Analýza bezpečnostních rizik IT infrastruktury vybrané organizace

David Zástřešek, DiS.

Bakalářská práce
2018

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: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**David Zástřešek, DiS.**
Osobní číslo:	**L15359**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**
Téma práce:	**Analýza bezpečnostních rizik IT infrastruktury vybrané organizace**

Zásady pro vypracování:

1. **Seznamte se s problematikou IT infrastruktury, počítačových sítí a kybernetické bezpečnosti.**
2. **Seznamte se s konkrétní analytickou metodou, která bude použita pro samotnou analýzu rizik.**
3. **Proveďte analýzu rizik IT infrastruktury na vybranou organizaci.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] DOHNAL, Jan a Jan POUR. IT v řízení podniku: MBI. Praha: Professional Publishing, 2016, 249 s. ISBN 978-80-7431-160-4.

[2] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání. Praha: Grada Publishing, 2015, 240 s. Management v informační společnosti. ISBN 978-80-247-5457-4.

[3] KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014, 622 s. ISBN 978-80-251-3825-0.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **RNDr. Jakub Trojan, MSc, Ph.D.**
Ústav environmentální bezpečnosti

Datum zadání bakalářské práce: **3. listopadu 2017**

Termín odevzdání bakalářské práce: **15. května 2018**

V Uherském Hradišti dne 15. listopadu 2017

doc. RNDr. Jiří Dostál, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení
L.S.

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

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby[1)];
- 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[2)];
- podle § 60[3)] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60[3)] 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 bakalářská práce 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 totožné.

V Uherském Hradišti 11. 5. 2018

.....
podpis studenta

---

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje bakalářské, diplomové, disertační a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy. Vysoká škola disertační práce nezveřejňuje, byla-li již zveřejněna jiným způsobem.

(2) Bakalářské, diplomové, disertační a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

(4) Vysoká škola může odložit zveřejnění bakalářské, diplomové, disertační a rigorózní práce nebo jejích částí, a to po dobu trvání překážky pro zveřejnění, nejdéle však na dobu 3 let. Informace o odložení zveřejnění musí být spolu s odůvodněním zveřejněna na stejném místě, kde jsou zveřejňovány bakalářské, diplomové, disertační a rigorózní práce, jíž se týká odklad zveřejnění podle věty první, jeden výtisk práce k uchování ministerstvu.

2) 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, § 35 odst. 3:
(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

3) 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, § 60 Školní dílo:
(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.
(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.
(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Bakalářská práce se zabývá analýzou rizik IT infrastruktury vybrané organizace. Teoretická část je zaměřena na základní popis IT infrastruktury. Jedná se o seznámení s počítačovou sítí a jejím rozlišením, druhy, hierarchií a standardy. Dále je zaměřena na obecné seznámení s analýzou rizik včetně základního představení použité metody analýzy rizik FMEA. V praktické části je uveden popis vybrané organizace a konkrétní laboratoře, na kterou byla analýza rizik zpracována. Zdroje rizik jsou analyzovány, a v konečné fázi je provedeno vyhodnocení s navrženými opatřeními.

Klíčová slova: IT infrastruktura, počítačová síť, riziko, analýza rizik, FMEA procesu

ABSTRACT

The bachelor thesis deals with the risk analysis of the IT infrastructure of the selected concrete organization. The theoretical part of the thesis is focused on a basic description of the IT infrastructure. Author describes the basic information of the computer network and its types, hierarchies and standards. There is also devoted to the general introduction to the risk analysis, including the basic presentation of the FMEA risk analysis, which was used by the author. The practical part describes the selected organization and the concrete laboratory for which the risk analysis was processed. Sources of risks are analyzed. In the conclusion the author carries out the final evaluation and describes the proposed measures.

Keywords: IT infrastructure, computer network, risk, analysis of risks, FMEA of the process

Rád bych touto cestou poděkoval vedoucímu bakalářské práce RNDr. Jakubu Trojanovi, MSc, MBA, Ph.D. za vstřícný přístup, cenné rady a podněty, které napomohly při zpracování této bakalářské práce. Dále bych chtěl poděkovat panu Milanu Hlůškovi, IT technikovi FLKŘ a Ing. Slavomíře Vargové, Ph.D. za ochotu a jejich čas věnovaný poskytnutí informací pro bakalářskou práci a také Mgr. Kristýně Krahulcové, Ph.D. za pomoc při jazykové korektuře.

V neposlední řadě děkuji mé přítelkyni, jejímu synovi, všem členům rodiny a známým za podporu a oporu v průběhu studia.

OBSAH

ÚVOD

IT infrastruktura, počítačové sítě, bezpečnostní rizika, kybernetická bezpečnost a internet. To vše jsou pojmy, které zná široká veřejnost. Většina z nás si dovede představit, co se za těmito názvy skrývá. Vždyť kdo dnes nevlastní mobilní telefon vybavený operačním systémem Android, Windows Mobile, i OS či dříve používaný Symbian OS apod., nebo notebook, stolní počítač či tablet, kde je operační systém Windows. A to i přesto, že existují další různé linuxové distribuce či Mac OS. To vše jsou zařízení a v nich běžící systémy, které dnes a denně používáme v soukromé i pracovní sféře. Tato zařízení spolu komunikují a jsou propojena způsobem, který stojí na nějaké IT infrastruktuře či počítačové síti. S tím souvisí výhody i bezpečnostní rizika.

Dále tu máme dnes snad už nepostradatelný internet, který také dokáže všechna zařízení propojit a umožnuje sdílení dat a informací. Bez tohoto elementu si dnes již náš život nedokážeme představit. A to nemám na mysli jen osobní stránku věci. Vždyť přes tuto síť sdílejí (na různé úrovni a zabezpečení) data bezpečnostní složky států, fungují na ní dopravní systémy, státní i soukromé organizace, pomáhá ve sféře vzdělávání, šíří se přes ni všemožné druhy informací (internetové noviny, deníky, blogy, sociální sítě apod.). Nepostradatelnou složkou, bez které by internet nefungoval, jsou servery. Úlohou těchto zařízení je ukládání a sdílení různých druhů dat pro potřeby uživatelů sítě. Poskytují ostatním počítačům v síti určité služby (souborové, aplikační, tiskové, databázové atd.) a současně plní funkci řídícího prvku v síti.

V poslední době je na velkém vzestupu také tzv. internet věcí. V jednoduchosti ho lze definovat jako síť fyzických zařízení se síťovou připojitelností, která umožňuje těmto zařízením se propojit a vyměňovat si data. Řadíme sem chytré ledničky, pračky, myčky, televize, ale také automobily apod.

Jenže dokážeme tuto vybudovanou a neustále se rozvíjející infrastrukturu nejen využívat, ale i dobře zabezpečit a chránit? Přestože se to někomu nemusí zdát, i člověk je její nedílnou součástí. Leckdy je to právě on, kdo se stává nejslabším článkem řetězu. Proto se v dnešní době stále více dostává do popředí otázka bezpečnosti, a s tím související analýza rizik. Pokud se chceme účinně bránit, je potřeba znát rizika a snažit se je co nejlépe eliminovat. Nejedná se jen o hardwarové či softwarové části, ale rovněž element lidského chování a přístup k bezpečnosti.

Teoretická část této práce má uvést do problematiky počítačových sítí a kybernetické bezpečnosti, a to včetně použité analytické metody. Praktická část tyto teoretické poznatky využívá pro provedení samotné analýzy rizik. A to na konkrétní organizaci – Fakultě logistiky a krizového řízení na Univerzitě Tomáše Bati ve Zlíně, reprezentované laboratoří Geografických informačních systému na Ústavu environmentální bezpečnosti.

I. TEORETICKÁ ČÁST

1 PROBLEMATIKA IT INFRASTRUKTURY, POČÍTAČOVÝCH SÍTÍ A KYBERNETICKÉ BEZPEČNOSTI

V této části bakalářské práce se budu zabývat uvedením do oblasti IT infrastruktury a počítačových sítí. Bude se jednat o základní přiblížení dané problematiky. Zaměřím se také na bezpečnostní hledisko a oblast kybernetického prostoru.

Infomační technologie (IT) jsou fenoménem, který se v průběhu let stal významnou součástí prakticky jakékoliv organizace, podniku či instituce, a to od těch nejmenších až po ty největší nadnárodní korporace. Pro většinu těchto institucí je příznačné, že IT se stále více stávají součástí jejich nejrůznějších aktivit. Téměř všechny řídící, správní a další aktivity jsou založeny na IT a jejich funkcích, a jsou s nimi velmi úzce provázány. Zatímco v minulosti se řízení IT chápalo jako zvláštní sféra, více či méně odříznutá od ostatních, tak v současnosti se považuje stále silněji za jeho standardní, integrální součást. Jako příklad nám může posloužit internet věcí (IoT).[1]

V centru pozornosti informatiky, tedy i IT infrastruktury, je informace. Informace je pojmenování pro obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním.[2] Mezi základní vlastnosti informace patří její pravdivost, srozumitelnost, včasnost, relevantnost a etické hledisko.[3] Výměna informace, tj. komunikace, je přenosem informace mezi minimálně dvěma účastníky prostřednictvím systému znaků. Dále máme pojem data (údaj). Je to formalizovaný záznam lidského poznání pomocí symbolů (znaků), který je schopný přenosu, uchování, interpretace či zpracování. Smysluplná informace pak vzniká v procesu interpretace dat člověkem.[4]

Také existuje termín systém. Ten je tvořen prvky a závislostmi mezi nimi, tedy vazbami. Systémem je například škola, jeho prvky mohou být studenti, studijní obory (předměty) a

---

[1] DOHNAL, Jan a Jan POUR. *IT v řízení podniku: MBI*. Praha: Professional Publishing, 2016. ISBN 9788074311604.
[2] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 9788024754574.
[3] RAK, Jakub. *Aplikovaná informatika - Základy informatiky a IT* [online]. s. 6 [cit. 2018-02-28]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=6085. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.
[4] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 9788024754574.

vazby reprezentují vztahy mezi nimi. Podstatnou charakteristikou systému je okolí (prostředí), tj. ostatní školy apod. V závislosti na tom, zda je nějaký prvek daného systému v interakci s prostředím či nikoliv, můžeme hovořit o otevřených nebo uzavřených systémech.[5]

Dalšími významnými charakteristikami systému pro pochopení principů informatiky jsou jeho struktura, stav a chování. Strukturou rozumíme způsob složení, uspořádání a stavbu prvků systému a jejich vztahů, jejichž vlastnosti jsou vyjádřeny atributy. Hodnoty atributů v určitém okamžiku utvářejí stav systému. Chování systému je reprezentováno akcí, reakcí a odezvou systému na vzniklé podněty, převážně z jeho okolí.[6]

1.1 Počítačové sítě a Internet

Dnešní internet je pravděpodobně největší technický systém, který kdy lidstvo vytvořilo. Obsahuje stovky milionů připojených počítačů, komunikačních spojení a přepínačů. Miliardy uživatelů, kteří se připojují prostřednictvím notebooků, tabletů a smartphonů. Také řady nově připojených zařízení, jako jsou například senzory, webové kamery, herní konzole, rámy obrazů, a dokonce i pračky tvořící tento systém.[7]

1.1.1 Počítačové sítě a jejich rozlišení

Počítačová síť je souhrn technického a programového vybavení, které umožňuje vzájemné propojení počítačů za účelem komunikace a sdílení uživatelů. Také ní rozumíme datové propojení dvou a více počítačů, které lze využívat za účelem mnoha funkcí. Mezi ty hlavní patří sdílení dat a aplikací na dané síti. Dalším je vzájemná komunikace, a to nejen v rámci vnitřní sítě (např. organizace), ale také na mezinárodní (celosvětové) úrovni.[8]

Vybavení počítačové sítě se rozlišuje na:

---

[5] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 9788024754574.

[6] Tamtéž

[7] KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

[8] RAK, Jakub. *Aplikovaná informatika* [online]. 86 s. [cit. 2018-02-28]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.

