebným vybavením, disponuje i moderními technologiemi jako je přístup do informačních systémů Thomayerovy nemocnice, jako jsou NIS = Nemocniční Informační Systém. Tudíž je tento STOU připraven k použití v případě nějaké hrozby, ať se jedná o válečný konflikt nebo současný stav, ve kterém se nacházíme, a to je epidemie COVID-19. Jediné novodobé využití bylo po roce 2000 tohoto STOU ubytování starších spoluobčanů v roce 2002, po vydatných povodních

v Praze. Dále zde byla provedena taky jedna infekční operace, která z důvodu významného rozšíření rizika šíření infekce nebyla provedena v povrchových pavilonech. Po této operaci zde proběhly odběry vzorků, zda se nenachází i po celkové desinfekci operačního sálu v jeho prostorech určité pozůstatky patogenů a na základě vyhodnocení bylo závěrem tohoto testování vyhodnoceno, že je operační sál i v dnešní době velmi bezpečný, nebyl zde nalezen žádný patogen, který by byl zdrojem potenciálního rizika. Tento objekt má tu nespornou výhodu, že k jeho zprovoznění musí dojít 60 minut od vyhlášení pokynu k aktivaci tohoto objektu, tudíž je připraven i na válečné konflikty i případné epidemie, neustále jsou v pohotovosti dva týmy zdravotníků, kteří by byly v krytu z titulu personálu. Vzhledem ke své konstrukci, tím že tento STOU disponuje i tzv. „ rozpraskovou deskou“ je schopen v případě válečného, tedy ozbrojeného konfliktu být kvůli této konstrukční vlastnosti chráněn. Disponuje taky velmi účinným filtroventilačním zařízením, které je schopno v objektu vytvořit přetlak, tak aby byl objekt chráněn proti vnějším nepříznivým vlivům, tj. nebezpečné látky jsou vytlačovány z objektu ven, nikoliv dovnitř. Celkově lze závěrem říci to, že STOU jsou i v dnešní době aktuální a velmi dobře užitelné objekty k ochraně obyvatelstva před potencionálními hrozbami. (Šafařík a Mikl, 2017)

2 BEZPEČNOST INFORMAČNÍ PODPORY

Bezpečnost informační podpory jako takové lze charakterizovat jako ochrana informačního systému proti úniku dat z těchto systémů, případné zneužití dat, nebo prevence proti ztrátě dat z úložišť těchto systémů.

Obecně lze popsat shodu v tom, že bezpečnost je výraz pro nějaká forma jistoty, pod kterou lze obsáhnout všeobecně to, že snižuje pocit ohrožení. V oblasti informačních systémů lze poznamenat, že máme příklad bezpečnosti informací. Bezpečnost informací lze popsat jako ochranu informací, v celé jejich škále a po dobu životní cyklus informace, lze to popsat jakožto ochranu ve fázích vzniku, zpracování, ukládání, přenosu i likvidace. (Jašek a Malaník, 2013)

V úvodu této kapitoly je vhodné také popsat problematiku kybernetických útoků. Kybernetický útok je obecně definován tak, kdy jeden nebo několik útočníků napadnou systém za pomocí internetu. Systém si představme tak jako osobní počítač, informační systém, či server. K tomuto útoku se zpravidla využívá speciálně připravený software. Jako obecnou strategii tohoto útoku lze popsat to, že jsou útoky standardně připravovány pro servery, které mohou obsahovat informace z důvodu například, že jsou na nich instalovány nějaké informační systémy. Jde vyjádřit jako vděčný příklad kybernetického útoku například DDoS (Distributed Denial of Server) v jednoduchém principu to znamená, že není třeba do serveru vniknout, ale stačí jej cíleně zahltit, útočník tak spouští svoji komunikaci stále dokola, jako prevenci je vhodné mít dobře nastavenou bránu firewall, kde lze omezit maximální počet datových spojení za jednotku času, tím lze spoustu rizikům předcházet. (Petrowski, 2014)

V případě řešení bezpečnostní problematiky lze poznamenat to, že každý subjekt a případně jeho bezpečnost vyžaduje individuální posouzení, dle daných podmínek a případně zájmu dotčeného subjektu. Dle publikace Bezpečnost informačních systémů, na které se podíleli autoři Jašek a Malaník si je vždy třeba v oblasti bezpečnostní problematiky položit několik otázek: *„ 1. Zda a co má být chráněno? , 2. Před čím má být předmět ochrany chráněn?, 3. Jakým způsobem a jakými prostředky má být ochrana prováděna? Odpovědi na uvedené otázky jsou závislé na řadě okolností, které z hlediska subjektu ochrany můžeme rozlišit na vnitřní a vnější.“ (Jašek a Malaník, 2013, str.11)*

V této oblasti je třeba se zaměřit na to, že je nutno informační aktiva (informační aktivum = cokoliv, co je třeba před okolní společností chránit) a infrastruktura organizací je neustále vystavena riziku ohrožení. Únik informací není pouze problémem technologickým, ale i obchodně sociálním, je totiž možnost tyto uniklé informace zneužít ve svůj prospěch, je třeba si uvědomit, že z pohledu obchodního je únik informací významné riziko, hrozí zde při úniku poškození dané společnosti, v případě, že se zaměříme na problém technologický, je lze zde s určitostí, že z tohoto pohledu je třeba možnost ohrožení technického vývoje v dané společnosti a v případě odcizení této informace obohacení společnosti jiné. Lze s jednoduchostí říci to, že zajištění ochrany informací se skládá z ochrany daných informací proti vyzrazení, případnému nechtěnému přenosu a v neposlední řade i poškození informace, ať již úmyslné či neúmyslné. V případě zabezpečování informací se je třeba zaměřit na důležitost dané informace, kterou je třeba chránit, následně od toho se odvíjí náklady na ochranu těchto informací, je třeba zvážit i ekonomickou stránku věci zabezpečení informace, je nutno zvážit to, zda se nám vyplatí danou informaci proti úniku chránit a zda je pro nás opravdu tak nesmírně důležitá. (Schou a Hernandez, 2015)

V momentě, kdy je zde zmíněna bezpečnost informací je také nesmírně důležité zde zmínit ISMS. (Information Security Management System). ISMS lze popsat jako část systému, kterým je řízena organizace, přehled pokynů a procesů, které jsou vytvořeny pro usnadnění řízení rizik v oblasti bezpečnosti informací. Je to část řízení organizace, která se zaměřuje na provoz, monitoring a následně zlepšování samotné bezpečnosti informací. (What is Information Security?, 2021)

Následně je třeba zmínit termín kybernetická bezpečnost. V souladu toho, že zde byla zmíněna i bezpečnost informací je vhodné podotknout, že se poměrně často stává, že tyto dva pojmy bývají velmi často zaměňovány, tj. bývají vykládány či definovány nesprávně. Hlavní rozdíl mezi informační bezpečnosti a kybernetickou bezpečností lze spatřit v tom, že informační bezpečnost je jednou ze zásadních součástí kybernetické bezpečnosti, nicméně se vyjadřuje výhradně vůči procesům, které se zaměřují na zabezpečení dat. Kybernetickou bezpečnost lze chápat jako obecný pojem, do kterého je zahrnuta podoblast informační bezpečnosti.

Kybernetickou bezpečnost lze definovat, jako ochranu všeobecně elektronických systémů, jako jsou počítačové sítě, zařízení, jak mobilní, tak i samotné počítače. Útoky se zpravidla dělí do různých kategorií, lze zmínit například tyto, zabezpečení sítě, zabezpečení aplikací, provozní zabezpečení a po případné katastrofě zotavení se zachováním kontinuity provozu.

Zabezpečení sítě, jak již plyne z názvu se zpravidla zaměřuje na zabezpečení počítačových sítí, dále na zabezpečení softwaru a celkově na slabá a zranitelná místa v systému. V případě, že dojde po kybernetickém útoku ke ztrátě dat, je dobré se zaměřit na zotavení, obnovení dat, která obnovit lze, zajištění provozní schopnosti dané organizace, kde se tento incident vyskytl. (Analytics India Magazine, 2020)

V prvé řadě je třeba, si ale definovat samotný pojem informační systém.

Informační systém lze definovat jako soubor zařízení, která se zapojují do sběru, zpracování, skladování a přenosu informací.

Jako součásti informačního systému lze označit za tu technickou část software a hardware, samozřejmě nelze opomenout že součástí informačního systému jsou taktéž lidé, které užívají procesně informační systém pro přenos, sběr a ukládání, případné zpracování informací, které potřebují ke svým běžným pracovním činnostem.

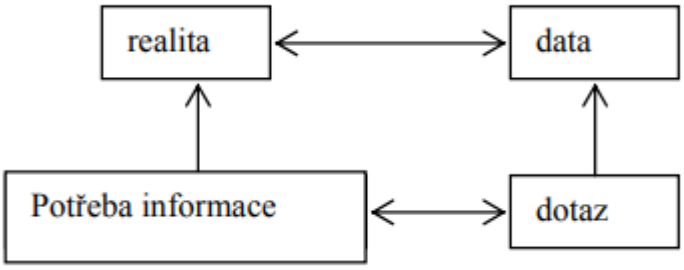
V praxi se informační systémy v podnicích používají například pro řízení dodavatelsko-odběratelských řetězců, popřípadě k jiné evidenci.

V oblasti krizového řízení se využívají pro plánování, zaznamenávání a jakožto samotná podpora krizového řízení, pro ukládání, sběr a zpracování informací pro tyto účely. (Techopedia)

Na informační systém v oblasti krizového řízení jsou poněkud odlišné požadavky, na rozdíl od podnikových informačních systémů je zde třeba specifika taková, aby tento IS odpovídal požadavkům ze strany legislativy krizového řízení.

V oblasti krizového řízení lze informační systém pro jeho podporu popsat tak, že jsou to systémy, které jsou využity ze strany orgánů krizového řízení, pro účely plánování krizových opatření, ale i pro řešení již nastalých krizových situací.

Lze s jednoduchostí popsat tato fakta, informační systém, který se sestává jakožto podpora krizového řízení musí integrovat data z jiných informačních systémů, které podporují rozhodovací a plánovací postupy. Lze i říci to, že se užívá k i při tvorbě preventivních opatření a je dostupný osobám podílejícím se na krizovém řízení, samozřejmě s předem definovanými přístupovými právy, dle hierarchie. (Katedra informatiky FEI VŠB-TU Ostrava)



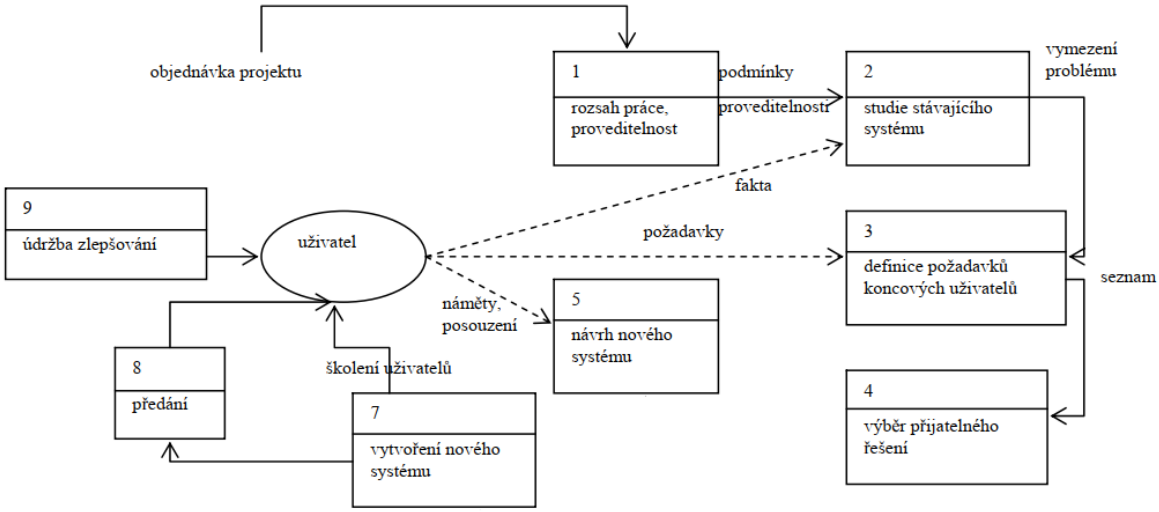
Obrázek č.5 – Základní schéma informačního systému z pohledu informatiky, (Informační systémy, 2007, str.19)

Důležité je si v této kapitole popsat i přístup uživatele vůči informačnímu systému jako takovému, konkrétní informační systém je již věc druhá, z pohledu využití v konkrétní oboru.

Uživatel, popřípadě administrátor do systému data vkládá, s tím předpokladem, že dojde k jejich dalšímu využití, v případě potřeby. Další možnost formy využití tohoto systému, tedy informačního systému je taková, že uživatel hledá data, která potřebuje dále využít, zpracovat je, předat je dále, publikovat, ať již v oblasti krizového řízení, tak i v oblastech jiných, je to princip naprosto shodný i s ostatními oblastmi. Pokud uživatel tyto data hledá, lze to zkráceně popsat jako odezva na požadavek uživatele.

Ještě je zde dobré se zaměřit na návrh informačního systémy, jsou zde prvky, které ovlivnit můžeme a které ovlivnit nemůžeme. K tomu, ale o pár vět později. Zaměřme se na pojem návrh informačního systému.

V případě návrhu jakéhokoliv informačního systému je třeba naslouchat potřebám organizace/jednotlivce, pro které/kterého se daný IS navrhuje a tím pádem je v návrhu třeba zakomponovat jeho požadavky, samozřejmě lze s úsměvem říci, že uživatel si občas přeje od informačního systému eufemisticky řečeno nereálné výstupy či výsledky, z toho důvodu je při návrhu informačního systému přistupovat na kompromisy z obou stran.



Obrázek č.6 – vývoj IS, upraveno, (Informační systémy, 2007, str.40)

Velmi dobrý přístup, je takový, pokud dvě strany diskutují o přípravě tvorby IS, vytvořit projekt informačního systému, resp. pro jeho samotnou tvorbu. V době přípravy projektu nějakého informačního systému je zde vhodné zahrnout nějakou úvodní studii, kde budou provedeny analýzy potřeby koncového uživatele, tak i obecný návrh, případně návrh podrobný. Dále je třeba implementovat samotnou myšlenku informačního systému a zařadit do daného informačního prostředí, tedy uvést myšlenku v praxi. V jednotlivých fázích je vhodno zařadit určitá východiska a analýzy, dále se zaměříme na vybraná východiska. Je důležité do IS zařadit celkovou strategii pracoviště, tj. podniku, veřejné organizace, orgánu krizového řízení, dále je třeba zhodnotit stávající IS, který je nasazen, zda se bude částečně či zcela migrovat na nový IS, případně některé jeho služby a moduly poběží paralelně, či budou od nového IS záměrně odděleny. Je třeba provést analýzu jak stavu IS, tak i kompletně IT v dané organizaci. Analýza by měla obnášet zmapování prostředí, kde bude IS využit, dále by měla proběhnout analýza vývojových trendů, tedy se zaměřit na to, co je již vyvinuto, případně zkoumat odlišnosti. Dále je třeba se zaměřit i na architektury IS, a to sice celkovou, funkční, datovou, technologickou, tyto pojmy odráží fázi informační strategie.

Dále je třeba se zaměřit na studie v případě návrhu IS a prvky těchto studií jsou východiska, návrh, řízení projektu, zajištění. Mezí východiska lze zařadit cíle projektu, analýza stavu, jak již bylo zmíněno v předcházejících větách. Ve fázi návrhu je třeba zmínit celkový návrh, funkce, funkční procesy, data se kterými je třeba pracovat, případně služby. Určitě je třeba

projekt nějak řídit, implementovat nutné procedury, standardy dané organizace, je také třeba vytvořit dokumentaci k tomuto IS. Ve fázi zajištění je nutné zajistit případnou migraci z předchozího IS, harmonogramy prací, dále je třeba se zaměřit i na ekonomickou stránku projektu, tedy tvorby samotného IS.

Po všech těchto fázích je třeba se zaměřit na uvedení do provozu, které téměř nikdy nebývá jednoduché a vždy jej provází tzv.„ porodní bolesti“ následně po uvedení v provoz tohoto systému jej provází spousta případných komplikací, které je třeba vylepšit v rámci údržby a ladění, většinou se toto realizuje na návrh uživatele, který se posoudí a případně implementuje. Taktéž je třeba zajistit fázi školení uživatelů, protože i pro ně je poměrně dosti složité přejít na nový IS. Závěrem tvorby IS je to, že přecházíme do fáze předání a následně do fáze provozu a údržby.

Jak bylo uvedeno již dříve, je vhodné se zaměřit na to, co lze návrhem IS ovlivnit a co nikoliv. Návrhem lze ovlivnit, média, kam budou ukládána data z tohoto IS, mohou to být vlastní servery, případně s nimi související disková pole nebo taktéž i možnost uložení těchto dat do cloudu, což je v dnešní době poměrně oblíbené řešení z důvodu, že není třeba se o tento hardware následně starat. Ovšem hrozí zde nepoměrně vyšší riziko zneužití těchto dat, tudíž je i vcelku logickou cestou, pokud se někdo nechce vzdát vlastního úložiště dat. Dále je v rámci kategorie, toho, co lze ovlivnit zařízení HW, na kterém tento IS chceme provozovat, v neposlední řadě lze zmínit to, že lze také ovlivnit algoritmy daného software.

Mezi záležitosti, či faktory chceme-li, které nemůžeme ovlivnit nejčastěji řadíme lidský faktor, technologie, uživatele, provozovatele, a dokonce ani administrátory těchto IS v rámci organizace, která toto provozuje. Lidský faktor ovlivnit taktéž nelze, ovšem je možno proti lidskému zavinění ošetřit některé chyby již předem. Prostředí lze občas ovlivnit, například místo, kde bude daný HW, na kterém je IS instalován, samozřejmě prostředí nelze ovlivnit z titulu internetového připojení, pokud je to defaultní nevyhovující a není zde možnost změny poskytovatele této služby, tak je třeba IS již k návrhu tohoto IS přistupovat tak, aby neměl vysoké nároky na přenos dat. V závěru teorie vývoje IS lze poznamenat to, že nejdůležitější typy IS jsou všeobecně informační systémy ekonomické, dále je třeba daný systém integrovat a mít jej komplexní pro efektivní práci. Pro vývoj IS je často tvořena celá řada různých modelů, typicky procesní a technologické. Je zde také velmi důležité zmínit to, že v samotných postupech vývoje IS se dost často objevuje požadavek na integraci IS a aplikaci vhodných metod pro zvýšení efektivity a flexibility. (Informační systémy, 2007)

2.1 Legislativa v oblasti bezpečnosti informačních systémů

V prvé řadě je třeba si uvědomit, že oblast bezpečnosti informačních systémů vychází z určité legislativy, tedy je dána ze zákona, lze zmínit například GDPR (General Data Protection Regulation), dále lze zmínit

Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti č.181/2014 Sb.).

Následně lze zmínit zákon č. 412/2005 Sb. – Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti. O veškeré této legislativě bude pojednáno níže v pořadí, v jakém byly zmíněny.

V základě je třeba se zaměřit na GDPR (General Data Protection Regulation). Je to zákon, který vešel v celé Evropské Unii v platnost, od 25. května 2018, vychází z Nařízení Evropského parlamentu a Rady (EU) č. 2016/679. GDPR je Evropský zákon, který se specializuje na ochranu osobních údajů a zabezpečení. Lze o tomto zákoně s jednoduchostí poznamenat, že se jedná o nejpřísnější zákon, který se týká ochrany osobních údajů na světě. I přes to, že je to nařízeno ze strany EU a taktéž schváleno v EU, zaměřuje se na organizace kdekoliv na světě a ukládá jim povinnost, pokud se to týká lidí v EU, resp. shromažďují údaje, které se týká lidí z EU chránit osobní údaje těchto lidí pocházejících z EU. V rámci GDPR se nachází relativně tvrdé pokutování, které se týkají jeho případného porušení. Tvrdé pokuty jsou zpravidla ukládány těm, kteří tuto směrnici EU poruší.

V případě porušení této směrnice je možno ukládat pokuty v řádu desítek milionů eur. Vzhledem k nařízení GDPR Evropská unie dosti jednoznačně dává na vědomí svůj velmi neoblomný postoj vůči ochraně osobních údajů. Je to zcela vhodné v současné době z důvodu, kdy stále více lidí využívá cloudové služby a svěřuje jim svá data.

K narušení osobních dat ze strany cloudových služeb dochází téměř denně. Dále je zde vhodné uvést vsuvku, že dle zákona č. 110/2019 Sb. Je zde třeba uvést tu informaci, že v případě nezletilých, udělení o souhlasu o zpracování osobních údajů až do věku 15 let dítěte uděluje rodič. Nařízení GDPR je poměrně dosti široké, nicméně obsahuje spousty konkrétních pojmů a předpisů, tudíž je GDPR opravdu velmi důležité respektovat do důsledku, aby se předešlo případným relativně rozsáhlým pokutám. (GDPR.EU, 2020, Zákon č. 110/2019 Sb.)

Dále je vhodné dle úvodního textu této kapitoly zmínit další legislativní nařízení, které se týká uvedené kapitoly. Tímto dalším legislativním nařízením je Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) – Zákon č. 181/ 2014 Sb.

Tento zákon o kybernetické bezpečnosti, upravuje práva, povinnosti osob, dále i pravomoc orgánů v oblasti veřejné moci v doméně kybernetické bezpečnosti. Tento zákon zahrnuje předpisy EU, dále také upravil zajištění bezpečnosti sítí a elektronických a informačních komunikačních systémů.

Hlavní cíle zákona jsou tyto, stanovení základní úrovně bezpečnostních opatření, zlepšení detekce kybernetických incidentů, zavádí hlášení těchto incidentů, taktéž zavádí opatření k reakci na bezpečnostní incidenty v oblasti kybernetické bezpečnosti, dále upravuje činnosti pracovišť, které vykonávají dohled. V tomto zákoně jsou vymezeny základní pojmy, co se rozumí kybernetickým prostorem, je to digitální prostředí, které umožňuje zpracování, výměnu, vznik informací, toto je tvořeno informačními systémy a službami, dále vymezuje, kdo je správcem informačního systému, kdo je provozovatelem informačního systému.

Dále jsou zde vymezeny orgány a osoby, kterým jsou ukládán povinnosti v oblasti kybernetické bezpečnosti. Je zde také pojednáno o bezpečnostních opatřeních, toto je zde popsáno jako souhrn úkolů, které slouží k zajištění bezpečnosti informací v informačních systémech. Je také uvedena definice kybernetické bezpečnostní události a sice je zde uvedeno, že je to taková událost, která může způsobit narušení bezpečnosti informací v informačním systému nebo bezpečnosti služeb, případně integrity sítí elektronických komunikací. Dále jsou zde uvedeny informace, které slouží k vysvětlení jakým postupem jsou hlášeny bezpečnostní incidenty. V neposlední řadě je zde uvedeno to, že je zde evidence, která zahrnuje evidování kybernetických bezpečnostních incidentů. V závěru je uvedeno, že ministerstvo vnitra stanoví vyhláškou významné informační systémy, dále stanoví úřad způsob likvidace dat, provozních údajů a informací, případně jejich kopií. (Zákon č. 181/2014 Sb.)

V následujících odstavcích budou popsány základy zákona č. 110/2005 Sb., tedy zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. V tomto zákoně jsou upraveny zásady pro stanovení utajovaných informací, podmínky pro přístup k nim, požadavky, jak s nimi nakládat, zásady, jak stanovit citlivé činnosti, podmínky pro jejich výkon a s tím svázaný výkon státní správy.

Utajovaná informace, která je v jakékoliv podobě zaznamenaná na určitém nosiči musí být označena v souladu s tímto zákonem. V případě vyzrazení tato informace může způsobit újmu zájmu ČR nebo může býti pro tyto zájmy naprosto nevhodná. Je zde také vymezeno, že újma zájmu České republiky je taková újma, či rozsah poškození, který ohrozí zájmy ČR, že dle závažnosti se újma člení na mimořádně vážnou újmu, vážnou újmu nebo prostou újmu. Dle definice z tohoto zákona může mít mimořádně vážná újma za následek ohrožení svrchovanosti a územní celistvosti České republiky, rozsáhlé ztráty na lidských životech, případně rozsáhlé ohrožení zdraví a života obyvatel.

Dále tento zákon definuje stupně utajení, a to na přísně tajné, tajné, důvěrné, vyhrazení. Jsou zde také uvedeny informace, týkající se druhů ochrany utajovaných informací, a to na základě personální bezpečnosti, kterou tvoří výběr fyzických osob, které mají přístup k utajovaným informacím. Dále je zde průmyslová bezpečnost, tuto tvoří systém k zajištění a ověření podmínek pro přístup podnikatele k utajovaným informacím a dále také zajištění nakládání s touto informací v souladu s tímto zákonem. Následně jsou zde zajištění ochrany pomocí administrativní bezpečnosti, fyzické bezpečnosti, bezpečnosti informačních, popřípadě komunikačních systémů, v neposlední řadě také kryptografickou ochranou, která je tvořena systémem opatření na ochranu utajovaných informací užitím kryptografických metod při zpracování.

Je zde také uvedena způsobilost zabezpečení ochrany utajovaných informací, tuto podmínku nesplňuje dle litery zákona podnikatel, který není schopen zajistit dodržení jednotlivých druhů ochrany utajovaných informací, dle tohoto zákona v závislosti na stupni utajení a formě přístupu k této informaci.

Následně je zde uvedena informace o režimových opatřeních. Tato opatření stanovují oprávnění vstupu osob a vjezdu dopravních prostředků do objektu kde se nacházejí zabezpečené oblasti a jednací oblasti.

Způsob kontroly těchto opatření, manipulace se vstupovými prostředky a identifikačními prostředky, které se užívají pro systémy zabezpečení vstupů dle § 30 odst1 písm. B), a způsob manipulace s danými technickými prostředky a jejich používání. Režimová opatření též stanoví oprávnění k výstupu osob, výjezdu dopravních prostředků v objektu zabezpečené oblasti, případně způsob kontroly a zabránění případnému úniku utajovaných informací.

V tomto zákoně je také zmíněna bezpečnost informačních a komunikačních systémů. Dle definice zákona je informační systém, systémem, který nakládá s utajovanými informacemi,

je to počítač včetně periferií nebo soustava počítačů, případně jejich programové vybavení, správa informačních systémů a k tomu se vztahující prostředky, které jsou schopné provádět tvorbu, zpracování a ukládání, případně přenos utajovaných informací.

V závěru lze podotknout to, že zákon pamatuje v oblasti informačních systémů i na to, že je vhodné v oblasti informačních systémů pamatovat i na bezpečné provozní podmínky jeho používání. Je zde také zmínka o tom, že komunikační systém je definován jako systém, který zajišťuje přenos informací mezi koncovými uživateli a taktéž zahrnuje koncová komunikační zařízení, přenosové prostředí, obsluhu a také provozní podmínky a postupy, tento komunikační systém nelze provozovat bez projektu schváleného Národním úřadem pro kybernetickou bezpečnost. (Zákon č. 412/2005 Sb.)