- **Technické:**
  - Kabely sítě nebo bezdrátové technologie.
  - Aktivní prvky počítače (síťové karty).
  - Aktivní prvky sítě (switch, router, bridge, getaway).
- **Sdílený hardware:**
  - Sdílení procesorového času.
  - Sdílení paměťových médií.
  - Sdílení tiskáren.
  - Sdílení připojení k vnější síti.
- **Programové vybavení:**
  - Síťová nadstavba operačního systému.
  - Vlastní operační systém.
- **Sdílení software:**
  - Sdílení programového vybavení.
  - Sdílení jednotlivých aplikací.[9]

1.1.2 Druhy počítačových sítí

Kritérií, podle nichž můžeme dělit, je více. Mezi hlavní patří klasifikace podle rozlehlosti:

- **Lokální počítačová síť LAN** (Local Area Networks). Je omezena na jedno lokální místo (podnik, místnost, budova). Zajišťuje sdílení lokálních prostředků (tiskáren, dat, aplikací).
- **Městská počítačová síť MAN** (Metropolitan Area Network). Je větší než LAN, ale menší než WAN.
- **Rozlehlá počítačová síť WAN** (Wide Area Networks). Skládá se z více vzájemně propojených sítí LAN. Jejich spojení se provádí speciálními linkami či bezdrátově. Rozlehlost může být různá (firma s pobočkami ve více městech, zemích nebo kontinentech až po nejznámější celosvětovou síť Internet).[10]

---

[9] RAK, Jakub. *Aplikovaná informatika* [online]. 86 s. [cit. 2018-02-28]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.

[10] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 9788025131763.

Tabulka 1. Sítě podle velikosti (zdroj dat: [11,12])

SÍT	CHARAKTERISTIKA	ROZSAH
LAN	Obvykle se skládá z osobních počítačů doplněných o potřebné hardwarové prostředky (síťové adaptéry, konektory) a spojené síťovými kabely. Pro funkci jednotlivých komponentů jsou využívány softwarové prostředky (operační systém, aplikační software), které mohou být na jedné nebo několika platformách operačních systémů. Přenosová média jsou různá (kroucené dvojlinky, koaxiální kabely, optické kabely).	Do 1 km
MAN	Rozsahově větší než LAN o oblasti několika měst. Podobnost s LAN jen s tím rozdílem, že zde jsou využity i veřejné komunikační sítě pro spojení uvnitř MAN. V dnešní době příliš nepoužívaný druh sítě.	Do 75 km
WAN	Sítě se skládají z řídících prvků (uzlové počítače – prvky), které jsou navzájem propojeny pomocí komunikační podsítě (různých typů – pevné linky, optické kabely, mikrovlnné a družicové spojení). Uzly jsou obvykle výkonné počítače, které jsou schopné sloužit většímu počtu uživatelů současně a pracují nepřetržitě. V poslední době se za uzly používají i jednotlivé LAN, které mezi sebou komunikují. Propojení probíhá zprostředkovaně, kdy zpráva je předávána postupně od jednoho prvku ke druhému, a to až k cílovému místu.	Nad 75 km

1.1.3 Hierarchie počítačových sítí

Základní rozdělení je:

- **Peer-to-Peer** (rovný s rovným). V tomto případě data zůstávají tam, kde byla uložena a dochází k jejich sdílení. Žádný z počítačů nemá roli nadřazeného ani podřízeného prvku. Všechny jsou na stejné úrovni. V síti jsou provozovány pouze pracovní stanice, které jednotlivě nabízí ostatním stanicím prostředky a služby ke sdílení. Tento princip je využíván v jednodušších sítích bez požadavku na zabezpečení.

[11] RAK, Jakub. *Aplikovaná informatika* [online]. 86 s. [cit. 2018-02-28]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.
[12] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 9788025131763.

- **Server / Client** (nadřazený prvek / klient). Server poskytuje (nabízí) službu, kterou klient využívá dle svého uvážení. Tato síť se skládá z počítače nadřazeného ostatním. Ten se označuje jako server. Dále je složena z velkého počtu podřízeních počítačů neboli klientů. Server má speciální funkce. Běží na něm operační systém úzce spjatý se síťovými prostředky a služby, které kontrolují a řídí síť. Rovněž nabízí prostředky ke sdílení. Klienti se k serveru přihlašují podle přidělených přístupových práv, na jejichž základě mají možnost využívat služeb serveru.[13]

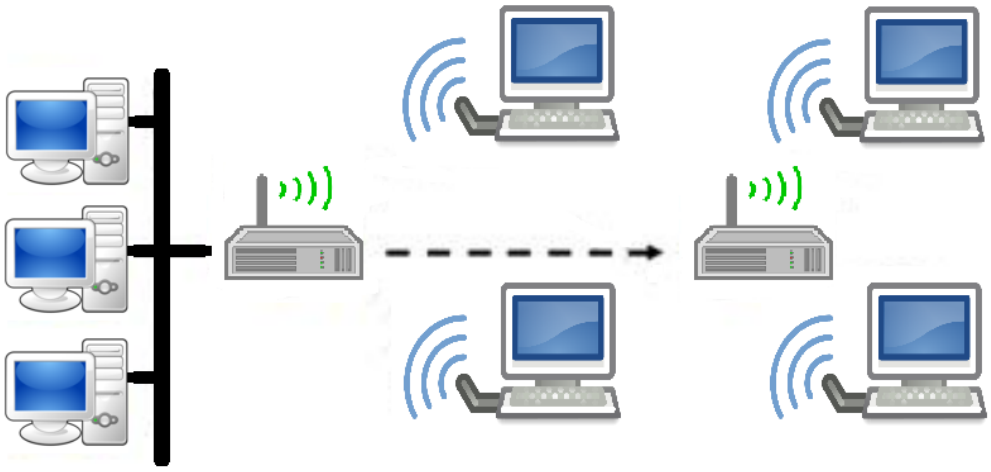
1.1.4 Standardy počítačových sítí

Jednotlivé části síťového hardwaru je možno různě kombinovat. Problém nastává, když různě sestavené sítě spolu nekomunikují. Proto, aby se tomu předešlo, byly přijaty normy (standardy), které definují základní požadavky na technické provedení sítě zajišťující kompatibilitu jednotlivých zařízení. Od 70. let se tímto zabývají dvě mezinárodní organizace. Jedná se o ISO (International Organization for Standardization) a IEEE (Institute of Electrical and Electronics Engineers). Standard síťového hardwaru definuje tyto základní vlastnosti sítě:

- **Topologie sítě** popisuje strukturu, rozložení a komponenty (schémata zapojení celé sítě):
    - Topologie sběrnicová (Příloha P I) je jedna z nejstarších a dnes již není příliš rozšířenou. Stanice (PC) jsou zapojeny na společném vodiči (koaxiální kabel), který sdílí.
    - Topologie kruhová (Příloha P II) je o propojení počítače s předchozím a následujícím do podoby kruhu. Informace jde od vysílací stanice v jednom směru po kruhu přes jednotlivé stanice až do cílové. V dnešní době je tato technologie již zastaralou.
    - Topologie hvězda (Příloha P III) představuje jednoznačně nejpoužívanější druh. Ke svému fungování využívá centrální prvek, na který jsou napojeny všechny ostatní.

[13] RAK, Jakub. *Aplikovaná informatika* [online]. 86 s. [cit. 2018-02-28]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.

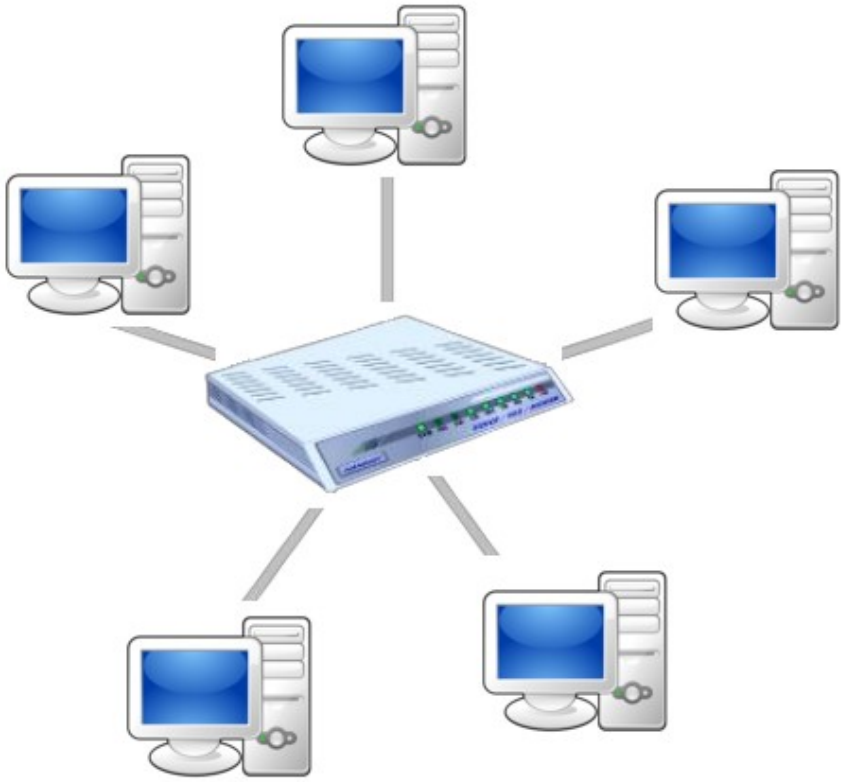
  - Topologie strom (Příloha P IV) funguje na stejném principu jako topologie hvězda. Jedná se o propojení dvou hvězdicových topologií hlavním (páteřním) rozvodem.
  - Topologie páteřní síť (Příloha P V) si klade za cíl vytvořit jednu hlavní část, na kterou jsou napojeny ostatní subsystémy (jiné sítě). Subsystémy mohou mít různý charakter, např. hvězda, kruh, sběrnice atd. [14]
- **Rychlost přenosu dat** (bit za sekundu a jeho násobky = kB/s; MB/s; GB/s; TB/s).[15]
- **Typ kabelu, jeho délku a konektor:**
  - Metalická vedení (koaxiální kabel nebo kroucený pár).
  - Optická vedení.
  - Vzduch (radiový signál).
  - Strukturovaná kabeláž (koncept kroucené dvojlinky).[16]
- **Přístupová metoda:**
  - Opakovač (repeater) je určen k regeneraci signálu, neumí řízení přenosu dat do jednotlivých segmentů sítě.



Obrázek 1. Schéma principu opakovače

[14] RAK, Jakub. *Aplikovaná informatika* [online]. 86 s. [cit. 2018-02-28]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.
[15] Tamtéž
[16] Tamtéž

- Rozbočovač (hub) může fungovat jako jednoduchý repeater.

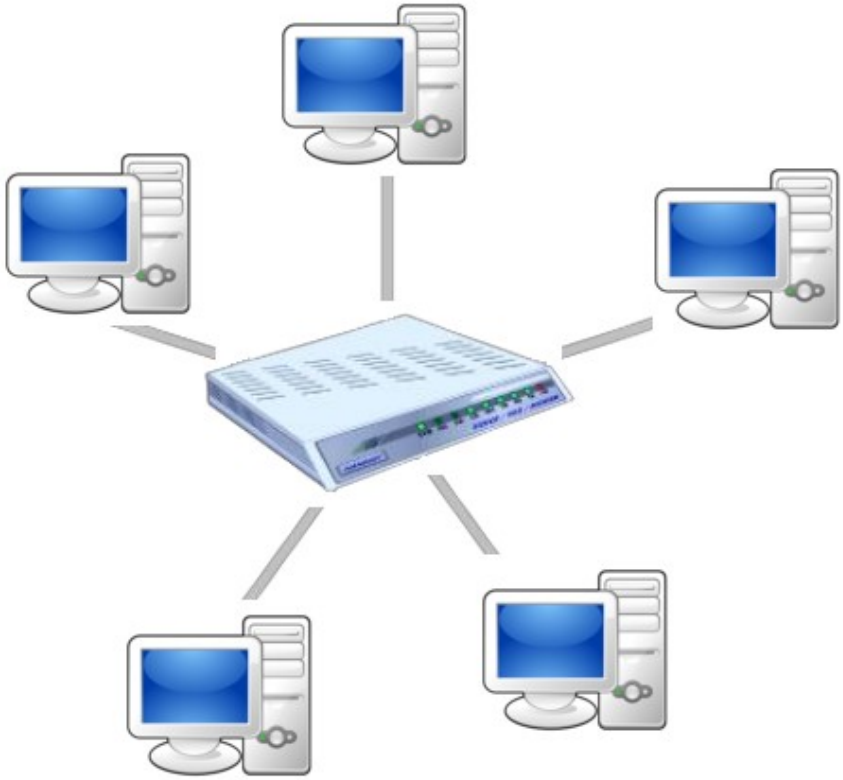


Obrázek 2. Schéma principu rozbočovače

- Most (bridge) umí řízení přenosu dat do jednotlivých segmentů sítě.