3 ANALÝZA RIZIK V OBLASTI BEZPEČNOSTI INFORMAČNÍCH SYSTÉMŮ

V této práci je třeba taktéž zmínit analýzu rizik, kterou je nutné provádět v oblasti bezpečnosti informačních systémů. A sice je to z důvodu toho, aby za pomocí této analýzy provedlo zjištění a případné odhalení zdrojů rizik v těchto informačních systémech.

Je třeba v případě tvorby nového IS zavést analýzu rizik potenciálních zranitelností, v případě stávajících systémů je vhodné provádět analýzu rizik z důvodu vylepšení stávajícího stavu zabezpečení. Tyto rizika se v rámci analýzy rizik vyjadřují za pomoci spojení následků a pravděpodobnosti, že tato rizika mohou nastat. Analýza rizik může být kvalitativní, semikvantitativní, případně kvantitativní.

V případě analýzy rizik je třeba si v první řadě definovat analýzu, resp. analytickou metodu, kterou je třeba, tedy spíše vhodno využít v rámci dané problematiky. Je třeba si také stanovit hloubku studie. Jistou důležitost zastává i popis analyzovaného systému, a to z toho důvodu, že je třeba k danému systému využít metodu, která se k němu nejvíce hodí a dává smysl.

Například metoda HAZOP je vhodná pro použití v chemickém průmyslu, tak je tedy nesmysl ji použít v oblasti řízení lidských zdrojů například. Dále je třeba si uvědomit, že je nutné ocenit závažnosti případných zdrojů potencionálního rizika, tyto zdroje je třeba jasně definovat pro správnost provedení analýzy. Taktéž je třeba identifikace případných příčin havárie, poruch a podmínek za jakých se havárie může vyskytnout. (Encyklopedie BOZP, 2005)

Nyní již k samotným metodám analýzy rizik.

V následujících odstavcích bude pojednáváno o metodách rizik, CLA – checklist, metoda What if, dále o metodě FMEA.

Analýza prováděná pomocí kontrolního seznamu – CLA je jednou z hodně jednoduchých metod, využívá seznam položek či úkolů, dle kterých je následně ověřena správnost nebo úplnost daného postupu.

Bývá často taktéž považována za základ různých sofistikovaných metod v oblastech: kvality, bezpečnosti, rizik. - Kontrolní seznam zpravidla vychází z praxe pomocí, které je také vytvořen, vůči tomuto seznamu probíhá kontrola správnosti počínání nebo stav kontrolovaného předmětu.

Výsledek může být zaznamenán jako ANO/NE nebo může být přiřazeno kontrolnímu seznamu více možnosti. Tato metoda je hojně využívána pro zjištění, zda jsou kontrolované objekty v souladu s normami nebo standardy. CLA je využitelní jako preventivní metoda, ale může být i metodou zpětného zjištění příčiny daného problému. (Analýza pomocí kontrolního seznamu – CLA)

Je to analytická technika používaná při rozhodování a řízení rizik. Princip této analytické metody je postaven na hledání různých dopadů vybraných situací.

Zjednodušeně lze tuto metodu definovat jako diskuzi a hledání nápadů. Skupina dobře obeznámených pracovníků s procesem klade otázky, vyslovuje případné úvahy o možných nehodách. Není vnitřně strukturovaná (vnitřně strukturované jsou HAZOP a FMEA).

Po osobě provádějící analýzu požaduje, aby přizpůsoboval základní koncept šetření k danému účelu.

Postup této metody je následující: Vytyčení oblasti zájmu, definice cíle – problému, generování otázek, odpovědí, závěrem je třeba definovat opatření rozhodnutí na nastalé situace.

Tato metoda má univerzální využití a výstupem této metody je popis potencionálních problémů a následné doporučení, jak jim předcházet. (Co – když analýza (What if Analysis)

Metoda FMEA je analytickou technikou, která má za cíl identifikovat místa možného vzniku vad nebo poruch v systémech.

V této metodě je postup založený na rozboru selhání a jejich důsledků, který umožňuje hledání dopadů a příčin se základem strukturovaně vymezených selhání zařízení.

Tato metoda slouží ke kontrole jednotlivých prvků systému, kde se předpokládá kvantitativní přístup řešení. Je zde možnost tuto metodu využít na celou škálu systémů.

Tato metoda také vyžaduje zkušený tým a tím pádem je založena na principu znalostí a zkušeností jednotlivých členů týmu. (FMEA (Failure Mode and Effect Analysis)

II. PRAKTICKÁ ČÁST

4 POPIS FUNKCE KONKRÉTNÍHO INFORMAČNÍHO SYSTÉMU

Nejprve je třeba si definovat co bude hlavním předmětem v praktické části. Praktická část této bakalářské práce je zaměřena na porovnání vývoje informačního systému Terex, vyvinutého společností T-soft, a.s.

Konkrétně bude probíhat porovnání desktopové starší verze 3.1.1 a aplikaci, která má uživatelské rozhraní zobrazované ve webovém prohlížeči, ta se nachází ve verzi 3.1.2.0. Je důležité zmínit, že se bude jednat především o porovnání v oblasti bezpečnosti a taktéž zde bude provedena analýza rizik.

Také je v úvodu třeba si uvést ve zkratce pro koho je tento software určen a co obsahuje, je určen zejména podnikům, institucím, samosprávným a státním orgánům, případně složkám integrovaného záchranného systému, tento systém obsahuje poměrně dosti širokou databázi chemických látek, kterou lze případně rozšířit na konkrétní užití a přizpůsobení na míru zákazníkovi, lze také s jistotou říci to, že tento software je určen pro okamžité vyhodnocení případných dopadů, či úniku nebezpečných chemických látek, případně použití nástražného výbušného systému. Je to určeno v prvé řadě pro operativní, rychlé využití, lze taktéž výsledky zobrazit přímo v mapovém podkladu.

Tato součást praktické části je velmi důležitá z důvodu zjištění potencionálních bezpečnostních rizik v těchto informačních systémech. Je nutné si v této kapitole přestavit informační systémy, o kterých se bude jednat v dalších částech této bakalářské práce. Z principu tohoto software lze říci, že je to informační systém, který je schopen okamžitě vyhodnotit dopady úniků nebezpečných chemických a otravných látek, případně nástražného výbušného systému.

Je taktéž třeba nutné poznamenat, že většina ostatních informačních systémů, které mají taktéž schopnost poskytovat určité modely v oblasti nebezpečných látek má princip v tom, že ve většině případů pracují zejména s haváriemi, kdežto tento software – Terex je v principu založen na matematickém modelu, což bylo také cílem při přípravě vývoje a projektu tohoto software. Součástí vývoje tohoto počítačového software bylo to, že probíhalo ověřování za pomocí terénních testů v praxi. Následně po vyhodnocení, a implementaci této zkušenosti byl v rámci vývoje na základě požadavku upřednostněn matematický model.

Název TEREX vychází ze spojení slov TERoristický EXpert. V rámci principu tohoto software v obou verzích, jak ve starší, tak i novější verzi lze popsat to, že zde lze snadně a jednoduše zadat vstupy, tím pádem se k tomuto váže i jednoduše interpretovatelný výstup,

chceme – li výstupy. V tomto informačním systému lze k výsledkům modelování dojít i s minimem vstupních údajů, což je jeho velkou předností. Dá se zde kombinovat odhad následků průmyslových havárií, výbuchů, popřípadě působení otravných látek. V databázi nebezpečných látek v tomto software lze najít charakteristiky těchto nebezpečných látek, jejich popis, v neposlední řadě zde lze najít zásady první pomoci a návod na případné odmoření, tedy dekontaminaci. Vzhledem k tomu, že tento informační systém je schopen poskytnout model případného úniku nebezpečné látky, popřípadě výbuchu či průmyslové havárie je vybaven také integrovaným modulem mapy, který slouží ke zobrazení výsledků – výstupů, které jsou požadované v mapovém podkladu a při využití tohoto software je tento výstup daleko názornější a užitečnější z hlediska představivosti, jak může nebezpečná látka uniknout, tedy působit na svoje okolí, toto je zakresleno v mapě.

Lze zde také zmínit to, že je v tomto informačním systému možnost taktéž exportovat výstupy, chceme – li získaná data do různých formátů jako jsou xls – dnes také i xlsx, txt, CAP a mnohé další. Je zde dobré taktéž zmínit, že je možné tento software používat ve vícejazyčných mutacích, přes češtinu, slovenštinu, angličtinu až po litevštinu, toto má za cíl využití tohoto software nejen v České republice, ale i v zahraničí.

Taktéž je velmi důležité zmínit z hlediska čistě praktického, že tento software tvoří několik modulů. Jsou to moduly pro nebezpečné chemické látky a to jsou: modely typu TOXI – tento model je schopen určit, odhadnout dosah a tvar oblaku, dle velikosti a koncentrace toxické látky. Modely typu UVCE – tento modul umí určit působnost vzdušné rázové vlny, která vyvolává detonace směsi látky se vzduchem. Model typu PLUME - tento model se zabývá déle trvajícími úniky plynu do oblaku, také únikem vroucí kapaliny s rychlým odparem do oblaku, případně pomalým odparem z louže do oblaku. Dále jsou zde modely PUFF – tento modul vyjadřuje případ jednorázového úniku plynu do oblaku, dále také únik vroucí kapaliny s rychlým odparem do oblaku Modely typu – FLASH FIRE – tento model se zabývá velikostí prostoru, ve kterém jsou ohrožovány osoby plamennou zónou (efekt Flash Fire, Jet Fire, Pool Fire) .

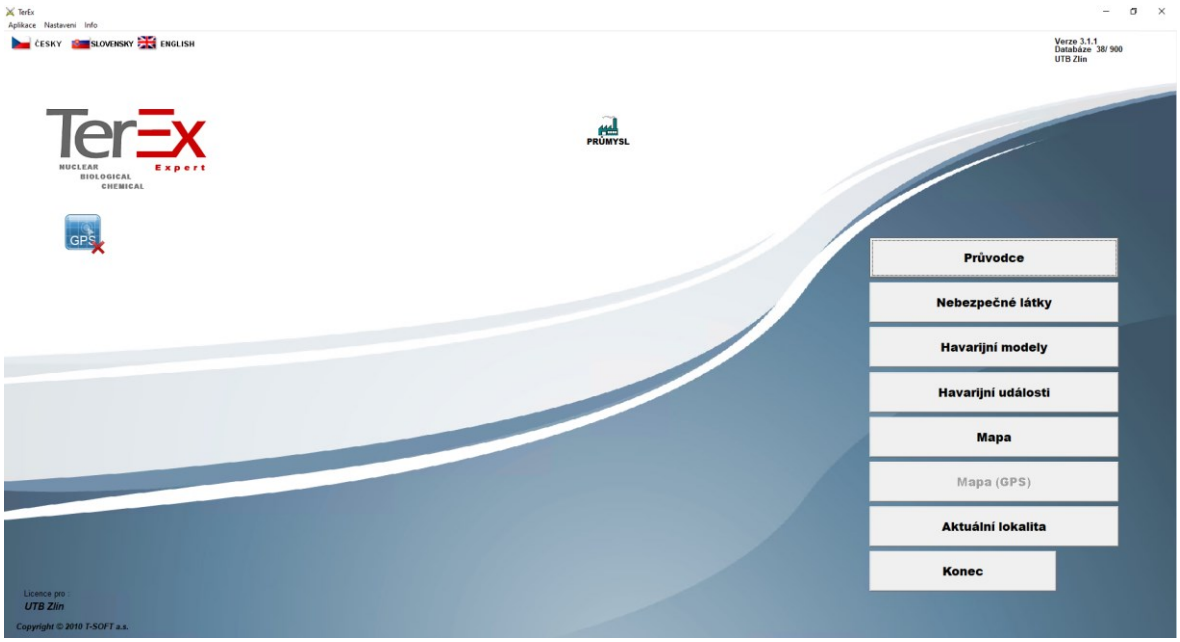
Je zde třeba také zmínit i další moduly, je zde modul, který zabývá působením výbušného systému a tím je Model typu EXPLOSIVE – zobrazuje možné dopady detonace výbušného systému, které jsou založeny na kondenzované fázi, používané s cílem ohrožení okolí detonací.

Následně je vhodné si zde popsat funkcionalitu, která se zabývá otravnými látkami a taktéž disponuje moduly, SPREAD – tento modul má za úkol vyhodnotit toxický a havarijní dosah

aerosolů, které jsou rozprášeny výbuchem a mohou být případně nosičem CBRN látek. Dále je zde modul SPREAD Explosive – slouží k porovnání havarijního dosahu nástražného výbušného systému a k vyhodnocení modelu SPREAD. Jako poslední je dobré si zmínit také model POISON - tento se zaměřuje na šíření oblaku, který vznikl rozptýlením otravné látky na definované území (podle rozlohy, typu nebezpečné látky, způsobu rozptýlení, dále také sekundárního odparu). (T- SOFT, a.s., 2006)

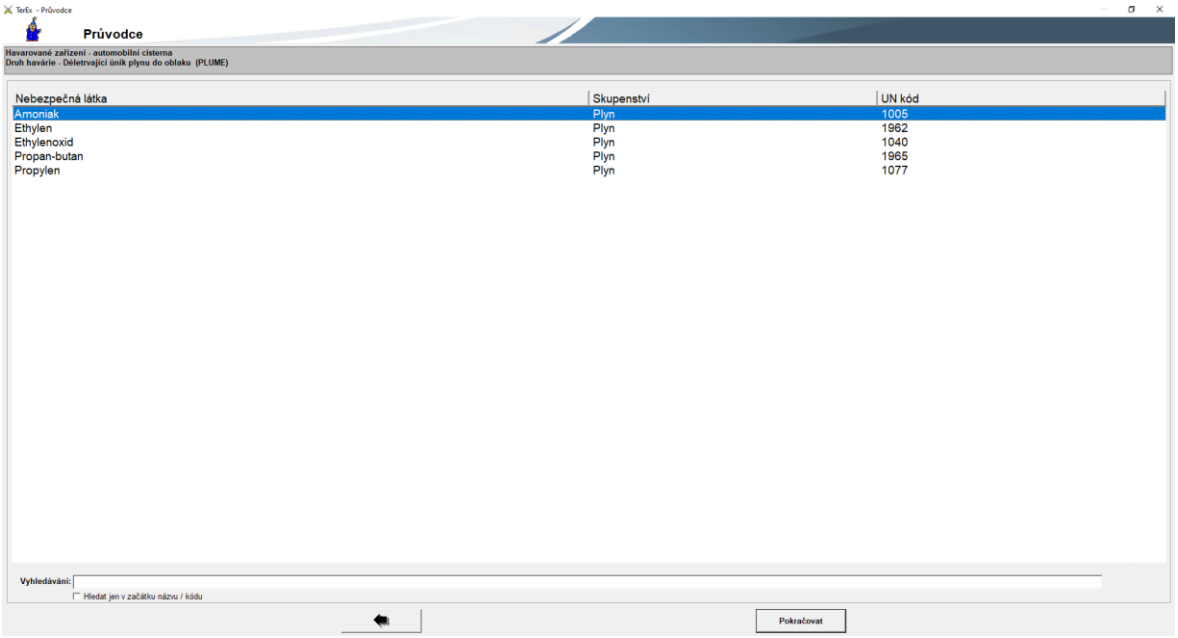
4.1 Popis konkrétní verze – desktopová verze 3.1.1 TEREX

V této podkapitole bude stručně popsána starší verze, která byla okrajově uvedena v kapitole předchozí. Je třeba zde znovu zdůraznit, že funkcionalita daných verzí je velmi podobná, v tomto případě starší verze si je třeba upřesnit to, že se nachází v klasické desktopové verzi, což může mít své výhody, ale i svá úskalí. Minimálně se sluší zmínit to, že na dnešní dobu a poměry nemá aplikace úplně nejrychlejší odezvu, tedy v porovnání s onou aplikací webovou, tj. ve verzi 3.1.2.0. Naopak významnou výhodou v tomto případě je to, že desktopová aplikace nepotřebuje přístup k internetu, tudíž je možno ji použít i mimo dosah internetového připojení. Aplikace je ve skutku jednoduchá, uživatelsky relativně přívětivá, veškerá ovládací tlačítka jsou dostupná a přehledná. Níže na obrázku č.7 bude uvedena aplikace, tak jak vypadá při spuštění pro názornou ukázku.



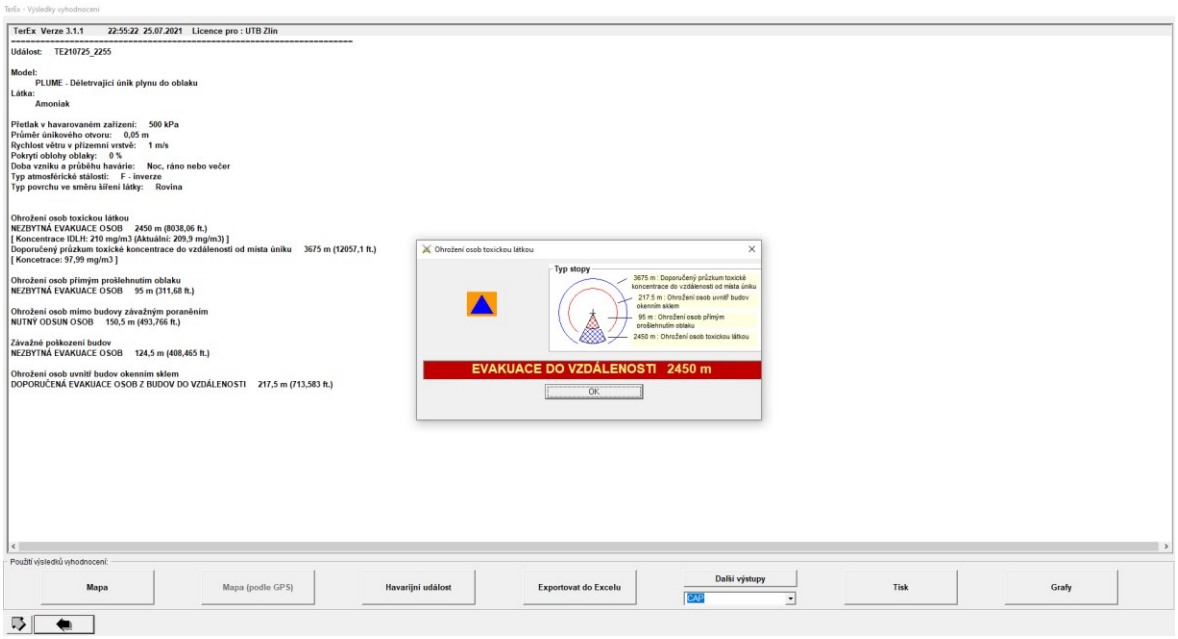
Obrázek č.7 – Úvodní obrazovka TEREX desktopová verze, (upraveno)

Jak již bylo zmíněno v předchozím textu, tak je zde opravdu přehledné ovládání, které je umístěno na pravé straně, vyjímaje kontextová menu, která jsou umístěna v horní části obrazovky. Výhodou je, že tento software v rámci opravdu operativního použití disponuje průvodcem, ve kterém si zvolíme přehledně jednotlivé parametry události, kterou potřebujeme vymodelovat a tím dostat kýžené výsledky. Po kliknutí na tlačítko průvodce se nám zobrazí nabídka, kde vybereme požadované havarované zařízení (Jako jsou automobilní cisterna, nálož, potrubní trasa, skladovací nádrž, technologické zařízení, železniční cisterna), kde potřebujeme simulovat dopady nějaké nežádoucí události. V následujícím kroku vybereme požadovanou nebezpečnou látku, pro kterou chceme získat požadované výsledky. Dále je v průvodci taktéž možné vyhledávat, například nebezpečné látky, jak podle názvu, tak dle UN kódu (čtyřčíslí, které charakterizuje danou látku), což je v případě velkého množství látek v nabízeném seznamu velmi užitečná funkce, která je schopna v případě nutné operativy ušetřit značné množství času. V případě výběru látky nezbývá nic jiného než pokračovat dále v rámci předpřipraveného průvodce. V našem případě pro účely čistě demonstrativní, tedy pro představení funkcionalit uvedeného software byl výběr havarovaného zařízení předurčen na automobilní cisternu a druh havárie byl stanoven na déletrvající únik plynu do oblaku. Jako nebezpečná látka byl vybrán amoniak. Na obrázku č. 8, tedy viz níže bude pro názornost uvedeno to, jak probíhá práce s průvodcem, který byl zmíněn o několik řádků výše.



Obrázek č.8 – Obrazovka průvodce TEREX desktopová verze, (upraveno)

Po výběru požadované nebezpečné látky lze přistoupit k dalšímu kroku naší demonstrace pro vysvětlení a tím je určení podrobností dané havárie, v našem případě lze určit přetlak v havarovaném zařízení, ve více jednotkách jak v kilopaskalech, tak i v barech. Následně se zde také určuje průměr únikového otvoru a toto lze určit jak v metrech, tak i ve stopách, v posledním řádku je určena rychlost větru v přízemní vrstvě, v metrech za sekundu, ale i ve stopách za sekundu. Níže na obrázku č. 9 bude uveden výsledek výpočtu, jak výsledek práce s tímto SW vypadá. V momentě, kdy máme všechny požadované údaje vyplněné, tak lze přistoupit k výpočtu.



Obrázek č.9 – Vysledek výpočtu, upozornění na evakuaci TEREX desktopová verze, (upraveno)

V případě výstupu zobrazeného na obrázku č. 9 je třeba ještě poznamenat, že s daty lze dále pracovat, tj. lze je exportovat do xls, případně vytisknout, v neposlední řadě je možnost zobrazit grafy jednotlivých fází, jako je doporučený průzkum, případná oblast možného výstupu, dále také ohrožení výbuchem.

Nevýhodou této desktopové verze oproti verzi, která je řešená přes webový prohlížeč, tj. ta novější je zejména to, že veškerá data je nutno někam exportovat, popřípadě tisknout, že tato verze aplikace nedisponuje, „něčím“ jakožto uživatelskou bankou vykonaných případných prací, pro případ operativy. V dnešní době je to poměrně dosti omezující faktor, z důvodu, že poměrně hodně informačních systémů běží ve webovém rozhraní a je k jejich datům přístup odkudkoliv „zevnitř“ organizace – tedy z pravidla ze vnitřní sítě a nikoliv vnější z důvodu zvýšené bezpečnosti jak dat, tak případných přístupových údajů. Další fáze

porovnání je v tom, že uložení dat na serveru, tj. v případě webového rozhraní má mnohem vyšší standard zabezpečení než samotné klientské stanice, tudíž je rozhodně v případě dané webové aplikace vhodnější využít, jak z důvodu uživatelského komfortu, tak i z důvodu vyššího standartu zabezpečení.

Navíc i způsob ověřování v případě desktopové aplikace je výrazně méně sofistikovaný. Vzhledem k tomu, že desktopová verze této aplikace byla vázána ještě na starší infrastruktuře, kde nebylo řešení přihlašování svým uživatelským jménem do domény, active directory, resp. ověřování vůči LDAPu, přesně tedy nebylo přihlašování řešeno přímo pro konkrétní uživatele, ale protože byl SW využíván pro výukové účely, přihlašování i na jednotlivé pracovní stanice probíhalo přes cca 20 definovaných uživatelských jmen ve tvaru student01 až student20, tudíž v případě nasazení tohoto způsobu přihlašování, ověřování v produkčním a ne pouze demonstrativním prostředí by nebylo docíleno kýženého standartu bezpečnosti.

V rámci toho, že toto bylo využíváno pouze pro demonstraci a výukové účely tak to bylo na svoji dobu, tedy dobu zařízení dané laboratoře, kde byl SW TEREX poskytován v desktopové verzi dostačující. Jenže v rámci toho, že i laboratoře po určité době potřebují zaznamenat určitou obměnu, tak bylo vyhodnoceno a přistoupeno k odklonu od tohoto standardu přihlašování přes tzv. „univerzální uživatelská jména“.

V souvislosti s vybudováním laboratoře s tímto nastavením přístupu k přihlašování zde byly i další aplikace, tedy zejména webové, ke kterým se přistupovalo pomocí webového prohlížeče, byla zde využívána shodná uživatelská jména, nicméně již nebyla provázána s databází active directory a neprobíhalo jejich ověření vůči LDAPU, tj. mohla nastat situace, že student01 byl ve webové aplikaci přihlášen za pomocí údajů přihlašovacích student05, což způsobovalo i relativní problém s tím, jak a jakým způsobem bylo s daty nakládáno, hrozilo jejich případné zneužití.

I v případě uložení informací z desktopové aplikace TEREX hrozilo v případě úniku dat jejich zneužití, tudíž zneužití jiným studentem (v praxi by se samozřejmě tohoto způsobu přihlášení a ověření nevyužívalo tímto způsobem, proběhla by určitá modifikace). Dále je vhodné zmínit, že tento systém přihlašování byl zvolen z důvodu instalace jiného, tedy druhého doménového řadiče oproti standartnímu, využívanému na jiných klientských stanicích. Bylo to z důvodu záměru i fyzického oddělení sítě od zbytku počítačové sítě v našem případě tedy univerzity, resp. fakulty.

Cílem a záměrem tohoto způsobu přihlašování, respektive přístupem k daným technologiím, bylo studentům přiblížit specifický přístup k laboratorním technologiím, případně přiblížit, demonstrovat využití software ve specifických podmínkách, tj. využití specifických přihlašovacích údajů, přesun výzkumných dat na jiné úložiště či médium. Často se v laboratorních podmínkách stává to, že počítače nedisponují klasickou možností přihlašování, tedy není možno se přihlásit standartními přihlašovacími údaji.

Tento specifický přístup v laboratořích je často dán i specifickou technologií, která je případně spojena se starší výpočetní technikou, kterou je často z důvodu příliš nízkého standartu bezpečnosti, tj. staršího SW a staršího, často již nepodporovaného operačního systému.