Obrázek 3. Schéma principu mostu

- Přepínač (switch) umožňuje paralelní komunikace mezi segmenty sítě a jejich uzly, tj. komunikace z více počítačů prostřednictvím jednoho média.



Obrázek 4. Schéma principu přepínače

- Směrovač (router) má v základní rovině stejnou funkci jako přepínač.
- Brána (getaway) představuje zařízení umožňující propojení heterogenních sítí (používajících více přenosových protokolů).[17]

1.2 Kybernetická bezpečnost

V souvislosti s používáním informačních a komunikačních technologií vyvstává otázka nejen pro management firem, státní organizace, ale i pro jednotlivce ohledně bezpečnosti a ochrany dat a informací. Na firemní účet (respektive u přepážky na pobočce banky), vlastní peněženku, občanský průkaz nebo cestovní pas jsme se naučili si dávat pozor. Vkladní

[17] RAK, Jakub. *Aplikovaná informatika* [online]. 86 s. [cit. 2018-02-28]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.

knížky bývají pečlivě uschovány, ale se zabezpečením nebo ochranou dat při využívání informačních a komunikačních technologií si již rady nevíme.[18]

Problematika kybernetické bezpečnosti je poměrně obsáhlou, a ještě do roku 2010 v České republice podceňovanou, záležitostí. V dnešní době, kdy skoro každý vlastní nějaký ten osobní počítač, notebook, tablet či chytrý smartphone a používá cloudová uložiště (např. Dropbox, Google Drive, Microsoft OneDrive apod.) či má nějaký ten profil na sociální síti typu Facebook, Google+, LinkedIn, se vystavuje riziku kyber útoku. Státní instituce a jejich servery s databázemi obyvatel, nezaměstnaných, registry vozidel apod. nevyjímaje. A tak není radno kybernetickou bezpečnost podceňovat. Také dávno pryč jsou doby, kdy útočníci cílili na naše PC jako celky či jejich komponenty typu formátování hard disku apod. Dnes se cílem útoků stávají jednotlivci a jejich bankovní konta nebo profily na sociálních sítích s citlivými údaji na ně vloženými. Na pozoru by se také měli mít pracovníci státních institucí a důležité infrastruktury. Dozorem v oblasti kybernetické bezpečnosti byly pověřeny instituce jako Národní bezpečností úřad (NBÚ), ústřední orgán státní správy, jehož součástí se stalo Národní centrum kybernetické bezpečnosti (NCKB). Národní centrum kybernetické bezpečnosti má vládní tým CERT (GovCERT.CZ) a týmy typu CSIRT, jež hrají klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů podle zákona o kybernetické bezpečnosti.[19]

NCKB bylo založeno dne 19. října 2011, a to přijetím usnesení vlády České republiky č. 781 o ustanovení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autority pro tuto oblast. Národní centrum kybernetické bezpečnosti je součástí Národního bezpečnostního úřadu a sídlo má v Brně.[20]

Ovšem na základně zákona č. 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti došlo k formálním změnám. Úřad se přejmenoval na Národní úřad

---

[18] DRASTICH, Martin. *Systém managementu bezpečnosti informací*. První vydání. Praha: Grada Publishing, a.s., 2011. ISBN 978-80-247-4251-9.
[19] ZÁSTŘEŠEK, David. *Národní centrum kybernetické bezpečnosti a CERT*. Zlín, 2016. Semestrální práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Petr Svoboda.
[20] Tamtéž

pro kybernetickou a informační bezpečnost (NÚKIB) a sám se stal ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany.[21]

Zajištění kybernetické bezpečnosti státu i jeho občanů je jednou z klíčových výzev současné doby. Závislost veřejného a soukromého sektoru na informačních a komunikačních technologiích je naprosto zřejmá. Sdílení a ochrana informací např. v oblasti bezpečnosti, ekonomiky a hospodářství, je v dnešní době zásadním zájmem nejen státu, ale i jeho obyvatel. Zatímco veřejnost se nejvíce obává majetkové újmy, ztráty svých dat či zneužití osobních údajů, realita celé problematiky kybernetické bezpečnosti je mnohem rozsáhlejší. Významnými riziky jsou kybernetická špionáž (průmyslová, vojenská, politická či jiná), působení organizovaného zločinu v kyberprostoru, hacktivismus (blokování webových stránek, narušování webových stránek či spamming), záměrné šíření dezinformací (za účelem dosažení politických a vojenských cílů), či v budoucnu i kyberterorismus. Tyto neformální skupiny hactivistů se mohou stát bezpečnostním problémem pro celý stát. Jako příklad lze uvést Juliena Assange a jeho stránky Wikileaks. Riziko představují nejen velmi frekventované útoky prováděné za účelem ekonomického prospěchu, ale i případy narušení bezpečnosti a integrity sítí způsobené nezáměrně, např. selháním lidského faktoru, živelnou pohromou apod. Ochrana spočívá v efektivním zajištění prvků kritické informační infrastruktury (dále jen „KII“), ale také celkové bezpečnosti sítě a kyberprostoru, v jehož rámci vyvíjejí aktivity rovněž obyvatelé jednotlivých států a kyberprostor se stal zásadní pro jejich ekonomický a sociální zájem.[22,23]

Přestože útoky na KII mají jednoznačně technologickou povahu, provádějí je lidé. Na základě tohoto hlediska jsou klasifikovány jako hybridní problém (technologicko-lidský aspekt). Morálka, etika a sociální odpovědnost jsou otázky zaměřené na člověka, které se při navrhování bezpečnostních a informačních systémů stávají neodlučitelnou složkou, jež je

---

[21] *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2018-04-10]. Dostupné z: https://www.govcert.cz/

[22] ZÁSTŘEŠEK, David. *Systémově vyjádřené modely Národního centra kybernetické bezpečnosti a CERT pro prostředí kybernetické bezpečnosti*. Zlín, 2017. Semestrální práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Prof. Ing. Jiří Dvořák, DrSc.

[23] WOSZCZYNSKI, Amy B. a Andrew GREEN. Learning Outcomes for Cyber Defense Competitions. *Journal of Information Systems Education* [online]. 2017, **28**(1), 21-41 [cit. 2018-03-27]. ISSN 10553096. Dostupné z: http://search.ebscohost.com/login.aspx?direct=true&db=lxh&an=126157286&scope=site

nutno brát v úvahu. To zahrnuje nejen koncepci samotného bezpečnostního systému, ale rovněž vzdělání týkajícího se profesionálního chování, ochrany soukromí, duševního vlastnictví ze stran IT specialistů.[24]

V dnešním kybernetickém prostoru je celá řada možností, jak být napaden. V rámci toho existuje řada možných způsobů obrany. Faktem ovšem zůstává, že obránci budou vždy o krok zpět před útočníky a jejich způsoby. Proto spatřuji velký význam v ucelených a systematických opatřeních.

Takovému celku říkáme bezpečnostní politika. Je to soubor pravidel a postupů k dosažení a udržení definovaných bezpečnostních standardů. Tato opatření musí být jasná a úplná. V případě selhání těchto pravidel a postupů (bezpečnostní politiky) může nastat bezpečnostní incident, který představuje narušení bezpečnostních pravidel informačního systému či IT infrastruktury definované k jeho ochraně. Zjištěné bezpečnostní incidenty a nedostatky musí být nahlášeny zodpovědným osobám, archivovány, zdokumentovány, prozkoumány a odstraněny s ohledem na příčiny, které je vyvolaly, tak aby mohlo být dosaženo nápravy.[25]

1.2.1 Typy bezpečnostních incidentů a jejich členění

- **Podle cíle:**
  - Aktivní (přerušení dostupnosti, narušení integrity, modifikace).
  - Pasivní (odposlech).
- **Podle charakteru:**
  - Úmyslné.
  - Způsobené nevědomostí, nedbalostí či neznalostí.
- **Podle způsobených škod:**
  - Obecně počítačové viry (programy které se dokáží samy šířit bez vědomí uživatele).
  - Červy (programy schopné rozesílat kopie sebe sama na další PC a šířit se tak).

---

[24] WOSZCZYNSKI, Amy B. a Andrew GREEN. Learning Outcomes for Cyber Defense Competitions. *Journal of Information Systems Education* [online]. 2017, **28**(1), 21-41 [cit. 2018-03-27]. ISSN 10553096. Dostupné z: http://search.ebscohost.com/login.aspx?direct=true&db=lxh&an=126157286&scope=site

[25] ŠAFAŘÍK, Zdeněk. *Analýza rizik* [online]. 170 s. [cit. 2018-01-30]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.

- Trojské koně (programy nebo funkce, se kterými uživatel nesouhlasí např.: sniffer = odposlouchávání přístupových jmen či hesel, keylogger = záznam zadávaných znaků na klávesnici apod.).
- Spamy (nevyžádaná sdělení masově šířená sítí internet).
- DoS útoky (útoky znemožňující ostatním uživatelům použití internetových služeb).
- Sniffing (programy na odposlouchávání síťového provozu).
- Password cracking (prolamování hesel).
- Zkompromitování uživatelského účtu.
- Phishing (získání citlivých údajů jako hesel, čísel kreditních karet apod. od obětí útoků pomocí podvodných emailů).
- Pharming (získání citlivých údajů jako hesel, čísel kreditních karet apod. od obětí útoků pomocí DNS a IP adres).
- Porušení autorských práv.
- Porušení občanských práv, zákonů apod.[26]

1.2.2 Vybrané možnosti předcházení bezpečnostním incidentům

- Vhodná architektura sítě (privátní sítě).
- Bezpečnostní údržba systému.
- Vyřazení nebezpečných nebo nepoužívaných služeb (např. FTP).
- Zabezpečení serverů, ochrana hesel, šifrované služby.
- Antivirové nástroje a antispamová ochrana.
- Kontrolní činnost proti rootkitům.
- Auditní nástroje a kontroly integrity souborů.
- Detekční systémy.
- Firewally, paketové filtry.
- Nepodporování anonymního užívání sítě.
- Zavádění jednoznačné autentizace uživatelů.

---

[26] ŠAFAŘÍK, Zdeněk. *Analýza rizik* [online]. 170 s. [cit. 2018-01-30]. Dostupné z: http://vy-uka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.

- Logování akcí uživatelů (přístupy na servery).
- Archivace a zabezpečení logů pro možnost pozdějšího dohledání pachatele.
- Směrnice pro provoz sítě a osvěta uživatelů a správců.
- Vhodná volba a změna hesel.
- Ochrana hesel a klíčů.
- Uvědomění si, že každý systém je nejnapadnutelnější zevnitř.
- Archivace a šifrování citlivých dat.
- Používání vhodných nástrojů a utilit.
- Znalost funkcionality používaných nástrojů a operačních systémů (webové prohlížeče, pamatování si hesel, mazání cookies, …).
- Mít povědomí o psychologickém nátlaku.
- Ochrana vlastní identity (heslo, elektronický podpis, PIN) apod.[27]

[27] ŠAFAŘÍK, Zdeněk. *Analýza rizik* [online]. 170 s. [cit. 2018-01-30]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.