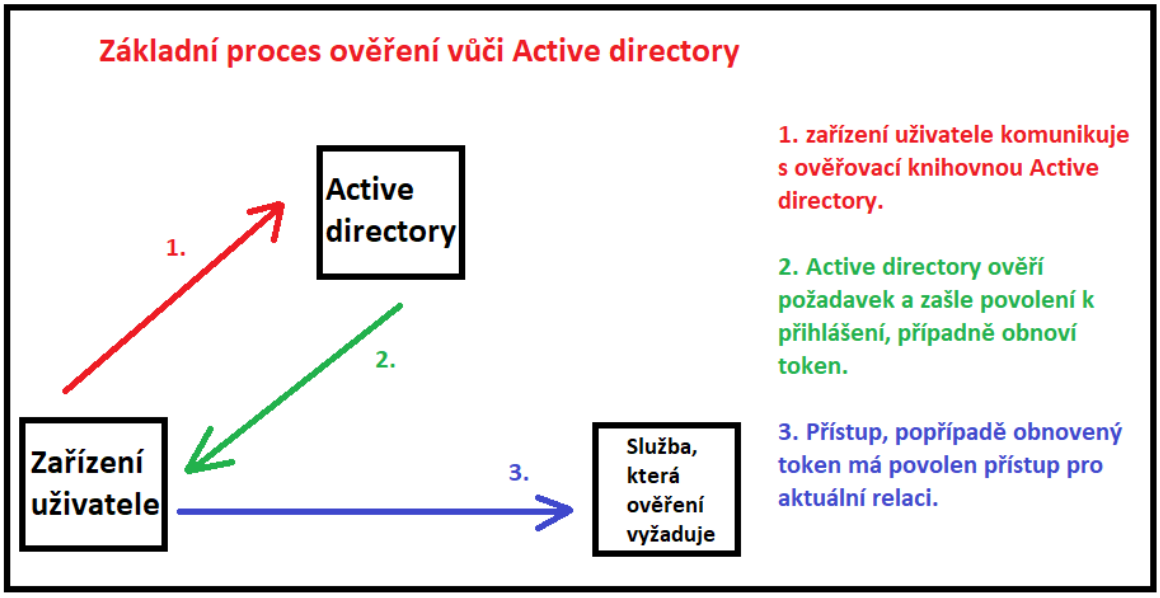
Proto se v praxi užívá i dost často přihlašování přes lokální uživatelské účty, ve kterých nedochází k ověřování vůči samotnému serveru, ale pouze na samotné klientské stanici, v mnoha případech také často v laboratorních podmínkách tyto klientské stanice, tedy koncové počítače, na kterých probíhá výzkum nebývají připojené k internetu, nutnost transportu dat tak vyvstává jakožto otázka, zpravidla se přenášejí pomocí vyměnitelných médií a popřípadě pokud nehrozí významné bezpečnostní riziko je toto přenášeno za pomocí cloudových technologií, chceme – li úložišť.

Z hlediska transportu dat, jak již bylo zmíněno vyvstává otázka, týkající se i bezpečnosti případných vyměnitelných úložišť. Používaná vyměnitelná úložiště jako jsou flash disky, tak i disky externí by měla být patřičně prověřena, aby nedošlo k narušení případného chodu laboratoří, měla by být prověřena z titulu toho, že neobsahují případný škodlivý kód, a nemůže být tedy zavlečen a laboratorní výpočetní techniku.

Důvodem takovéhoto přístupu v laboratorních podmínkách bývá často náklad poměrně vysoký na pořízení nového laboratorního zařízení, které by bylo schopno komunikovat s novější výpočetní technikou, v případě laboratoří často naprosto dostačuje soudobé vybavení laboratoře, které je často jak z pohledu výzkumného, tak i z pohledu přesnosti daného výkonu dostačující, tím pádem není úplný důvod k výměně či inovaci laboratorního SW i HW. Nicméně právě v těchto případech je nutno přistupovat k daným technologiím o to zodpovědněji, tedy snižovat riziko poškození jak HW tak i SW. Výše byly popsány přístupy k desktopové aplikaci a s ní související aplikace proč byl zvolen přístup lokálního ověření a případného oddělení sítě, bylo to ve zkratce aby bylo ve studentech vybudováno povědomí, které by je přimělo k vyšší opatrnosti a snížení případného rizika při práci s těmito systémy.

4.2 Popis konkrétní verze – webová verze 3.1.2.0 TEREX

U současné verze je dobré zmínit to, že oproti verzi předchozí má zcela dořešené přihlašování a ověřování tohoto přihlášení. Současná aplikace TEREX ve své webové verzi 3.1.2.0 je integrována do portálu, který sdružuje aplikace, jak pro laboratoř informační podpory ochrany obyvatelstva, tak i laboratoř kybernetické bezpečnosti. Přihlašování do portálu, tj. tedy i do aplikace TEREX je řešeno jednotným přihlašováním, obdobně jako je již dnes standard i přihlašování do jiných aplikací, či přímo koncových počítačů – klientských stanic. Ověření tohoto způsobu přihlašování probíhá vůči AD, resp. vůči LDAPu. Toto ověřování je výhodné zejména z důvodu bezpečnostního, a to sice z důvodu, že v případě, že probíhá ověřování přístupu vůči AD tak to má tu nespornou výhodu, v případě, že proběhne změna hesla v AD, tak se tato změna projeví ve všech využívaných systémech. Zpravidla probíhá tato synchronizace všech systémů, z pohledu změny hesla do pěti minut od samotné změny hesla, pak lze již nově vytvořené heslo využívat průřezem ve všech systémech. Na obrázku 10 viz níže je popsán proces ověření vůči active directory.



Obrázek č.10 – Proces ověření vůči active directory

V principu je proces ověření vůči active directory je relativně jednoduchá záležitost, nicméně poměrně podstatná v oblasti bezpečnosti informačních systémů. V první fázi vyšle zařízení uživatele komunikaci vůči doménovému řadiči, resp. ověřovací knihovně, poté

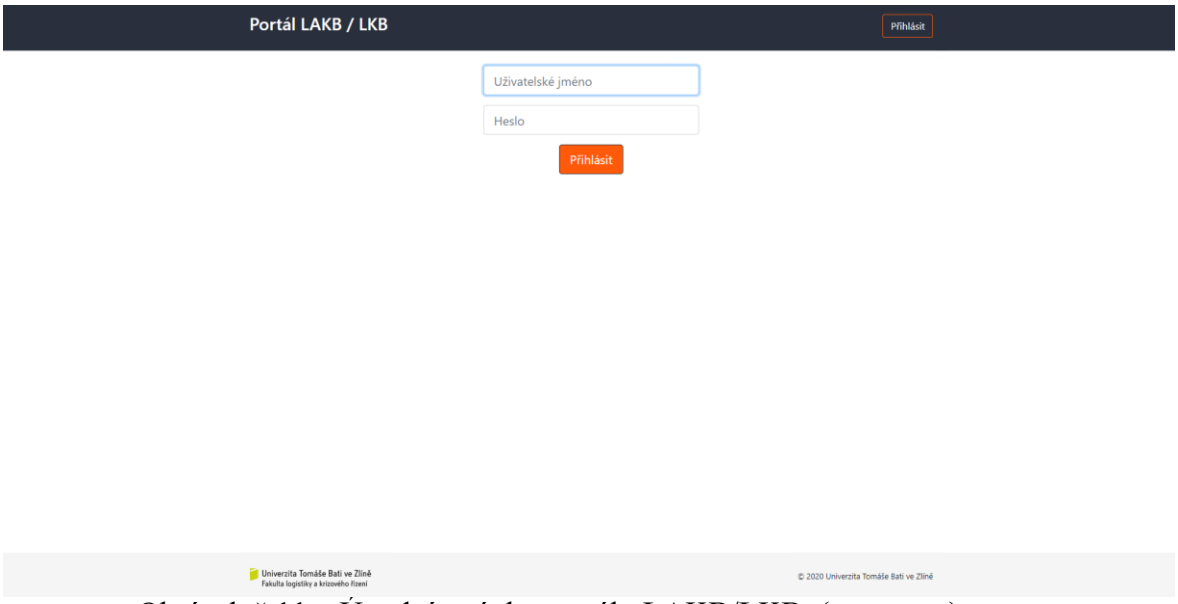
samotné active directory ověří daný požadavek vůči své knihovně. V případě shodného ověření přístup povolí a relace pokračuje. Třetí fáze je již samotný přístup, který je na základě ověření vůči AD povolen pro danou relaci a pokračuje až do přerušení nebo obnovení komunikace mezi zařízením uživatele, doménovým řadičem, resp. jeho knihovnou a službou, která toto ověření pro přístup potřebuje, při následující relaci se celý proces opakuje.

Dále je třeba si poznamenat informace týkající se webové verze. Je třeba si připomenout informaci, která se nachází o několik řádků výše. V rámci portálu, tedy úplně přesně nového portálu se nachází zcela jistě více aplikací nežli webová verze TEREXu. Nachází se zde i další aplikace, chceme-li podpůrné informační systémy, které se zabývají modelováním a simulací v oblasti krizových situací.

Nachází se zde systémy a aplikace jako jsou například Riskan, Practis, Situnet, Practis GO, Situboard. Každý z těchto systémů je určený pro jiné použití v oblasti krizového řízení a ochrany obyvatelstva. Tyto všechny systémy spojuje to, že jsou dostupné na jednom portále, jsou tedy sdružené jaksi pod jednu platformu webové stránky a není nutné je dělit na více rozcestníků z důvodu případné zbytečné složitosti.

K tomuto portálu lze dodat to, že obsahuje jak obecné informace o fungování laboratoří, tak i návody k použití daných aplikací, následně taktéž umožňuje určitou správu uživatelů, kde je možnost, jak importovat uživatele z AD, tak vytvořit uživatele i mimo AD, například pro účely testování. Také je zde umístěno značné množství podpůrných materiálů k daným aplikacím, přesněji jejich návody k použití a příklady, v neposlední řadě tento portál integruje i přístup k analytickým nástrojům kamerových systémů, které se využívají pro výuku jak na laboratoři informační podpory ochrany obyvatelstva, tak i na laboratoři kybernetické bezpečnosti.

Níže bude stručně popsáno i za pomocí obrázků pro ilustraci, jak vypadá daný portál.



Obrázek č.11 – Úvodní stránka portálu LAKB/LKB, (upraveno)

K obrázku č. 11 lze uvést ve stručnosti to, že jak již bylo zmíněno přihlášení probíhá za pomocí předem definovaných přihlašovacích údajů, v našem případě i do ostatních informačních systémů univerzity, jako jsou IS/STAG, moodle a jiné. Tedy má každý uživatel své přihlašovací údaje, tudíž je s nikým nesdílí, tedy i data si ukládá do svého předdefinovaného adresáře na portále. Je také zcela namístě zmínit tu skutečnost, že úložiště, potažmo celá infrastruktura se nachází na centrální virtualizační platformě na CVT ve Zlíně, na rektorátu, tudíž je zajištěná i případná fyzická bezpečnost z důvodu lepšího zabezpečení fyzického přístupu k serverům, taktéž je zajištěna lepší možnost chlazení, než v předchozím případě, kdy se SW nacházel fyzicky na fakultě a v neposlední řadě je zde i lepší situace týkající se i zabezpečení po SW stránce a to z důvodu toho, že je na tyto záležitosti speciálně vyškolený a vyčleněný tým CVT, který se primárně specializuje na správu serverové infrastruktury a celkově počítačové sítě UTB, tudíž neřeší podružné záležitosti jako je podpora koncových uživatelů a jiné, v neposlední řadě je tu již letitá zkušenost s centrální virtualizační platformou. Tato platforma je v základě postavená na modulárních serverech od společnosti DELL, primárně tedy na tzv. „bladech“ v doslovném českém překladu na „žiletkách“, což zapříčiňuje tu skutečnost, která obnáší velmi jednoduchou možnost modularity, tedy rozšíření, dle aktuální potřeby. Tato technologie je sice o poznání dražší než řešení rackových serverů, ale také z dlouhodobého hlediska celkově výrazně výhodnější v případě provozu typu UTB. K této infrastruktuře se samozřejmě váže i určité úložiště, které je dnes již provozováno tedy postupně přesouváno v rámci modernizace na disky, kterém neobsahují točivé části, na tzv. SSD disky, jejichž výhodou je především značně vyšší přenosová rychlost, ale s tím přirozeně souvisí i jejich vyšší pořizovací cena. Je taky

dobré v tomto případě zmínit i velký benefit centrální virtualizační platformy, jako je zálohování, které probíhá na několik míst nezávisle na sobě, z toho důvodu jsou zálohy vždy duální, a neexistuje pouze jedna kopie, toto zálohování probíhá rozdílovou metodou, tj. vždy se zálohuje jen a pouze rozdíl těchto dat. Také je na místě zmínit i to, že tato centrální serverovna má také nezávislé napájení pro případ výpadku dodávky elektrické energie a tou nezávislostí v případě výpadku standartního přívodu elektrické energie je to, že je zde umístěn diesel-agregát, tento se pravidelně zkouší, aby v případě přerušení dodávky elektrické energie nedošlo k nemožnosti jej využít z důvodu jeho případné závadě.

V závěru této kapitoly je zcela určitě vhodno popsat i samotné prostředí novější verze TEREXu, tedy jeho webové verze. Z principu dané aplikace, chceme – li informačního systému, který je schopen operativně modelovat únik nebezpečných látek, ale i výbuchy nástražných systémů či jiné lze říci, že je to velmi podobný způsob přístupu, tedy ovládání k dané aplikaci jako je u desktopové verze, taktéž se zde nachází průvodce, nicméně není tak viditelně označen jako v předchozí desktopové verzi, taktéž vybíráme havarijní model, prostředí, ve kterém toto nastane a případně i nebezpečnou látku a její množství. Přínosem oproti desktopové aplikaci může být to, že i pokud data ihned po dokončení modelace neexportujeme, tak nám nadále v rámci systému zůstávají uložena, což je jistě velkým přínosem, pokud se k datům potřebujeme vrátit, je třeba je modifikovat, upravovat, tak nemusíme tím pádem všechno vyplňovat znovu, ale je možnost tato data pouze upravit. Níže na obrázku č. 12 můžeme spatřit prostředí tohoto informačního systému v novější, chceme-li ve webové verzi, z důvodu demonstrace a předvedení daného systému.

Obrázek č.12 – Ukázka prostředí webového TEREXu, (upraveno)

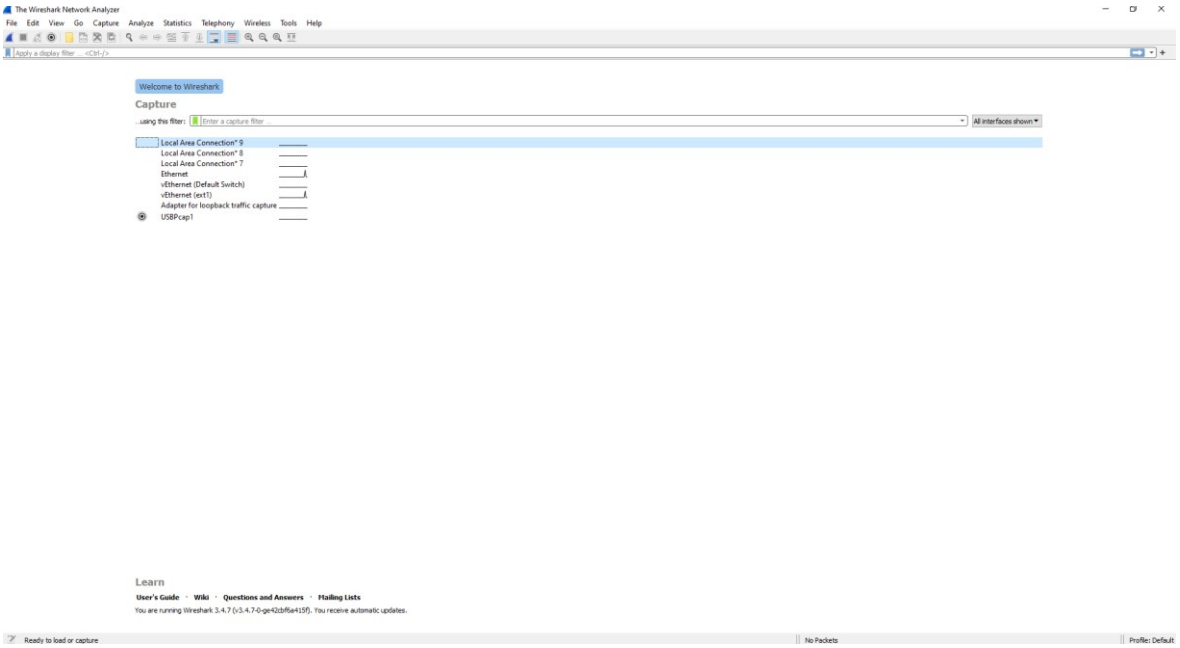
Z pohledu vyhodnocení se zde nacházejí obdobné možnosti jako u verze desktopové tohoto SW, lze získané výsledky tisknout, exportovat, či případně graficky znázornit. Tudíž je z logiky věci zbytečné opět jen z důvodu drobných grafických změn ve výstupním protokolu z tohoto IS zde znázorňovat za pomocí obrázku. I v této části jen z důvodu rekapitulace je dobré zmínit to, že je v této aplikaci se taktéž nachází i mapové podklady a případný výsledek ohrožení lze tedy zaznamenat do mapového podkladu, taktéž i tato novější verze disponuje různými možnostmi přepnutí do jiných jazykových mutací, což lze v dnešní době již považovat za standard jak u webových, tak i jiných informačních SW. Také se zde nachází možnost přehledu nebezpečných látek v databázi, dále je zde možno pohlížet přímo na havarijní modely. Závěrem tohoto vyjádření k webové verzi je záhodno poznamenat, že z titulu ovládání této verze je výrazně pohodlnější, což způsobují právě vychytané detaily na navrženém informačním systému, v dnešní době jsou požadavky zákazníků relativně vysoké a potrpí si na detaily, což je v tomto IS vidět, že oproti předchozímu IS je zde vyšší plynulost, pohodlnější ovládání, a i vyšší rychlost zpracování operativních modelů v případě potřeby.

4.3 Prověření bezpečnosti informačního systému za pomocí WireSharku

V této kapitole je třeba si představit nástroj WireShark, který slouží pro paketovou analýzu, nebo-li analýzu paketů. Pro vysvětlení si v rámci následujícího souvětí zjednodušeně definujeme, co je to paket. Paket lze označit jako jakousi jednotku, která má za úkol přenášet informaci mezi jednotlivými sítěmi. Lze ve zkratce označit jako blok dat, který zajišťuje přenos dat v počítačových sítí, které jsou tedy založeny na přepojení paketů. V případě, že za řešíme analýzu paketu, tj. řešíme obsah vlastní komunikace. Lze ve zkratce poznamenat i to, že je to metoda extrémně časově náročná, tato metoda je také vzhledem k obsahu a velikosti analyzovaných dat náročná i na kapacitu případného úložiště.

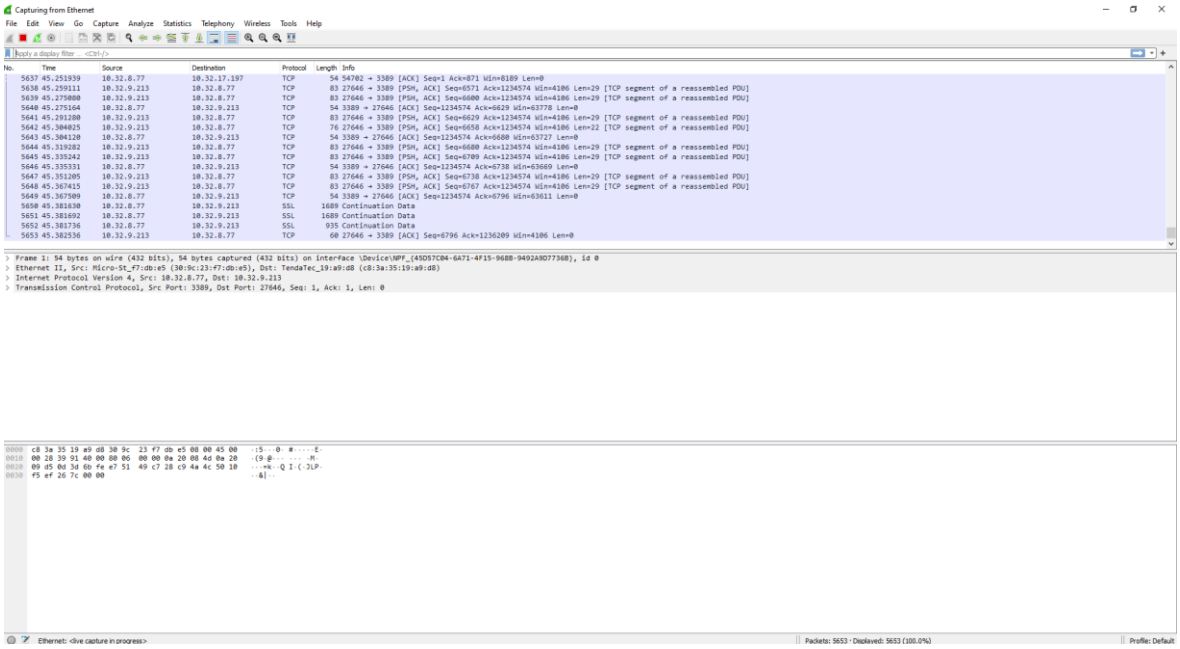
Vzhledem k tomu, že pomocí tohoto nástroje lze monitorovat síťový provoz v čase, tak je zde možnost tvořit statistiky tohoto síťového provozu, ať již o datových přenosech, tak i o zdrojové a cílové straně, tj. odkud kam putovaly pakety, odkud kam se přenášela data, při shrnutí si lze říct, že v prostředí počítačové sítě a jejího monitoringu sledujeme objem dat, čas, porty prostřednictvím, kterých probíhá komunikace, sledujeme také zdrojové a cílové IP adresy. V případě, že se, ale dostaneme do situace, kdy nám tady tyto obecné informace již nedostačují, tak musí nastoupit na scénu paketová analýza. Toto je analýza, která je zaměřena na analyzování přenášených dat, více méně, lze říci, že je to přímo analýza obsahu

komunikace. V případě analýzy provozu počítačové sítě se lze setkat s dvěma základními přístupy, a to je neustále probíhající záznam provozu v síti, ale toto je velmi časově náročné a vyplývá z toho i jistá náročnost na disková pole, obzvláště na jejich přenosové rychlosti. Další z často používaných přístupů je ten, že se sleduje pouze podezřelý provoz, na ten se zpravidla správci sítě zaměřují. V případě našeho konkrétního SW WireShark si je vhodné popsat nějaké vlastnosti a funkce, výhodou tohoto SW pro odchytávání síťového provozu je to, že disponuje grafickým rozhraním, což může být značným přínosem pro správce, kteří buďto neradi anebo nedisponují vědomostmi pracovat se softwarem v textovém režimu. Lze říci, že velmi podobný SW WireSharku existuje, je jím TCPDUMP, ale nedisponuje bohužel grafickým rozhraním, což jak již bylo zmíněno výše, tak je možnost s ním pracovat jen a pouze v příkazové řádce, což může být i pro některé správce značně nekomfortní, případně i méně přehledné, v tom případě, že jsou zvyklí pracovat s grafickým rozhraním. TCPDUMP je SW, který pracuje většinou s unixovými systémy, pro OS MS Windows existuje verze, která se nazývá WINDUMP. Nicméně tato kapitola se týká většinou SW WireShark, který bude popisován v následujících řádcích. Je důležité poznamenat to, že v rámci grafického prostředí má nástroj WireShark integrované volby filtrování, případně řízení monitoringu síťového provozu. Nespornou výhodou tohoto SW je to, že obsahuje volby, kde si uživatel, tedy v tomto případě spíše pokročilý uživatel – správce sítě nastaví rozhraní, kde je možnost vidět provoz, který se odehrává na těchto adaptérech. Velkou výhodou tohoto SW je však to, že je schopen pracovat se strukturou různých protokolů v oblasti počítačových sítí. V případě práce s tímto SW je možno zachytit data přímo online z provozu sítě, popřípadě je vyčíst z uloženého souboru, tato zachycená data lze filtrovat za pomocí filtrů, taktéž lze monitorovat i provoz v rámci USB portů. Níže na obrázku č. 13 bude zobrazeno výchozí prostředí WireSharku po spuštění.



Obrázek č.13 – Úkázka úvodní obrazovky WireShark (upraveno)

Zde na obrázku č. 13 viz výše lze spatřit možnost výchozí obrazovky v software WireShark, kde lze vidět možnosti jednotlivých síťových rozhraní v tomto SW. Lze zde u těchto rozhraní i vidět jednotlivé síťové adaptéry a vedle nich po pravé straně lze spatřit i síťový provoz, který je zde znázorněn pomocí jednoduchých grafů. V našem konkrétním případě vidíme i více možností lokálních připojení, tak i klasického ethernetu. Dále je zde vidět taktéž vEthernet, což je adaptér, který je využíván jako defaultní virtuální switch v softwaru určeném pro plnou virtualizaci, a tím je Microsoft Hyper-V. Dále je zde USBPcap1, což umožňuje zachytávání nějakého základního provozu na USB portech. V případě výběru portu klasického ethernetu, přímo připojeného do sítě, lze vidět a zachytávat síťový provoz na tomto portu viz obrázek č. 14.



Obrázek č.14 – Zachycení provozu na portu Ethernet (upraveno)

Na obrázku č. 13 lze zachytit provoz na již představeném portu výše, tedy ethernetu. Je zde možnost vidět délku trvání spojení, taktéž je zde možnost vidět zdrojovou IP adresu a taktéž i cílovou IP adresu, je zde také vidět i protokol, který se v dané komunikaci používá, ať již je to TCP, nebo SSL jako na obrázku. Dole pod zachyceným provozem lze spatřit podrobnosti, jako je rámec přenosu, počet bajtů, které byly zaznamenány na tomto rozhraní. V případě odchytávání komunikace v oblasti webového portálu je třeba zmínit, že hesla na tento portál v případě přihlašování putují v šifrované podobě a skutečně je není možno odposlouchávat, což je velkou výhodou a cestou k vysokému standardu zabezpečení.

5 ANALÝZA RIZIK KONKRÉTNÍHO INFORMAČNÍHO SYSTÉMU

V prvé řadě zde analýza rizik informačního systému bude realizována za pomocí kontrolního seznamu, tedy check-listu, označovaného taktéž někdy jako CLA. Toto nám pomůže identifikovat případná rizika pro další metody a další hodnocení těchto rizik.

Identifikace nebezpečí		
Otázka	Ano	Ne
Je místnost, kde je server uložen dostatečně zabezpečena? Přístup, limit přístupu?	Ano	
Je v případě serverové infrastruktury, resp. jejího SW vybavení prováděna pravidelná aktualizace?	Ano	
Je zajištěn náhradní zdroj energie v případě jejího výpadku?	Ano	
Jsou správci sítě v rámci údržby a podpory serverové infrastruktury patřičně proškolení?	Ano	
Probíhají pravidelné zkoušky náhradního zdroje energie, v případě jejího výpadku?		Ne
Je dobře zásoben náhradní diesel agregát naftou? Je jí dostatek na pokrytí celé doby výpadku?		Ne
Je prováděna pravidelná údržba chladícího zařízení v serverovně?	Ano	
Probíhá pravidelné testování bezpečnosti informačního systému?	Ano	
Probíhá pravidelné školení uživatelů informačního systému v oblasti jeho bezpečnosti?		Ne
Je hardwarová kapacita z pohledu výkonu dostatečná?	Ano	
Lze kapacitu hardwaru v případě potřeby rozšířit?	Ano	
Je možnost podpůrné podsystémy informačního systému sledovat I vzdáleně?	Ano	
Je databáze informačního systému dostatečně zabezpečena?	Ano	
Probíhá ověření přihlášení vůči vyšší instanci, například AD?	Ano	
Je ověřování vůči AD při přihlášení do IS dostatečně silné, funkční?	Ano	
Je ostatní infrastruktura dostatečně zabezpečena v případě napadení IS Terex?	Ano	
Jsou data, která jsou uchovávána v rámci IS příznačně chráněna?	Ano	
Existuje riziko úniku dat z tohoto IS?	Ano	

Tabulka č. 1 – CLA, checklist

Z checklistu je viditelné, že jsou zde tři odpovědi záporné, tedy o hodnotě ne, je dobré se tedy na tyto odpovědi zaměřit a následně snížit či úplně eliminovat rizika z tohoto plynoucí.