2 ANALÝZA RIZIK

Nebezpečí hodnotí takřka nepřetržitě každý. Nejen člověk, ale i každý živý organizmus, neboť *hodnocení nebezpečí je základní podmínkou přežití*. Takové hodnocení je však převážně podvědomé a není téměř nikdy numerické. Probíhá automaticky velkou rychlostí, aniž by cílem bylo jakékoliv číslo. Téměř vždy je cílem *minimalizace možných škod*, neboť subjekt se rozhoduje podvědomě tak, aby utrpěl co nejmenší nebo vůbec žádnou ztrátu. Kdybychom při přecházení ulice vědomě analyzovali možná rizika, nikdy bychom asi žádný přechod nepřešli.[28]

Až ve vyšším stupni cílevědomého uvažování se dospěje k podrobnějšímu numerickému zhodnocení situace. Čím je složitější (skupina lidí, organizace apod.), tím náročnější je hodnocení. Doba rozhodování je delší. Vědomé uvažování o ztrátě (zisku) spočívá v rozboru a hodnocení známých nebo očekávaných skutečností. To jsou již výchozí operace analýzy rizika: *identifikace nebezpečí, kvalifikace nebezpečí a kvantifikace rizika*.[29]

Proces stojí na třech otázkách, které si na počátku každé analýzy rizika klademe:

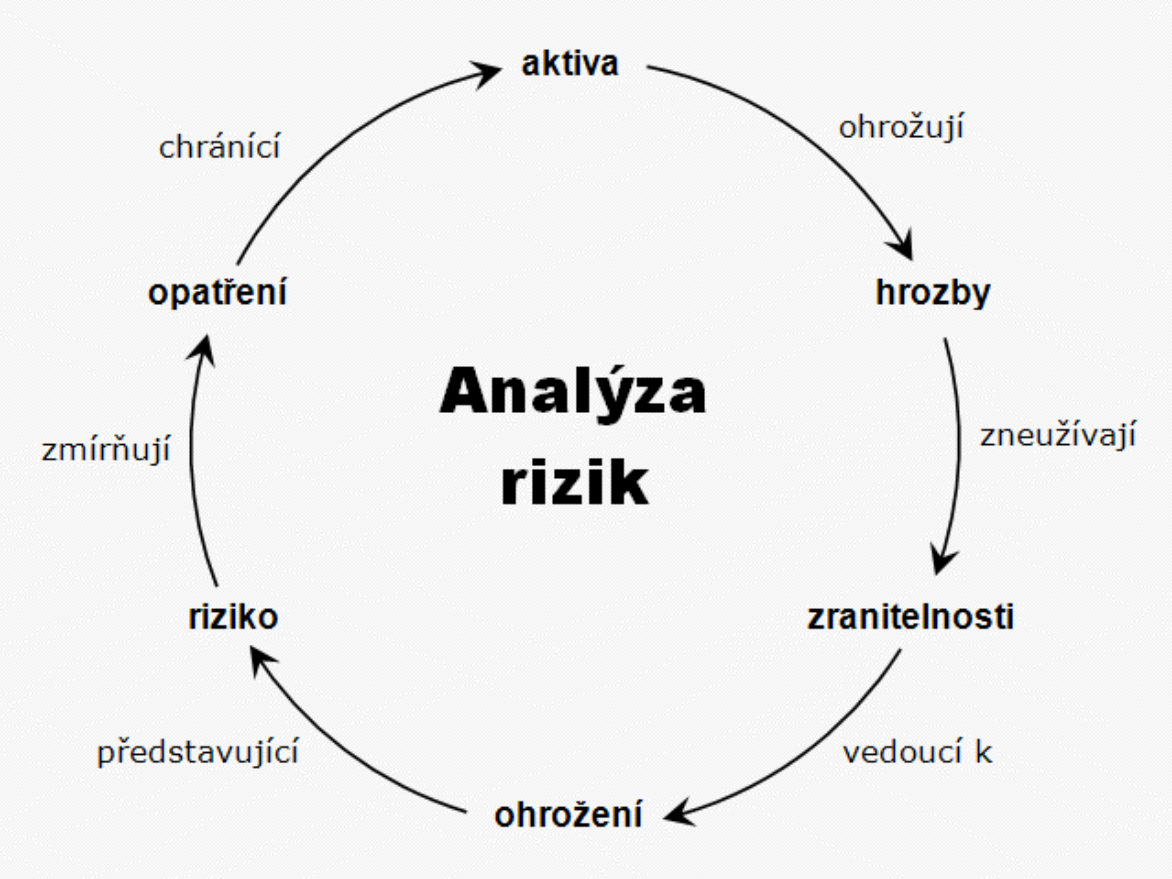
- *Jaké nepříznivé události mohou nastat?*
- *Jaká je pravděpodobnost nepříznivých událostí?*
- *Pokud některé nastanou, jaké to může mít následky?*

Formulace těchto jednoduchých otázek znamenala významný krok v rozvoji teorie rizika a zejména přechodu od kvalitativních ke kvantitativním odhadům.[30]

Dost často také dochází ke ztotožnění pojmů riziko a hrozba. Je třeba si uvědomit, že hrozba může být zdrojem pro jedno či více rizik a sama o sobě riziko nepředstavuje. Hrozby pouze zneužívají zranitelnosti vedoucí k ohrožení, což je riziko, které lze snížit prostřednictvím opatření chránící aktiva před působením těchto hrozeb (Obrázek 5.).[31]

---

[28] TICHÝ, Milík. *Ovládání rizika: analýza a management*. V Praze: C.H. Beck, 2006. Beckova edice ekonomie. ISBN 80-7179-415-5.
[29] Tamtéž
[30] Tamtéž
[31] ŠAFAŘÍK, Zdeněk. *Analýza rizik* [online]. 170 s. [cit. 2018-01-30]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.



Obrázek 5. Schéma analýzy rizik

zdroj: ČERMÁK, Miroslav. [Schéma analýzy rizik]. In: *CLEVER AND SMART* [online]. 20. 1. 2013 [cit. 2018-01-11]. Dostupné z: https://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/

2.1 Přístupy k analýze rizik

Pokud se jedná o samotné přístupy k provedení analýzy, tak dle ISO/IEC 13335 jsou to následující:

- **Základní přístup** – žádná analýza rizik se neprovádí, pouze je vybrána a implementována základní sada opatření z nějakého katalogu.
- **Neformální přístup** – jedná se o pragmatický přístup k analýze rizik, kdy se provádí rychlá, tzv. orientační analýza, založená na zkušenostech expertů a vyhodnocení možných scénářů.
- **Formální přístup** – jde o detailní analýzu rizik, tj. provádí se hodnocení aktiv, hrozeb a zranitelnosti nejčastěji za použití matematického aparátu.

- **Kombinovaný přístup** – na základě provedené orientační analýzy, kdy byla pro organizaci identifikována kritická aktiva nebo procesy, se provede detailní analýza rizik.[32]

2.2 Fáze analýzy rizik

Vlastní analýza se skládá z několika fází: identifikace a kvantifikace aktiv, analýza hrozeb, zranitelností a stanovení výsledného rizika. Samotná analýza může být provedena interně nebo externě.[33]

Tabulka 2. Srovnání interní a externí analýzy (zdroj dat: [34])

INTERNĚ	*výhody:*	-všichni rozumí výstupům -nejlevnější (i když se kupuje metodika či nástroj) -znalost interního prostředí -větší ochota respondentů spolupracovat s kolegy než s externisty
	nevýhody:	-vysoká zátěž organizace -nejistota správného výsledku (pokud nejsou vlastní odborníci) -neefektivní spotřeba lidských zdrojů (pokud analýzu provádí pracovníci ke svým každodenním povinnostem) - „vnitropodniková slepota“
EXTERNĚ	*výhody:*	-nezatěžuje organizaci (pouze rozhovory a dotazníky) -není nutné mít vlastní odborníky -odpovědnost je na straně dodavatele -není nutnost koupě metodiky či nástroje
	nevýhody:	-nesrozumitelné výstupy -vysoká cena -s posledním expertem odejde i know-how

[32] ČERMÁK, Miroslav. Analýza rizik: Jemný úvod do analýzy rizik. *CLEVER AND SMART* [online]. 2013 [cit. 2018-04-08]. Dostupné z: http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/
[33] Tamtéž
[34] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009. Knihovnicka.cz. ISBN 978-80-7399-731-1.

2.2.1 Identifikace a kvantifikace aktiv

V rámci analýzy musíme identifikovat pro organizaci její kritická aktiva a určit jejich hodnotu. Tomu se říká inventarizace aktiv, v rámci, kterého se vytváří tzv. registr aktiv.[35]

2.2.2 Analýza hrozeb

Jedná se o identifikace a kvantifikace hrozeb. Také se nazývá analýzou hrozeb (threat analysis), při které vycházíme ze seznamu obecných nebo specifických hrozeb.[36]

2.2.3 Analýza zranitelnosti

Musí se identifikovat a kvantifikovat všechna slabá místa na úrovni fyzické, logické a administrativní bezpečnosti. Také se ji někdy říká analýza zranitelnosti (vulnerability analysis / vulnerability assessment).[37]

2.2.4 Stanovení výše rizika nebo škody

V okamžiku kdy známe hodnotu aktiv, pravděpodobnost hrozeb a míru zranitelnosti, můžeme přistoupit k vyjádření rizika. Pokud jsme provedli kvantitativní analýzu, vyjádříme výši rizika v peněžních jednotkách. V případě, že byla provedena analýza kvalitativní, vyjádříme výši ve stupních.[38]

2.3 Analýza bezpečnosti informačního systému

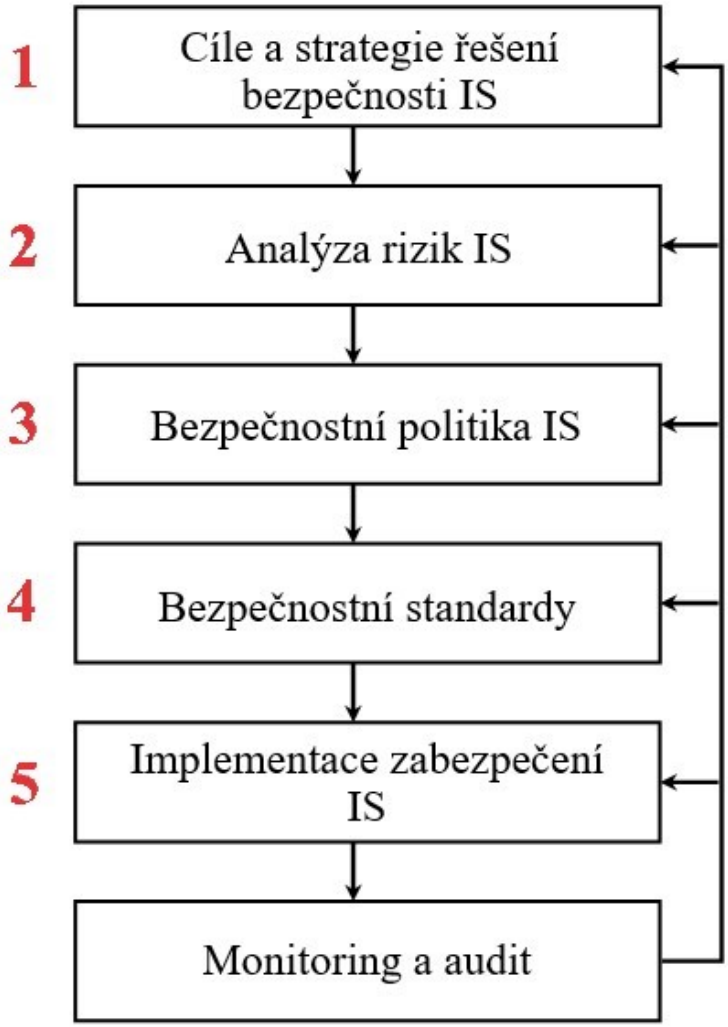
Při analýze rizik bezpečnostního systému je naším cílem prověřit aktuální stav bezpečnosti, odhalit slabá místa a najít nejvhodnější opatření k jejich odstranění. Analýza ovšem nezahrnuje jen počítačovou část, ale také veškeré činnosti a subjekty, které s informacemi přicházejí do styku. A to v podobě papírové, elektronické či jiné. Z tohoto důvodu je třeba neopomenout a významně se zabývat sociální oblastí, tedy lidským faktorem.[39]

---

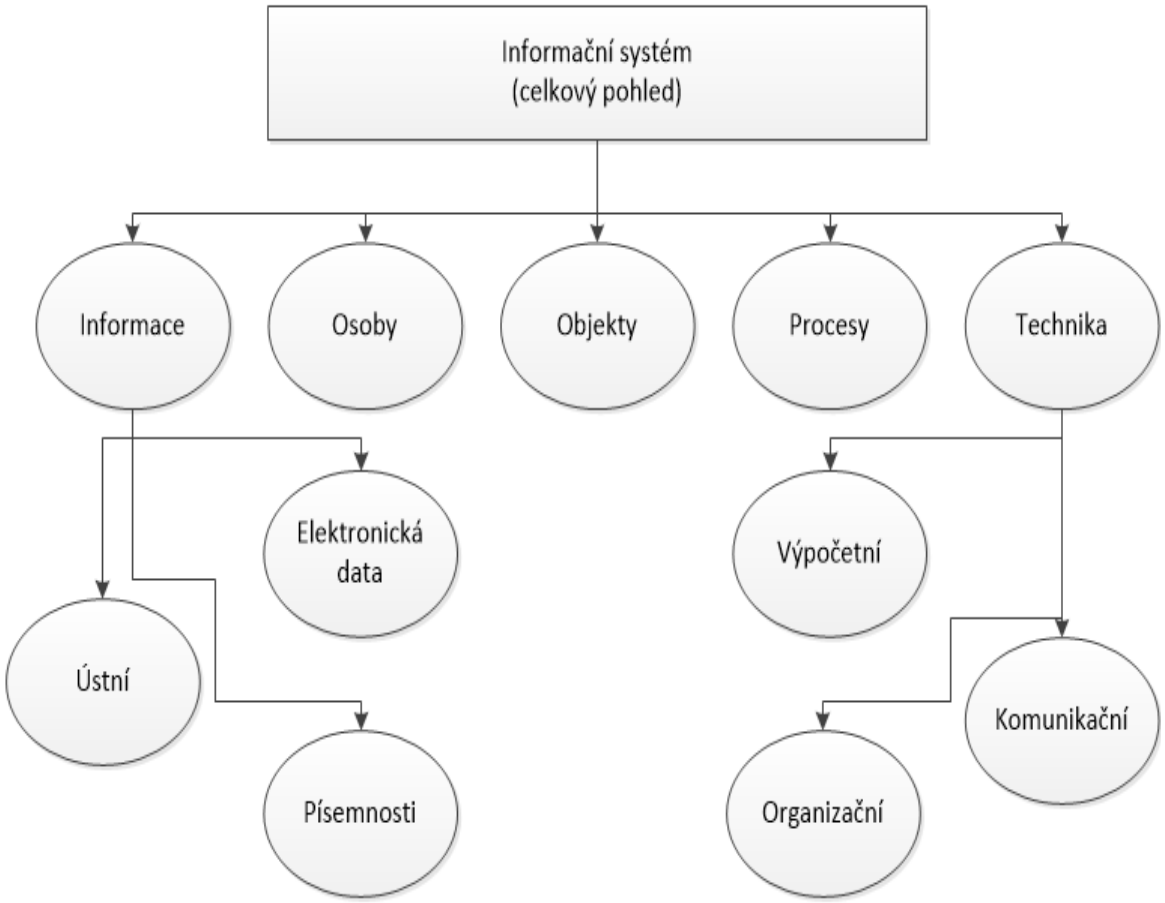
[35] ČERMÁK, Miroslav. Analýza rizik: Jemný úvod do analýzy rizik. *CLEVER AND SMART* [online]. 2013 [cit. 2018-04-08]. Dostupné z: http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/
[36] Tamtéž
[37] Tamtéž
[38] Tamtéž
[39] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů* [online]. Vyd.1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 9788074543128. Dostupné také z: http://hdl.handle.net/10563/25821

2.4 Proces bezpečnostní analýzy

Tento proces je jasně z názorně na níže zobrazených schématech (Obrázek 6. a Obrázek 7.).



Obrázek 6. Schéma procesu rešení IT bezpečnosti



Obrázek 7. Rozsah analýzy rizik

zdroj: JAŠEK, Roman a David MALANÍK. [Rozsah analýzy rizik]. In: *Bezpečnost informačních systémů* [online]. 2013 [cit. 2018-01-25]. Dostupné z: http://hdl.handle.net/10563/25821

2.5 Použitá metoda analýzy rizik

Vzhledem k zaměření a tématu bakalářské práce byla jako nejvhodnější zvolena metoda FMEA.

2.5.1 Historie Analýzy vzniku možných poruch a jejich následků

Metoda FMEA (Failure Mode and Effect Analysis / Fehler Möglichkeits und Einfluss Analyse), v českém překladu analýza vzniku možných poruch a jejich následků, má svůj původ ve vojenském předpisu, který byl vytvořen v listopadu roku 1949. V počátcích tato metoda používala techniku hodnocení spolehlivosti. Tím bylo možné posoudit různé poruchy zařízení nebo určitých systémů. Následně se posuzoval vliv na výsledek osob, bezpečnost nebo výkonnost zařízení. V 60. letech minulého století tuto myšlenku aplikovala NASA na projekt

Apollo 13 a využila FMEA jako spolehlivostní analýzu složitých systémů v kosmickém výzkumu a jaderné energetice. 10 let poté se metoda aplikuje v civilním sektoru na sériovou výrobu automobilky Ford, jako preventivní zajištění výroby. V 80. letech 20. století dochází k jejímu kompletnímu zpracování do jednotné příručky a je zahrnuta do normy QS9000. Od roku 1993 je norma FMEA použita např. u Chrysler Corporation, Ford Motor Company a General Motor Corporation.[40,41]

2.5.2 Definice a cíle Analýzy vzniku možných poruch a jejich následků

FMEA je systemizovaná skupina aktivit, která zahrnuje:

- Identifikaci a hodnocení potenciálních poruch výrobků / procesů a jejich následků.
- Identifikaci činností, které mohou eliminovat anebo redukovat možnost výskytu těchto poruch.
- Dokumentaci tohoto procesu.[42]

Je nápomocná v procesech specifikace, pro konstrukci anebo i jiné procesní požadavky či požadavky zákazníků. Pomáhá identifikovat či analyzovat potenciální ale i existující (nejkritičtější a nejpravděpodobnější) chyby. Vytváří předpoklady pro efektivní prevenci minimalizace příčin (což jsou účinná nápravná opatření) dřív, než se důsledky chyb projeví u odběratele (externího i interního). Jedná se o odhalení kritických komponentů a potenciálně slabých míst, kdy důležitým faktorem je včasnost rozpoznání chyby. Také odhad a vyčíslení rizik pocházejících z chyby má své nezastupitelné místo. Metoda kategorizuje chyby na základně odhadovaných rizik a zabývá se chybami procesu anebo systému, které ještě nenastali. Cílem FMEA je navrhnout opatření pro následnou eliminaci exitující nebo potenciální chyby.[43]

---

[40] VESELÝ, Milan. *Použití metody FMEA pro prevenci chyb v průmyslové výrobě* [online]. Brno, 2012 [cit. 2018-03-29]. Dostupné z: https://dspace.vutbr.cz/bitstream/handle/11012/4439/2012_DP_Vesel%C3%BD_76060.pdf?sequence=-1. Diplomová práce. Vysoké učení technické v Brně. Vedoucí práce Ing. Luboš Kotek, Ph.D.

[41] VARGOVÁ, Slavomíra. *LBRAR Analýza rizik: FMEA* [přednáška]. Uherské Hradiště: LUKR FLKŘ UTB, 21. 4. 2017.

[42] Tamtéž

[43] Tamtéž

2.5.3 Analýzy vzniku možných poruch a jejich následků procesu

Pro provedení analýzy rizik IT infrastruktury v praktické části bude použita metoda FMEA procesu. Jedná se o jednu z variant metody FMEA.

Metoda FMEA se používá v následujících formách:

- FMEA konstrukce – FMEA-K zkoumá všechna možná selhání systému, přičemž vychází z jeho funkcí.
- FMEA procesu (výrobní) – FMEA-P zkoumá všechny potenciální poruchy procesu a jejich příčiny. Určuje jejich nezbytná nápravná opatření.
- FMEA výrobku – FMEA-V zkoumá konstrukci a výrobní proces výrobku jako celku a analyzuje je v jednom projektu FMEA.
- FMEA výrobních prostředků – FMEA-VP optimalizuje výrobní prostředky s cílem snížit rizika možných poruch důležitých zařízení.[44]

FMEA procesu je určená pro přezkoumání a validaci návrhu technologického postupu. Je rovněž vhodnou metodou pro analýzu přezkoumání již používaného postupu, protože dokáže odhalit jeho slabá místa a iniciovat jeho zlepšení.[45]

Průběh je složen ze tří částí:

- **Analýza a hodnocení současného stavu**, kdy se postupně analyzují jednotlivé dílčí operace procesu v pořadí, jak na sebe navazují. Jedná se o vymezení možných vad, které se můžou při procesu vyskytnout. Hovoříme o:
    - *Závažnosti*, kdy číselná hodnota (1–10) nám vyjadřuje závažnost důsledku chyby na celý proces.
    - *Výskytu*, což je pravděpodobnost, že se určitá chyba při procesu vyskytne. Vyjadřujeme ji číselnou hodnotou (1-10).
    - *Odhalení*, což je známka (1-10), která je přiřazena nejlepším opatřením k odhalení.

---

[44] FMEA Analýza příčin a důsledků. *SVĚT PRODUKTIVITY Beta* [online]. c2012 [cit. 2018-04-14]. Dostupné z: http://www.svetproduktivity.cz/slovnik/FMEA-Analyza-pricin-a-dusledku.htm

[45] KADLČÍKOVÁ, Nela. *Analýza zdrojů rizik možného ohrožení prvku kritické infrastruktury* [online]. Uherské Hradiště, 2016 [cit. 2018-04-14]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/38736/kadl%c4%8d%c3%adkov%c3%a1_2016_dp.pdf?sequence=1&isAllowed=y. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení. Vedoucí práce Ing. Slavomíra Vargová, Ph.D.

- *Rizikovém čísle*, které je součin závažnosti (Z), výskytu (V) a odhalení (O).
  - Rizikové číslo = (Z) x (V) x (O)
  - Rizikové číslo 0-125 malé riziko.
  - Rizikové číslo 126-768 střední riziko.
  - Rizikové číslo 769-1000 vysoké riziko.

- **Návrh opatření** možných vad s vyššími hodnotami rizikového čísla, než je zvolená mezní hodnota, se navrhují opatření, jež by riziko měla snížit.
- **Hodnocení stavu po realizaci opatření** se nejprve analyzuje, zda provedená opatření odpovídají plánovaným opatřením. Nově zjištěné hodnoty umožňují posoudit účinnost jednotlivých opatření a případně opětovně vyčlenit možné vady s vysokou mírou rizika.[46,47]

Průběh analýzy se postupně zaznamenává do formuláře FMEA. Vyplněný formulář by neměl být pouhým záznamem, ale živým dokumentem dokládajícím soustavnou péči.[48]

[46] KADLČÍKOVÁ, Nela. *Analýza zdrojů rizik možného ohrožení prvku kritické infrastruktury* [online]. Uherské Hradiště, 2016 [cit. 2018-04-14]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/38736/kadl%c4%8d%c3%adkov%c3%a1_2016_dp.pdf?sequence=1&isAllowed=y. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení. Vedoucí práce Ing. Slavomíra Vargová, Ph.D.

[47] ZEMAN, Martin. *Zavedení metody FMEA do podniku Störi Mantel s.r.o.* [online]. Zlín, 2010 [cit. 2018-04-14]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/11911/zeman_2010_dp.pdf?sequence=1&isAllowed=y. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta technologická. Vedoucí práce Ing. Josef Hrdina.

[48] Tamtéž

II. PRAKTICKÁ ČÁST

3 UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ, FAKULTA LOGISTIKY A KRIZOVÉHO ŘÍZENÍ A LABORATOŘ GEOGRAFICKÝCH A INFORMAČNÍCH SYSTÉMŮ

Na úvod bych rád přestavil organizaci, její fakultu i konkrétní pracoviště, které zpracování analýzy rizik umožnilo. Jedná se o laboratoř geografických informačních systémů (GIS) na Fakultě logistiky a krizového řízení (FLKŘ) Univerzity Tomáše Bati ve Zlíně (UTB).

3.1 Historie Univerzity Tomáše Bati ve Zlíně

Univerzita Tomáši Bati ve Zlíně navazuje na dlouholetou tradici Fakulty technologické, která existovala ve Zlíně od 15. dubna 1969 jako součást Vysokého učení technického v Brně. Léta se zde vychovávali odborníci především v oboru technologie kůže, plastů a pryže. Projekt vzniku samostatné univerzity se začal rodit v 90. letech 20. století. V roce 1995 vnikla Fakulta managementu a ekonomiky, a to znovu v rámci VUT. Za další dva roky pak Institut reklamní tvorby a marketingových komunikací. Když 14. listopadu roku 2000 podepsal prezident České republiky Václav Havel zákon č. 404/2000 Sb., o zřízení Univerzity Tomáše Bati ve Zlíně, začíná se od 1. ledna 2001 datovat samostatná historie UTB.[49,50]

UTB se v současnosti skládá ze 6 fakult kde studuje cca. 9200 studentů. Jedná se o:

- *Fakultu technologickou* (FT) založenou 15. dubna 1969.
- *Fakultu managementu a ekonomiky* (FaME) založenou 27. června 1995.
- *Fakultu multimediálních komunikací* (FMK) založenou 1. ledna 2002.
- *Fakultu aplikované informatiky* (FAI) založenou 1. ledna 2006.
- *Fakultu humanitních studií* (FHS) založenou 1. ledna 2007.
- *Fakultu logistiky a krizového řízení* (FLKŘ) založenou 1. září 2009.[51,52]

[49] Univerzita Tomáše Bati ve Zlíně. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-10]. Dostupné z: https://cs.wikipedia.org/wiki/Univerzita_Tom%C3%A1%C5%A1e_Bati_ve_Zl%C3%ADn%C4%9B

[50] Historie univerzity. *Univerzita Tomáše Bati ve Zlíně* [online]. Zlín, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/o-univerzite/historie-univerzity

[51] Kdo jsme. *Univerzita Tomáše Bati ve Zlíně* [online]. Zlín, c2000-2018 [cit. 2018-04-10]. Dostupné z: http://www.utb.cz/o-univerzite/kdo-jsme

[52] Univerzita Tomáše Bati ve Zlíně. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-10]. Dostupné z: https://cs.wikipedia.org/wiki/Univerzita_Tom%C3%A1%C5%A1e_Bati_ve_Zl%C3%ADn%C4%9B

3.2 Fakulta logistiky a krizového řízení

Fakulta logistiky a krizového řízení Univerzity Tomáše Bati ve Zlíně je její nejmladší fakultou a také jedinou, která sídlí mimo Zlín, konkrétně v Uherském Hradišti. Svojí činností ovšem navazuje na vzdělávací a výzkumné aktivity Institutu bezpečnostní technologií v Uherském Hradišti, jenž náležel pod Fakultu technologickou. Ve své vědecko-výzkumné činnosti se fakulta zaměřuje na oblast logistiky, logistického zabezpečování mimořádných a krizových situací a krizovým řízením. V současnosti nabízí studium v těchto akreditovaných bakalářských a magisterských programech:

- Procesní inženýrství – obor Ovládání rizik.
- Ochrana obyvatelstva – obor Ochrana obyvatelstva.
- Bezpečnost společnosti – obor Řízení environmentálních rizik.[53]

Fakulta má danou strukturu, která se skládá z:

- Orgánů fakulty, kterými jsou děkan, akademický senát, vědecká rada a tajemník.
- Ústavů, kdy na FLKŘ se nacházejí 4. Jedná se o Ústav logistiky, Ústav krizového řízení, Ústav environmentální bezpečnosti a Ústav ochrany obyvatelstva.
- Poradní sborů a pracovních skupin, které se skládají z rady studijních programů, kolegia děkana, disciplinární a stipendijní komise.[54]

3.2.1 Ústav logistiky

Tento ústav garantuje výuku studijního programu Procesní inženýrství, oboru Ovládání rizik, a to i v profilu Řízení výrobních rizik a logistických systémů v prezenční i kombinované formě bakalářského stupně studia. Dále pak Rizika výrobních a logistických procesů magisterského stupně studia. K podpoře výuky a výzkumu je k dispozici logistická laboratoř se softwarovým vybavením Witness (SW určený pro modelování, simulaci a optimalizaci lo-

[53] Profil fakulty. *Univerzita Tomáše Bati ve Zlíně* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/o-fakulte/profil-fakulty-2
[54] Struktura FLKŘ. *Univerzita Tomáše Bati ve Zlíně: Fakulta logistiky a krizového řízení* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/struktura/struktura-flkr-1

gistických procesů), PTV-VISION (SW k modelování, simulaci a optimalizaci procesů spojených s problematikou logistiky měst a obcí), logistickým informačním systémem a dalšími softwarovými aplikacemi.[55]

3.2.2 Ústav krizového řízení

Ústav garantuje a realizuje výuku studijního programu Procesní inženýrství, oboru Ovládání rizik v prezenční i kombinované formě studia. Dále Rizikové inženýrství v magisterském stupni studia. Vychovává odborníky v oblasti analýzy, prevence a řešení mimořádných událostí způsobených přírodními živly nebo činností člověka, ale i analýzy a řešení ekonomických rizik a optimalizaci podnikových procesů. V rámci činnosti ústavu je také realizována výuka kybernetické bezpečnosti. K podpoře a výzkumu slouží laboratoř kybernetické bezpečnosti s kvalitním softwarovým vybavením.[56]

3.2.3 Ústav environmetální bezpečnosti

Je nejmladší ústav fakulty. Realizuje výuku studijního programu Bezpečnost společnosti, oboru Řízení environmentálních rizik. Celkový rámec je založen na vzdělávací a vědecko-výzkumné práci v oblasti interdisciplinárních environmentálních, přírodních, humanitních a socio-ekonomických věd integrovaných do struktur tuzemských stejně jako i mezinárodních aktivit. Součástí je i laboratoř Geografických a informačních systémů.[57]

3.2.4 Ústav ochrany obyvatelstva

Do oblasti činnosti spadá garance a realizace výuky předmětů profilujících studenty ve studijním programu Ochrana obyvatelstva, oboru Ochrany obyvatelstva v prezenční i kombinované formě. Dále pak Bezpečnost společnosti v magisterském stupni studia. Výuka je zaměřena na výchovu odborníků, kteří budou mít potřebné znalosti pro výkon funkcí souvisejících s krizovým řízením a ochranou obyvatelstva, majetku a životního prostředí na různých

---

[55] O nás. *Univerzita Tomáše Bati ve Zlíně: Fakulta logistiky a krizového řízení* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/struktura/o-nas-8

[56] O nás. *Univerzita Tomáše Bati ve Zlíně: Fakulta logistiky a krizového řízení* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/struktura/o-nas-6

[57] O nás. *Univerzita Tomáše Bati ve Zlíně: Fakulta logistiky a krizového řízení* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/struktura/o-nas-7

stupních státní správy, ale i v soukromé sféře. Příprava vychází ze současných potřeb vyplývajících z možných ohrožení obyvatelstva v nevojenské oblasti. Zahrnuje hrozby a rizika přírodní i antropogenní povahy, terorismus a sekundární, eventuálně terciární důsledky globální hospodářské recese.[58]

3.3 Laboratoř Geografických a informačních systémů

Jedná se o specializované pracoviště, které vzhledem k zaměření Ústavu environmentální bezpečnosti na vzdělávací a vědecko-výzkumnou práci, slouží k ověřování a převádění teoretických poznatků do praktické oblasti. Samozřejmostí je, že v případě potřeby tuto laboratoř využívají i další ústavy dle svých potřeb.

3.3.1 Technické parametry laboratoře

Základní technické parametry laboratoře GIS:

- Internet je na FLKŘ, a tedy i do laboratoře GIS přiveden kabelem.
- Typem kabelu je optického vedení.
- Druhem počítačové sítě je LAN.
- Hierarchií počítačové sítě je forma client / server.
    - Jedná se o Active Directory což je adresářová služba od společnosti Microsoft. Hlavní cíl Active Directory je ověřovat uživatele a počítače vůči doméně a spravovat politiky členských počítačů.
    - Jsou využity místní uživatelské profily (oproti cestovním).
    - Uživatelé mají své cloudové uložiště o kapacitě 1 TB.
- Topologií sítě je forma HVĚZDA.
- Přístupové metody 25 ks PC jsou přes switch, router i getaway.
- Disky na 25 PC nejsou sdílené v rámci sítě.
- Propojení s WiFi sítí eduroam je přes router, který umožňuje spojení VLAN pro PC v laboratoři do VLAN, kde se nacházejí klienti WiFi eduroam.

[58] O nás. *Univerzita Tomáše Bati ve Zlíně: Fakulta logistiky a krizového řízení* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/struktura/o-nas

3.3.2 Rizika pro laboratoř

Laboratoř se nachází v budově Fakulty logistiky a krizového řízení označené UH1 na adrese Studentské nám. 1532 v její přízemní části vpravo.

Díky tomuto umístnění se zde z pohledu kategorizace jedná o objektivní přírodní hrozbu zatopení laboratoře, protože v blízkosti protéká řeka Morava (Obrázek 8.), ale v úvahu jsou vzaty i přívalové deště.

Obrázek 8. Mapové zobrazení blízkosti řeky Moravy

zdroj: [Mapové zobrazení blízkosti řeky Moravy]. In: *Google Maps* [online]. [cit. 2018-04-19]. Dostupné z: https://www.google.cz/maps/@49.0705487,17.4719694,16.5z

Další objektivní přírodní hrozby představují požáry a výpadky elektrického napětí zapříčiněné mimořádnými přírodními událostmi. Rovněž zde nacházíme objektivní hrozbu fyzikální, kdy hovoříme o elektromagnetickém pulsu. Poslední objektivní hrozbou jsou technické nebo logické příčiny. Zde mluvíme o možném selhání klimatizace potřebné pro chod serverů, poruchách HW komponentů jako je zdroj PC, grafická karta, síťová karta, základní deska, paměti, procesor, zvuková karta apod. Dále se pak bavíme o softwarových problémech, mezi které lze řadit ochranu dat a informací, programů v laboratoři GIS používaných, protože to nejhorší, co nás může potkat, je jejich ztráta.

Tabulka 3. Seznam software laboratoře GIS

PRODUKT	VERZE	ZAMĚŘENÍ	LICENCE	POTENCIÁL MEZIOBOROVÉHO VYUŽITÍ
ArcGIS Desktop	10.4.1	GIS	Educational licence	ANO
ArcGIS Earth	1.3	GIS	Freeware	ANO
ArcGIS Pro	1.3	GIS	Educational licence	ANO
Blender	2.78.1	3D tisk	General public license	NE
Garmin BaseCamp	4.6.2	GIS	Freeware	NE
GeoDa	1.8	GIS	General public license	ANO
GIMP	2.8.18	Grafika	General public license	ANO
Google Earth Pro	7.1	GIS	Freeware	ANO
Inkscape	0.92	Grafika	General public license	ANO
MeshLab	2016	3D tisk	General public license	NE
PSPP	0.10.2	Statistický SW	General public license	ANO
QGIS	2.18.3	GIS	General public license	ANO
QMapShack	1.7.2	GIS	General public license	NE
R	3.3.2	Statistický SW	General public license	ANO
Scribus	1.4.6	Grafika	General public license	ANO
GRASS GIS	7.2	GIS	General public license	NE
gvSIG	2.3.1	GIS	General public license	NE
uDig	2.0	GIS	Open source (Eclipse public license)	NE
openJUMP	1.9.1	GIS	General public license	NE
Pronterface	2014.08.1	3D tisk	General public license	NE
Slic3r	1.2.9	3D tisk	General public license	NE
Kisslicer	1.5	3D tisk	Educational licence	NE

Ztrátě, poškození, úpravě dat nebo informace se obecně říká bezpečnostní incident. Ty lze dělit na:

- Úmyslné, kde je jasný úmysl poškodit data či systém laboratoře GIS ze strany studenta, učitele či jiného osoby (útočníka).
    - Pasivní, kdy se hovoří o odposlechu, ovlivňování výkonu systému apod. Do systému se dostává program (škodlivý kód), který útočníkovi tuto činnost umožní.
    - Aktivní, což je pozměňování dat atd. Útočník maže soubory s daty, odinstalovává software, přidává upravená data apod.
- Neúmyslné, kam řadíme např. chybu uživatele, neodbornou manipulaci nebo nedodržování bezpečnostních standardů (nařízení), kdy k incidentu dochází nedbalostí.

Tyto útoky jsou buďto:

- Uvnitř laboratoře GIS, tj. páchá útočník přímo na zařízení v laboratoři.
- Zvenčí laboratoře GIS, kdy hovoříme o hackingu, crackingu.
- Kombinací a mohou se dále členit:
    - Úmyslné, tedy útočník (zaměstnanec, student) neutočí sám, ale předá informace třetí straně.
    - Neúmyslné, tj. nevědomky. V tomto případě hovoříme o sociálním inženýrství (útočník správně zvolenými dotazy získá potřebné informace), šíření poplašené zprávy nebo invazivním hackingu.[59]

[59] SVOBODA, Petr. *LARBI Bezpečnost informací* [přednáška]. Uherské Hradiště: LUOO FLKŘ UTB, 4. 3. 2016.

4 ANALÝZA RIZIK LABORATOŘE

Vzhledem k tomu, že tato bakalářská práce je veřejně dostupnou a samotná analýza se dotýká bezpečnosti, rozhodl jsem se některé z bezpečnostních prvků a postupů neanalyzovat konkrétně. Analyzovány budou pouze v obecné rovině, neboť zveřejnění těchto informací by samo o sobě přestavovalo hrozbu a bezpečnostní riziko.

4.1 Analýzy vzniku možných poruch a jejich následků procesu

Pro analýzu FMEA je klíčové zpracování do formuláře FMEA. Zde jsou definovány hlavní části formuláře FMEA (např. krok procesu / požadavky / možný způsob poruchy / možné důsledky poruchy atd.) do kterých se vyplní údaje k analýze. Poté se doplní číselná hodnota závažnosti, výskytu a odhalení, a to na základě doporučených kritérií hodnocení.

4.1.1 Hlavní části formuláře Analýzy vzniku možných poruch a jejich následků

Formulář FMEA procesu by měl jednoznačně určit zaměření a informace související s procesem. Samozřejmě jej lze upravovat dle potřeb organizace a prováděné analýzy. Měl by obsahovat:

- **Číslo FMEA**: neboli alfanumerický údaj, který se používá pro označení dokumentu.
- **Objekt**: zde se uvede název, číslo systému (subsystému, komponentu), pro něž je analyzován.
- **Odpovědnost za proces**: tj. uvede se výrobce originálního zařízení, organizace a útvar nebo skupina, která je odpovědná za návrh procesu.
- **Rok výroby modelu / programu**: který bude analyzován, nebo využívat analyzovaný proces, nebo který jím bude ovlivněný.
- **Funkce / proces**: že se uvede označení procesu nebo analyzované operace, a to na základě číslování procesu a terminologie. Funkce procesu popisuje účel nebo záměr dané operace.
- **Možný způsob poruchy (možná chyba)**: byl definován jako způsob, jakým by proces mohl při plnění požadavků na proces selhat. Při vypracování se předpokládá, že vstupy jsou správné.
- **Možný důsledek poruchy (možné následky chyby)**: jsou definovány jako důsledky poruchy, jak je vnímá zákazník. Měly by se popisovat tak, jak by je mohl postřehnout nebo pocítit zákazník. Je třeba si uvědomit, že zákazníkem může být interní zákazník

i konečný uživatel. Zákazníkem v této souvislosti může být další operace, následné operace nebo výrobní místa. Každý z nich musí být při posuzování možného důsledku poruchy brán v úvahu. Jestliže by způsob poruchy mohl ovlivnit bezpečnost nebo způsobit nesoulad s předpisy, mělo by to být jednoznačně identifikováno v rámci FMEA.

- **Závažnost (Z)**: je hodnota spojována s nejzávažnějším důsledkem v případě daného způsobu poruchy. Závažnost představuje relativní známkování v rámci předmětu jednotlivé FMEA (Tabulka 5.). Kritéria hodnocení systému známkování by se měla používat konzistentně.
- **Možná příčina poruchy (chyby)**: byla definována jako označení toho, jak se může porucha vyskytnout. Je popsána jako něco, co lze opravit nebo co lze řídit. Možná příčina poruchy může vyjadřovat slabou stránku návrhu produktu nebo procesu, jejímž následkem je způsob poruchy. Měla by být popsána co nejstručněji a nejúplněji. Neměli by se používat nejasné fráze (např. chyba operátora nebo těsnění je špatně instalované atd.).
- **Výskyt (V)**: znamená pravděpodobnost výskytu specifické příčiny poruchy. Známka vyjadřuje spíše relativní význam než absolutní hodnotu. Odhadne se pravděpodobnost výskytu poruchy (Tabulka 6.). Pro zajištění kontinuity by se měl používat konzistentní systém známkování výskytu. Známka hodnocení výskytu je relativní známkování v rámci předmětu FMEA a nemusí odrážet reálnou pravděpodobnost výskytu.
- **Stávající opatření (prevence)**: je eliminování (odstranění) výskytu příčiny poruchy nebo způsobu poruchy nebo snížení četnosti jejich výskytu.
- **Stávající řízení procesu (odhalování)**: je identifikování příčiny poruchy nebo způsobu poruchy, které vedou k vypracování souvisejících opatření k nápravě nebo protiopatření.
- **Odhalení (O)**: neboli známka hodnocení související s nejlepším nástrojem řízení detekce. Jedná se o relativní známkování v rámci FMEA (Tabulka 7.) a mělo by se používat konzistentně. Aby se dosáhlo nižší známky hodnocení, musí se obecně zlepšit plánovaný nástroj řízení detekce. Nemělo by se automaticky předpokládat, že je známka hodnocení nízká, protože je malý výskyt, nýbrž by se měla posoudit schopnost nástrojů řízení procesu při detekování způsobu poruchy o malé četnosti nebo při prevenci jejich dalšího výskytu v procesu. Kritéria by se měla opět používat konzistentně.

- **Rizikové číslo (RPN)**: je jeden z přístupů napomáhající stanovení priorit opatření a jejich použití. Když se dokončí počáteční identifikace způsobů a důsledků poruch, příčin a nástrojů řízení, včetně známkování z hlediska závažnosti, výskytu a odhalení, musí se rozhodnout, zda je ke zmírnění rizika zapotřebí další úsilí. Počáteční zaměření by mělo být orientováno na způsoby poruch s nejvyššími známkami hodnocení závažnosti. V případě, že je známka hodnocení 9 nebo 10, je naprosto nezbytné, aby se zajistilo řešení rizik nebo doporučilo opatření. V případě závažnosti 8 nebo nižší se zabývat příčinami, které mají nejvyšší známku hodnocení výskytu nebo odhalení. Pro lepší představu uvádím příklad:

  Tabulka 4. Modelový příklad vyhodnocení RPN versus závažnost (zdroj dat: [60])

Objekt	Závažnost	Výskyt	Odhalení	RPN
A	9	2	5	**90**
B	7	4	4	**112**

  Na základě tohoto příkladu je RPN vyšší u objektu B než A. Nicméně prioritou by měly být práce na A s vyšší závažností 9, ačkoliv RPN je 90, což je nižší hodnota a je pod danou prahovou hodnotou. Další záležitostí týkající se používání RPN je to, že neexistuje žádná konkrétní hodnota, která vyjadřuje mandatorní opatření.

- **Doporučená opatření**: jsou taková, kde obecně mají preventivní opatření (tj. snižování výskytu) přednost před detekčními. Příkladem toho je použití ochrany proti chybám v návrhu procesu než namátkové kontroly kvality nebo přiřazená inspekce.
- **Odpovědnost**: patří osobě a organizace za splnění každého doporučení opatření, včetně termínu dokončení.
- **Provedená opatření**: zahrnují po realizace stručný popis přijatého opatření.
- **Závažnost**: po dokončení preventivního opatření (opatření k nápravě) se určí a zaznamená výsledná známka hodnocení závažnosti.
- **Výskyt**: po dokončení preventivního opatření (opatření k nápravě) se určí a zaznamená výsledná známka hodnocení výskytu.

[60] *Analýza možných způsobů a důsledků poruch (FMEA): referenční příručka*. 4. vyd. Přeložil Ivana PETRAŠOVÁ. Praha: Česká společnost pro jakost, 2008. ISBN 9788002021018.

- **Odhalení**: po dokončení preventivního opatření (opatření k nápravě) se určí a zaznamená výsledná známka hodnocení odhalení.
- **Rizikové číslo**: vypočítá se a zaznamená výsledný ukazatel priority opatření (rizika) RPN.[61]

4.1.2 Doporučená kritéria hodnocení pro závažnost, výskyt a odhalení

Kritéria sloužila jako podklad pro zpracování vlastních hodnot ohodnocení rizik v rámci analýzy FMEA. Tyto hodnoty závažnosti, výskytu a odhalení jsou zásadní pro výpočet rizikového čísla a ohodnocení jednotlivých rizik.

Systém hodnocení a známkování by se měl používat konzistentně, a to i v případě modifikace pro konkrétní postup analýzy.[62]

Tabulka 5. Doporučená kritéria hodnocení závažnosti (zdroj dat: [63])

DŮSLEDEK	**KRITÉRIA:** Závažnost důsledku ve vztahu k produktu	**ZNÁMKA HODNOCENÍ**	**DŮSLEDEK**	**KRITÉRIA:** Závažnost důsledku ve vztahu k produktu
Nesplnění bezpečnostních požadavků a/nebo požadavků předpisů	Možný způsob poruchy, který bez varování ovlivňuje bezpečný proces a/nebo znamená nesoulad s právními předpisy.	**10**	**Nesplnění bezpečnostních požadavků a/nebo požadavků předpisů**	Bez varování může ohrozit operátora (stroj, montážní celek).
	Možný způsob poruchy, který i s varováním ovlivňuje proces a/nebo znamená nesoulad s právními předpisy.	**9**		S varováním může ohrozit operátora (stroj, montážní sestavu).
Ztráta nebo zhoršení primární funkce	Ztráta primární funkce (např. vozidlo je nepojízdné, neovlivňuje bezpečný provoz vozidla).	**8**	**Závažné porušení**	100 % produktů bude muset být vyřazeno. Odstávka linky nebo zastavení dodávky.

[61] *Analýza možných způsobů a důsledků poruch (FMEA): referenční příručka*. 4. vyd. Přeložil Ivana PETRAŠOVÁ. Praha: Česká společnost pro jakost, 2008. ISBN 9788002021018.
[62] Tamtéž
[63] Tamtéž

DŮSLEDEK	**KRITÉRIA:** Závažnost důsledku ve vztahu k produktu	**ZNÁMKA HODNOCENÍ**	**DŮSLEDEK**	**KRITÉRIA:** Závažnost důsledku ve vztahu k produktu
	Zhoršení primární funkce (např. vozidlo je pojízdné, avšak při snížení úrovně technických parametrů).	**7**	**Významné porušení**	Část výrobní dávky bude muset být vyřazena. Odchylka od primárního procesu včetně snížení rychlosti linky nebo dodatečného personálu.
Ztráta nebo zhoršení sekundární funkce	Ztráta sekundární funkce (např. vozidlo je pojízdné, ale funkce zajišťující pohodu / pohodlí nejsou funkční).	**6**	**Mírné porušení**	100 % výrobní dávky bude muset být přepracována mimo linku a schválena.
	Zhoršení sekundární funkce (např. vozidlo, je pojízdné, ale funkce zajišťující pohodu / pohodlí jsou na nižší úrovni technických parametrů).	**5**		Část výrobní dávky bude muset být přepracována mimo linku a schválena.
Nepříjemnost	Vzhled nebo hluk, tj. např. vozidlo je pojízdné, objekt nevyhovuje a všimla si toho většina zákazníků (>75 %).	**4**	**Mírné porušení**	100 % výrobní série bude muset být přepracována na pracovišti před dalším výrobním postupem.
	Vzhled nebo hluk, tj. např. vozidlo je pojízdné, objekt nevyhovuje a všimlo si toho mnoho zákazníků (50 %).	**3**		Část výrobní dávky bude muset být přepracována na pracovišti před dalším výrobním postupem.
	Vzhled nebo hluk, tj. např. vozidlo je pojízdné, objekt nevyhovuje a všimli si toho hodně nároční zákazníci (<25%).	**2**	**Minimální porušení**	Drobná nepříjemnost ve vztahu k procesu, operaci nebo k operátorovi.
Žádný důsledek	Žádný znatelný důsledek.	**1**	**Žádný důsledek**	Žádný znatelný důsledek.

Tabulka 6. Doporučená kritéria hodnocení výskytu (zdroj dat: [64])

PRAVDĚPODOBNOST PORUCHY	**KRITÉRIA:** Výskyt příčiny – PFMEA (počet případů na počet objektů / vozidel)	**ZNÁMKA HODNOCENÍ**
Velmi velká	≥ 100 na tisíc ≥ 1 z 10	**10**
Velká	50 na tisíc 1 z 20	**9**
	20 na tisíc 1 z 50	**8**
	10 na tisíc 1 ze 100	**7**
Střední	2 na tisíc 1 z 500	**6**
	0,5 na tisíc 1 z 2 000	**5**
	0,1 na tisíc 1 z 10 000	**4**
Malá	0,01 na tisíc 1 z 100 000	**3**
	≤ 0,001 na tisíc 1 z 1 000 000	**2**
Velmi malá	Porucha je eliminována nástroji řízení prevence.	**1**

Tabulka 7. Doporučená kritéria hodnocení odhalení (zdroj dat: [65])

MOŽNOST DETEKCE	**KRITÉRIA:** Pravděpodobnost odhalení nástrojem řízení procesu	**ZNÁMKA HODNOCENÍ**	**PRAVDĚPODOBNOST ODHALENÍ**
Žádná možnost detekce	Žádný nástroj řízení pro stávající proces / nelze odhalit nebo není analyzováno.	**10**	**Téměř nemožná**

[64] *Analýza možných způsobů a důsledků poruch (FMEA): referenční příručka*. 4. vyd. Přeložil Ivana PETRAŠOVÁ. Praha: Česká společnost pro jakost, 2008. ISBN 9788002021018.
[65] Tamtéž

MOŽNOST DETEKCE	**KRITÉRIA:** Pravděpodobnost odhalení nástrojem řízení procesu	**ZNÁMKA HODNOCENÍ**	**PRAVDĚPODOBNOST ODHALENÍ**
V žádné etapě není pravděpodobná možnost detekce	Není snadné zjistit způsob poruchy a/nebo chybu (příčinu) (např. namátkové audity).	**9**	**Velmi mizivá**
Detekce problému po provedení operace	Detekce způsobu poruchy po provedení operace operátorem pomocí vizuálních / taktilních / akustických prostředků.	**8**	**Mizivá**
Detekce problému u zdroje	Detekce způsobu poruchy na pracovišti operátorem pomocí vizuálních / taktilních / akustických prostředků nebo po provedení operace s využitím atributivního měření (vyhovuje / nevyhovuje, ruční kontrola utahovacího momentu / maticový klíč atd.)	**7**	**Velmi malá**
Detekce problému po provedení operace	Detekce způsobu poruchy po provedení operace operátorem s využitím měření proměnných veličin nebo na pracovišti operátorem s využitím atributivního měření (vyhovuje / nevyhovuje, ruční kontrola utahovacího momentu / maticový klíč atd.)	**6**	**Malá**
Detekce problému u zdroje	Detekce způsobu poruchy nebo chyby (příčiny) na pracovišti operátorem s využitím měření proměnných veličin nebo automatizovaných nástrojů řízení na pracovišti, kterými se zjistí neshodný díl a uvědomí se operátor (světlo, akusticky signál atd.). Měření se provádí při nastavení a kontrole prvního kusu (pouze pro příčiny při nastavování).	**5**	**Střední**
Detekce problému po provedení operace	Detekce způsobu poruchy po provedení operace automatizovanými nástroji řízení, kterými se zjistí neshodný díl. Díl se zablokuje, aby se zabránilo další výrobní operaci.	**4**	**Středně velká**
Detekce problému u zdroje	Detekce způsobu poruchy na pracovišti automatizovanými nástroji řízení, kterými se	**3**	**Velká**

MOŽNOST DETEKCE	KRITÉRIA: Pravděpodobnost odhalení nástrojem řízení procesu	ZNÁMKA HODNOCENÍ	PRAVDĚPODOBNOST ODHALENÍ
	zjistí neshodný díl. Díl se automaticky zablokuje na pracovišti, aby se zabránilo další výrobní operaci.		
Detekce chyby a/nebo prevence problému	Detekce chyby (příčiny) na pracovišti automatizovanými nástroji řízení, kterými se zjistí chyba a zabrání se zhotovení neshodného dílu.	**2**	**Velmi velká**
Detekce není aplikována (prevence chyby)	Prevence chyby (příčiny) v důsledku návrhu upínacího přípravku, návrhu stroje nebo návrhu dílu. Neshodné díly nemohou být vyrobeny, protože objekt je díky návrhu procesu / produktu odolný proti chybám.	**1**	**Téměř jistá**

4.2 Formulář Analýzy vzniku možných poruch a jejich následků procesu

Pro analýzu rizik laboratoře GIS byly kritéria závažnosti, výskytu, odhalení a rozmezí hodnot rizikového čísla upraveny následovně:

Tabulka 8. Kritéria závažnosti FMEA (upraveno podle: Tabulka 5. a [66])

DŮSLEDEK	KRITÉRIA ZÁVAŽNOSTI DŮSLEDKU	ZNÁMKA
Zanedbatelný	Je nepravděpodobné, že by chyba mohla mít negativní účinek na proces.	**1**
Nepatrný	Význam chyby je nepatrný.	**2–3**
Středně závažný	Význam chyby je středně závažný, proces může být ohrožen.	**4–6**
Velký	Význam chyby je velký, proces je ohrožen.	**7–8**
Mimořádně závažný	Význam chyby je mimořádně vysoký, je ohrožena bezpečnost.	**9–10**

- Známka vyjadřuje závažnost důsledku chyby na proces.

[66] VARGOVÁ, Slavomíra. *LBRAR Analýza rizik: FMEA* [přednáška]. Uherské Hradiště: LUKR FLKŘ UTB, 21. 4. 2017.

Tabulka 9. Kritéria výskytu FMEA (upraveno podle: Tabulka 6. a [67])

PRAVDĚPODOBNOST CHYBY	KRITÉRIA VÝSKYTU CHYBY	ZNÁMKA
Nepravděpodobná	Chyba je skoro vyloučena.	**1**
Nepatrná	Velmi ojedinělá chyba.	**2–3**
Malá	Chyba se může občas vyskytnout.	**4–6**
Velká	Chyba se vyskytuje často.	**7–8**
Velmi vysoká	Chybě můžeme sotva zabránit.	**9–10**

- Známka výskytu je pravděpodobnost, že se daná chyba při procesu vyskytne.

Tabulka 10. Kritéria odhalení FMEA (upraveno podle: Tabulka 7. a [68])

PRAVDĚPODOBNOST ODHALENÍ	KRITÉRIA ODHALENÍ CHYBY	ZNÁMKA
Vysoká	Metody zabezpečení procesu odhalí s velkou pravděpodobností možnou chybu.	**1**
Mírná	Metody zabezpečení procesu můžou odhalit možnou chybu.	**2–3**
Malá	Metody zabezpečení procesu mají pravděpodobnost odhalit možnou chybu.	**4–6**
Velmi malá	Metody zabezpečení procesu mohou sotva zjistit možnou chybu.	**7–8**
Nepravděpodobná	Metody zabezpečení procesu nezjistí, nebo nemůžou zjistit potenciální chybu.	**9–10**

- Známka je přiřazena nejlepším opatřením k odhalení a vyjadřuje pravděpodobnost odhalení příčiny vzniku chyby.

Stanovení rizikového čísla (RPN) se dá považovat za finální krok v rámci analýzy rizik FMEA. Jedná se o to, že odhalené chyby mají vyčíslenu svoji číselnou hodnotu. V případě, že hodnota dosahuje čísla vyššího, jak 125 (tato hodnota je výsledkem součinu středních hodnoty 5 závažnosti, výskytu a odhalení, tj. 5x5x5) jsou zpracována doporučená opatření. V tomto případě dochází k opětovnému hodnocení RPN a jsou analyzována provedená opatření. To proto aby se zjistilo, zda došlo ke snížení hodnoty RPN a tím pádem i samotného rizika. Takto snadno je možné provést kontrolu provedených opatření a jejich efektivitu.

[67] VARGOVÁ, Slavomíra. *LBRAR Analýza rizik: FMEA* [přednáška]. Uherské Hradiště: LUKR FLKŘ UTB, 21. 4. 2017.
[68] Tamtéž

Tabulka 11. Stanovení rozsahu rizikového čísla RPN (zdroj dat: [69])

ROZSAH RIZIKOVÉHO ČÍSLA	
Malé riziko	**0–125**
Střední riziko	**126–768**
Vysoké riziko	**769–1000**

[69] KADLČÍKOVÁ, Nela. *Analýza zdrojů rizik možného ohrožení prvku kritické infrastruktury* [online]. Uherské Hradiště, 2016 [cit. 2018-04-14]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/38736/kadl%c4%8d%c3%adkov%c3%a1_2016_dp.pdf?sequence=1&isAllowed=y. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení. Vedoucí práce Ing. Slavomíra Vargová, Ph.D.

Tabulka 12. Formulář FMEA procesu laboratoře GIS

Objekt: laboratoř GIS Univerzita Tomáše Bati ve Zlíně Fakulta logistiky a krizového řízení										**číslo FMEA: 1**					
Odpovědnost za proces: David Zástřešek, DiS.										**rok výroby modelu / procesu: 2018**					
ANALÝZA HODNOCENÍ SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Funkce / Proces	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (prevence)**	**Stávající řízení procesu (odhalování)**	**Odhalení (O)**	**Rizikové číslo**	**Doporučená opatření**	**Odpovědnost / Provedená opatření**	**Závažnost**	**Výskyt**	**Odhalení**	**RPN**
Objektivní hrozby přírodní	Povodeň	Ztráta HW	**3**	Klimatické podmínky / Protržení hráze	**2**	Žádné	Sledování výšky hladiny řeky / Sledování stupně povodňové aktivity	**4**	**24**	Beze změn	Beze změn	**3**	**2**	**4**	**24**
		Ztráta SW	**6**						**48**			**6**	**2**	**4**	**48**
		Ztráta dat	**7**			Zálohování dat			**56**			**7**	**2**	**4**	**56**
	Požár	Ztráta HW	**3**	Nedbalost na pracovišti / Úmyslné založen	**3**	Žádné	Detektory kouře	**3**	**27**	Beze změn	Beze změn	**3**	**3**	**3**	**27**
		Ztráta SW	**6**						**54**			**6**	**3**	**3**	**54**
		Ztráta dat	**7**			Zálohování dat / Hasicí přístroje			**63**			**7**	**3**	**3**	**63**
	Výpadek elektrické sítě	Ztráta dat	**8**	Klimatické podmínky (led, sníh)	**5**	UPS na serverech	Žádné	**9**	**360**	Instalace motorgenerátoru