V následující tabulce je uvedeno řešení analýzy rizik plynoucí z CLA, je to řešeno metodou What-if, která rozvíjí negativní odpovědi v tabulce č.1.

P.č.	Příčina	Následek	Návrh opatření k minimalizaci (preventivní, nápravné)	Pozn:
1	Porucha na chladícím systému	Zvýší se teplota v serverovně, sníží se výkon infrastruktury, dojde k vypnutí serveru, výpadku poskytování služeb	Častější kontrola chladícího systému	
2	Porucha na diesel-agregátu	Nemožnost provozovat IS, potažmo celou infrastrukturu v době	Častější frekvence kontroly diesel-	

		výpadku primárního zdroje energie	agregátu a jeho zkoušky	
3	Napadení databáze	Případné zneužití uložených dat	Pravidelné školení v oblasti heslové politiky, případně školení obsluhy IS	
4	Neaktuální operační systém serveru	Riziko bezpečnostních děr na serveru	Kontrola pravidelnosti aktualizací	
5	Vstup nepovolané osoby do místnosti serveru	Nízké zabezpečení vstupu do serverovny. Nepozornost ostrahy v budově.	Zabezpečení vstupu do serverovny, budovy, větší ostražitost ostrahy.	
6	Nedostatečná zásoba nafty v diesel agregátu.	Nemožnost provozovat náhradní zdroj energie po nutnou dobu.	Včasná kontrola hladiny nafty.	
7	Únik dat z IS vlivem lidského faktoru	Zneužití dat třetí stranou	Lepší proškolení uživatelů IS	
8	Nedostatek HW kapacity	Nemožnost rozšiřovat, provozovat databázi	Lepší plánování, nákupu HW a rozšíření infrastruktury.	
9	Nedostatečné ověření přihlášení do IS	Riziko vstupu nepovolané osoby do IS a jeho databáze	Tvorba silnější hesel, osvěta.	

10	Uživatel IS je neproškolen	Nesprávné zacházení s informacemi v IS	Neodkladné školení uživatelů.	

Tabulka č. 2 – What-if

Analýza možných chyb a jejich následků			FMEA č.: 1
			Strana: 1 z 4
Číslo pracoviště:	Činnost: Analýza rizik informačního systému	Zodpovědnost: Ředitel IT	Datum zprac.: 1.7.2021

Současný stav									Budoucí stav					
Prvek procesu	Možná vada	Možné následky	Význam (1-10)	Možné příčiny	Výskyt (1-10)	Stávající opatření k odhalení	Odhalitelnost (1-10)	Rizikové číslo (RN)	Opatření	Zodpověd-nost --- - Termín realizace	Význam (1-10)	Výskyt (1-10)	Odhalitelnost (1-10)	Rizikové číslo (RN)
Fyzická zařízení daného IS	Porucha na chladícím systému serverovny	Zvýší se teplota v serverovně, sníží se výkon infrastruktury, dojde k vypnutí serveru, výpadku poskytování služeb	8	Poškození klimatizace, nedostatek chladiva v okruhu	4	Častější kontrola klimatizačních, chladících jednotek	10	160	Zavedení pravidelných kontrol chlazení	Správce počítačové sítě	8	1	10	80
	Porucha na diesel agregátu	Nemožnost provozovat IS, potažmo celou infrastrukturu v době výpadku	10	Nedostatek maziva v diesel agregátu, nemožnost jej nastartovat,	3	Nepravidelná kontrola bez funkčních zkoušek.	10	300	Zavedení pravidelných kontrol diesel agregátu a jeho	Správce počítačové sítě	10	1	9	90

Akceptovatelné riziko RN ≤10 | Významné riziko 10 ≤ RN ≤ 100 | Nepřijatelné riziko RN ≥ 100

Tabulka č. 3 – FMEA

Analýza možných chyb a jejich následků			FMEA č.: 1 Strana: 2 z 4
Číslo pracoviště:	Činnost: Analýza rizik informačního systému	Zodpovědnost: Ředitel IT	Datum zprac.: 1.7.2021

Současný stav									Budoucí stav					
Prvek procesu	Možná vada	Možné následky	Význam (1-10)	Možné příčiny	Výskyt (1-10)	Stávající opatření k odhalení	Odhalitelnost (1-10)	Rizikové číslo (RN)	Opatření	Zodpověd-nost - Termín realizace	Význam (1-10)	Výskyt (1-10)	Odhalitelnost (1-10)	Rizikové číslo (RN)
		primárního zdroje energie		nedostatek nafty					funkčních zkoušek					
	Vstup nepovolané osoby do místnosti serveru	Ohrožení fyzického stavu infrastruktury, nebezpečí infiltrace do sítě a jejího napadení	8	Nízké zabezpečení vstupu do serverovny. Nepozornost ostrahy v budově.	1	Přístup na klíč i karty, nepravidelná kontrola vstupujících do budovy	6	48	Omezení vstupu pouze na kartu či kód, zvýšená pozornost ostrahy.	Správce počítačové sítě	5	1	7	35
	Nedostatek výkonu HW	Možnost omezení vývoje databáze	6	Nedostatečná predikce při nákupu	4	Zběžné plánování nákupu HW	4	96	Pečlivější predikce vývoje databáze IS a ostatních systémů,	Správce počítačové sítě. Vedoucí IT	4	1	3	12

Akceptovatelné riziko RN ≤10 — Významné riziko 10 < RN ≤ 100 — Nepřijatelné riziko RN > 100

Tabulka č. 4 – FMEA

Analýza možných chyb a jejich následků			FMEA č.: 1 Strana: 3 z 4
Číslo pracoviště:	Činnost: Analýza rizik informačního systému	Zodpovědnost: Ředitel IT	Datum zprac.: 1.7.2021

Současný stav									Budoucí stav					
Prvek procesu	Možná vada	Možné následky	Význam (1-10)	Možné příčiny	Výskyt (1-10)	Stávající opatření k odhalení	Odhalitelnost (1-10)	Rizikové číslo (RN)	Opatření	Zodpověd-nost - Termín realizace	Význam (1-10)	Výskyt (1-10)	Odhalitelnost (1-10)	Rizikové číslo (RN)
									optimalizace nákupu.					
Bezpečnost IS z pohledu softwaru	Únik dat z IS	Zneužití dat třetí stranou	10	Špatné zabezpečení databáze, únik přihlašovacích údajů	3	Platnost hesel jen po určenou dobu	2	**60**	Vytvoření heslové politiky, osvěta mezi uživateli	Vedení organizace	10	1	2	**20**
	Zneužití přihlašovacích údajů	Riziko úniku dat a jejich zneužití	10	Chyba lidského faktoru, vyzrazení hesla	4	Poučení uživatelů o citlivosti přihlašovacích údajů	4	**160**	Zavedení přístupu do IS vůči podpisu a podpis zodpovědnosti za své přihlašovací údaje.	Uživatel	8	2	3	**48**

Akceptovatelné riziko RN ≤10 — Významné riziko 10 < RN ≤ 100 — Nepřijatelné riziko RN > 100

Tabulka č. 5 – FMEA

Analýza možných chyb a jejich následků			FMEA č.: 1 Strana: 4 z 4
Číslo pracoviště:	Činnost: Analýza rizik informačního systému	Zodpovědnost: Ředitel IT	Datum zprac.: 1.7.2021

Současný stav									Budoucí stav					
Prvek procesu	Možná vada	Možné následky	Význam (1-10)	Možné příčiny	Výskyt (1-10)	Stávající opatření k odhalení	Odhalitelnost (1-10)	Rizikové číslo (RN)	Opatření	Zodpověd-nost --- Termín realizace	Význam (1-10)	Výskyt (1-10)	Odhalitelnost (1-10)	Rizikové číslo (RN)
	Únik dat v důsledku DDoS útoku	Možné zneužití dat vůči svému majiteli	8	Chybné nastavení firewallu	2	Zlepšení nastavení firewallu, zlepšení monitoringu sítě	6	**96**	Lepší nastavení firewallu, již při výstavbě a implementaci IS.	Správce počítačové sítě	6	1	6	**36**
Databáze IS	Snížená stabilita databáze při vyšším zatížení, možnost jejího pádu	Nedostupnost dat, která není jednoduše predikovatelná	7	Chyby v samotném kódu IS, již při vývoji projektu.	3	Ošetření dané chyby při jejich zjištění.	5	**105**	Ošetření chyb již při vývoji IS.	Realizační tým projektu	7	1	2	**14**

Akceptovatelné riziko RN ≤10 — Významné riziko 10 < RN ≤ 100 — Nepřijatelné riziko RN > 100

Tabulka č. 5 – FMEA

5.1 Diskuze získaných výsledků praktické části

V této části proběhne diskuze výsledků, které byly získány v praktické části této práce.

V praktické části byly získány cenné poznatky v oblasti praktického využití informačních systémů, resp. informačního systému TEREx a to v jeho obou verzích. V části, kde byly porovnávány tyto aplikace byly zmíněny jejich přednosti a nedostatky, za hlavní přednost novější verze, tedy té webové je vhodno zmínit svižnost prostředí, přihlašování za pomocí vlastních uživatelských účtů, a nikoliv za pomocí účtů univerzálních. Také výhodou webové verze je to, že není nutno data nikam exportovat, pokud to v daný okamžik není nutné a lze s nimi pak dále pracovat a upravovat je. V analýze rizik těchto informačních systémů byly použity 3 metody analýzy rizik, a to metoda CLA, tedy metoda kontrolního seznamu, dále také metoda What-if. Jako poslední byla využita metoda FMEA a to z toho důvodu, že v této oblasti poskytla nejrelevantnější výsledky, tedy výsledky číselné, předchozí dvě metody sloužily jako tzv. „odrazový můstek“ pro metodu FMEA, která čerpala prvky procesu a jejich vady z předchozích metod.

V rámci metody FMEA byla jako nejvyšší rizika vyhodnocena závada na chladícím zařízení, pro toto byla také navrhnuta patřičná opatření, jak těmto případným výskytům této závady předcházet. Jako další velmi významná vada byla vyhodnocena porucha na záložním zdroji elektrické energie, v našem případě na diesel-agregátu, tím pádem by byl IS pro celou organizaci nedostupný a nebylo by jej možno v případě potřeby použít. Byla zde také z oblasti těch „fyzických" rizik zmíněna i návštěva cizí osoby v serverovně, resp. nepovolané osoby a toto je taktéž velmi významným rizikem, z důvodu možnosti jak poškození infrastruktury, tak i možného úniku dat, jako opatření zde bylo navrhnuto zavést pouze karetní systém vstupu, popřípadě číselné kódy, kde je tento vstup logován.

Za většinu těchto stavů, pokud nastanou nesou zodpovědnost správci IT, ale taktéž i ředitel IT. Dále budou popsány i rizika, za která zodpovídá i sám uživatel. Dále je zcela vhodné zmínit, že může nastat riziko i v oblasti případného nedostatečného výkonu serveru v případě ku příkladu zásadního rozvoje informačního systému, případné rozšíření jeho modulů či databáze potom již nejsou úplně reálné, zpravidla většina informačních systémů, ale i jiných procesů v této oblasti běží na serverech virtualizovaných, tak tento problém v dnešní době není již tak častý, zpravidla mezi sebou tyto dynamické prostředky sdílejí. V případě plánování nákupu HW a jeho případné obrovy je vhodné tudíž pečlivěji predikovat potřebu vývoje výkonu, aby byl vždy upgrade proveden s nějakou zásadní rezervou. Obecně lze říci to, že v rámci analýzy rizik můžeme riziko dělit na akceptovatelné, to je v našem případě stanoveno na úrovni rizikového skóre nižšího než 10, dále je toto možno dělit na riziko významné, to se pohybuje v hodnotách 10 až 100 rizikového skóre. V poslední kategorii se ovšem nachází riziko nepřijatelné, a to s hodnotou s rizikovým skóre nad 100.

Zpravidla se v oblasti analýzy rizik snažíme toto rizikové skóre navrhnutím opatření nějakým způsobem snižovat, často toto snížení rizikového skóre bývá dosti zásadní. Toto bylo také důvodem zvolení metody analýzy rizik v takovém pořadí, v jakém byly zvoleny, v prvé řadě byly zvoleny metody kvalitativní, nikoliv kvantitativní z důvodu přípravy na metodu kvantitativní, kterou je FMEA, metoda FMEA byla zvolena s ohledem na to, že je možnost za pomocí ní získat relevantní číselné výsledky, resp. je možno je ohodnotit a tím získat názorný přehled, jak vysoké riziko je. Tato metoda je v případě například porovnání s metodou HAZOP daleko vhodnější pro danou aplikaci, resp. posouzení rizik informačního systému, z důvodu, že HAZOP je metoda původně určená pro užití v chemickém průmyslu, tudíž v rámci své charakteristiky by pro použití vyhodnocení rizik informačního systému

nebyla zcela vhodná. Dále v analýze rizik, v této práci probíhalo hodnocení rizik z pohledu software, tudíž ne z pohledu fyzické bezpečnosti, ale té softwarové, chceme-li i informační bezpečnosti. Bylo zde hodnoceno i to, že by mohlo dojít k případnému úniku dat z IS, v tomto případě hrozí riziko zneužití dat třetí stranou, příčiny byly vyhodnoceny jako špatné zabezpečení databáze, případně únik přihlašovacích údajů jako soudobé opatření platnost hesel pouze po určitý časově vymezený úsek se neukázala jako vhodná, protože ze znalosti toho, jak uživatelé přistupují k heslům a jejich změnám se toto nejevilo jako vhodný přístup. Proto jako opatření bylo navrhnuto vytvoření heslové politiky, tj. složitosti hesla, použití speciálních znaků v hesle, velká, malá písmena a jejich kombinaci.

Za toto zneužití nese dle analýzy rizik a jejího vyhodnocení zodpovědnost vedení organizace, i v tomto případě byla po provedení analýzy rizik hodnota rizikového skóre značně nižší než před provedením této analýzy. Dále je zde diskutována možnost zneužití přihlašovacích údajů, které zde bylo zaznamenáno jako vyzrazení hesla, často se setkáváme s tím, že uživatel si neuvědomuje, jak zásadní informace heslo je, jakou má moc člověk, který toto heslo případně zneužije. V tomto případě bylo jako opatření zavedeno, přiřazení přístupu do IS vůči podpisu, resp. písemné žádosti a zodpovědnost za své přihlašovací údaje nese uživatel, resp. za své utajení hesla. V tomto případě došlo k redukci rizikového skóre téměř na třetinu jeho původní hodnoty, což je jasný důsledek toho, že bylo navržené opatření správné a je funkční.

Byla zde také hodnocena možnost DDoS útoku, se kterou se v dnešní době taktéž můžeme setkat, tento útok funguje na principu zahlcení serveru požadavky, který v důsledku přetížení může vykázat pád celého systému. Většinou se tento problém ukazuje jako špatně nastavený firewall, který útočníkovi umožní vůči serveru, na kterém běží IS vyslat poměrně velké množství požadavků a tím jej přetížit. Jako optimální možnost se zde nachází zlepšení nastavení firewallu, případně monitorování sítě, jak již bylo předvedeno v předchozí kapitole, lze to i za pomocí software WireShark, ale existují i jiné SW, které disponují více možnostmi než právě zmínění WireShark, lze zde například zmínit FlowMon na monitoring síťového provozu, ale i mnoho dalších. Je zde nevýhoda, že FlowMon je poměrně drahou záležitostí, a tak se může stát, že je to mimo finanční možnosti organizace, tak se použije open source alternativa v podobě WireSharku.

Jako poslední zde lze zmínit riziko snížené stability databáze, toto může nastat v momentě kdy databázi ke čtení i zápisu využívá poměrně velké množství uživatelů a tato databáze případně tak není stabilní. Zpravidla se stává i to, že se nacházejí chyby v kódu již od

samotného vývoje projektu a tím pádem je snížená stabilita již zmiňované databáze. Jako soudobé opatření je v analýze rizik uvedeno ošetření dané chyby při zjištění, ale toto je již jako ošetření následku, je vhodné toto ošetřit již při návrhu IS, resp. jeho vývoji. Za tuto případnou chybu zodpovídá dle definice z tabulky FMEA realizační tým projektu, v momentě, kdy dojde k ošetření této chyby již při vývoji IS, tak je rizikové skóre cca devětkrát nižší, než před realizací a návrhem případných opatření. Dále je také vhodné zmínit systém ukládání hesel, v době dřívější se bylo možné setkat s tím, že hesla byla mnohokrát uložena v plain textu, často nebyl využit pro protokol https, zpravidla byl využit protokol http, který nebyl zabezpečen, což již v dnešní době již téměř nevyužívaný protokol z důvodu již nedostatečné bezpečnosti. Dnes se již výhradně využívají v případě webu a webových aplikací protokoly HTTPS, a hesla se ukládají za pomocí hashů, hash lze definovat jako šifrování, které je nutné pro zašifrování hesla, či jiných informací, hash je asymetrická šifrovací funkce, tzn. Není stejný při vytvoření a při dekódování. Často se případní útočníci snaží prolomit, ale nebývá to zpravidla úplně úspěšné. Mezi vlastnosti hashování se řadí to, že výstup dat je stejně dlouhý jako jeho vstup, tudíž je nereálné získat délku hashe. Je zpravidla nereálné z hashe získat původní data před zahashovním, toto je hlavním rozdílem oproti klasickému šifrování, taktéž se nestává příliš často to, že shodným datům by odpovídal jeden hash.

V rámci této kapitoly je vhodné si zmínit to, že největší hodnotou jsou dnes data, tedy informace obsažené v informačních systémech, proto je žádoucí, aby tato data byla řádně chráněna a bylo k nim přistupováno jako k citlivým datům. Lze dále také říci to, že v desktopové verzi TERExu dříve před ošetřením chyb docházelo k problémům stability databáze, nicméně po vydání updatu, resp. nové verze toto bylo vyřešeno, dále je vhodné zmínit to, že u novější verze TEREXu, tedy té webové, je databáze ošetřena a relativně stabilní.

ZÁVĚR

Lze říci to, že informační systémy v oblasti krizového řízení jsou poměrně citlivou záležitostí z pohledu případného úniku dat. Tento únik dat z informačního systému může mít fatální následky, obzvláště v případě krizového stavu. Dle obecné praxe je to nepoměrně vyšší riziko než v případě nějakého komerčně zaměřeného podniku, protože přeci v oblasti krizového řízení je třeba nutné vyšší zabezpečení dat, protože tento únik může mít fatální následky, například v případě obrany státu, ať již v době vojenského konfliktu, nebo v případě snižování dopadu například nakažlivé nemoci v době pandemie, ve které se stále nacházíme. Dalším důležitým faktem je i vzdělanost, poučenost uživatelů, aby nakládaly se svými uživatelskými daty uvážlivě. Je sice dobré, když je správce sítě takříkajíc na „správném místě“, ale ani ten nejlepší správce sítě není schopen držet nejvyšší standardy zabezpečení, pokud si případných rizik nejsou vědomi uživatelé.

V rámci informačních systémů je také důležité dodržet určitou hierarchii přidělovaných oprávnění, tzn. Aby všichni nedisponovali přístupy do všech částí IS, a měli oprávnění přistupovat k částem IS, které potřebují ke své práci. Zamezí se tím poměrně dosti účinně případným únikům dat.

Tato práce naplňuje cíle, které se týkají bezpečnosti informačních systémů, dále byla provedena analýza rizik systémů TEREx, díky které mohly být navrhnuty opatření ke zlepšení stávajícího stavu. Z metod lze zmínit metodu CLA, tedy checklistu lze podotknout, že tato metoda může být využívána pravidelně pro kontrolu jak hardwarových částí, tak i částí softwarových z důvodu její časové nenáročnosti a její poměrně významné pomoci při odhalování i provozních rizik těchto IS. Dalším latentním rizikem je u informačních systémů sofistikovaný nápad trestné činnosti.

Lze také podotknout to, že se na trhu práce v oblasti informační bezpečnosti a kybernetické bezpečnosti je stále nedostatek pracovníků odborně způsobilých v těchto oblastech, proto lze říci, že se může i v oblasti této vyskytnout někdo, kdo není úplně přesně odborně způsobilý pro tuto oblast, tím vzniká riziko, že se u určitých pracovníků nesladí kompetence nasbírané během vzdělání a praxe, často se stává, že mají nedostatečnou praxi a i to je rizikem pro případné bezpečnostní incidenty v oblasti IS.

V případě napadení IS v době krizového stavu se dá s nadsázkou říci, že je toto rizikem jak pro strategické záměry státu, ale i případné vyzrazení utajovaných informací osobě

nepovolané, případně to může značit i dokonce ztráty na životech v případě, že to vezmeme opravdu do důsledku.

SEZNAM POUŽITÉ LITERATURY

ANTUŠÁK, Emil, 2009. Krizový management: hrozby - krize - příležitosti. Praha: Wolters Kluwer Česká republika. ISBN 978-80-7357-488-8.

ANTUŠÁK, Emil a Josef VILÁŠEK, 2016. Základy teorie krizového managementu. Praha: Univerzita Karlova v Praze, nakladatelství Karolinum. ISBN 978-80-246-3443-2.

ANTUŠÁK, Emil a Zdeněk KOPECKÝ, 2008. Krizový management: úvod do teorie. Praha: Oeconomica. ISBN 978-80-245-0951-8.

Analytics India Magazine: Difference Between Cybersecurity & Information security [online], 2020. Indie: Analytics India Magazine [cit. 2021-7-14]. Dostupné z: https://analyticsindiamag.com/difference-between-cybersecurity-information-security/

Analýza pomocí kontrolního seznamu - CLA [online]. [cit. 2021-7-9]. Dostupné z: https://managementmania.com/cs/analyza-kontrolni-seznam-cla-checklist-analysis

Co - když analýza (What-if Analysis). Managementmania [online]. [cit. 2021-7-9]. Dostupné z: https://managementmania.com/cs/co-kdyz-analyza-what-if-analysis

Encyklopedie BOZP: Analýzy rizik, 2005. Encyklopedie BOZP: Analýzy rizik [online]. x: Encyklopedie BOZP [cit. 2021-7-15]. Dostupné z: https://ebozp.vubp.cz/wiki/index.php/Anal%C3%BDzy_rizik

FMEA (Failure Mode and Effect Analysis). Managementmania [online]. [cit. 2021-7-9]. Dostupné z: https://managementmania.com/cs/failure-mode-and-effect-analysis

GDPR.EU: What is GDPR, the EU's new data protection law?, 2020. GDPR.EU: What is GDPR, the EU's new data protection law? [online]. EU: GDPR.EU [cit. 2021-7-14]. Dostupné z: https://gdpr.eu/what-is-gdpr/

HZS ČR: KRIZOVÉ PLÁNOVÁNÍ [online]. [cit. 2021-7-11]. Dostupné z: https://www.hzscr.cz/clanek/krizove-rizeni-a-cnp-krizove-planovani-krizove-planovani.aspx#:~:text=Krizov%C3%BD%20pl%C3%A1n%20je%20z%C3%A1kladn%C3%ADm%20pl%C3%A1novac%C3%ADm,%C5%99%C3%ADzen%C3%AD%20a%20dal%C5%A1%C3%AD%20dot%C4%8Den%C3%A9%20subjekty.

Informační systémy, 2007. Phoneix Inf Upol [online]. Olomouc: UPOL [cit. 2021-7-13]. Dostupné z: https://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf

JAŠEK, Roman a David MALANÍK, 2013. Bezpečnost informačních systémů. Zlín: Academia centrum. ISBN 978-80-7454-312-8.

Ministerstvo vnitra České republiky: Bezpečnostní strategie 2003, Riziko [online]. [cit. 2021-7-11]. Dostupné z: https://www.mvcr.cz/clanek/riziko.aspx

Ministerstvo vnitra České republiky, web: Bezpečnostní strategie, hrozba [online]. [cit. 2021-7-11]. Dostupné z: https://www.mvcr.cz/clanek/hrozba.aspx

PETROWSKI, Thorsten, 2014. Bezpečí na internetu pro všechny. Liberec: Dialog. ISBN 978-80-7424-066-9.

Ochrana obyvatelstva a krizové řízení: skripta, 2015. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR. ISBN 978-80-86466-62-0.

Slezská univerzita: KRIZE A KRIZOVÉ JEVY [online]. [cit. 2021-7-11]. Dostupné z: https://www.slu.cz/math/cz/knihovna/ucebni-texty/Krizovy-management/Krize-a-krizove-jevy.pdf/

Svaz měst a obcí České republiky, web: Co je krizový štáb a kdo ho zřizuje, 2020. Svaz měst a obcí České republiky, web [online]. Praha: - [cit. 2021-7-11]. Dostupné z: https://www.smocr.cz/cs/novinky/vse-o-koronaviru/a/co-je-krizovy-stab-a-kdo-ho-zrizuje

ŠAFAŘÍK, Zdeněk a Václav MIKL. VÝZNAM A POSLÁNÍ OBJEKTU CHRÁNĚNÉHO ZDRAVOTNICKÉHO PRACOVIŠTĚ – FAKULTNÍ THOMAYEROVA NEMOCNICE, PRAHA 4 – KRČ (OBJEKT KO 17). In: Trilobit [online]. s. 8 [cit. 2021-7-9]. ISSN 1804-1795. Dostupné z: http://trilobit.fai.utb.cz/Data/Articles/PDF/da893f1e-47cd-4a2c-a52a-ef6e65c0e1e4.pdf

SCHOU, Corey a Steven HERNANDEZ, 2015. Information Assurance Handbook: Effective Computer Security and Risk Management Strategies. USA: McGraw-Hill Education. ISBN 978-0-07-182165-0.

T- SOFT, a.s., 2006. T- SOFT, a.s. [online]. Praha: T- SOFT [cit. 2021-7-24]. Dostupné z: https://www.tsoft.cz/dokumentace/#undefined

Zákony pro lidi: Zákon č. 412/2005 Sb. - Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti, 2006. Zákony pro lidi: Zákon č. 412/2005 Sb. - Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti [online]. ČR [cit. 2021-7-14]. Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412#cast1

Zákony pro lidi: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), Zákon č. 181/2014 Sb., 2015. Zákony pro lidi: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), Zákon č. 181/2014 Sb. [online]. ČR [cit. 2021-7-14]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181?text=z%C3%A1kon+o+kybernetick%C3%A9+bezpe%C4%8Dnosti#cast1-hlava6

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

NATO – Severoatlantická aliance

ČR – Česká republika

STOU – Stálý Tlakově Odolný Úkryt

EU – Evropská Unie

IS – Informační Systém

KŘ – Krizové řízení

TZV – takzvaně

AD – Active Directory – adresářové služby implementované Microsoftem

LDAP – Lightweight Directory Access Protocol – protokol definovaný pro ukládání a přístup k datům na adresářovém serveru

CVT – Centrum Výpočetní Techniky

UTB – Univerzita Tomáše Bati ve Zlíně

Tj. – To je

TZN – to znamená

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH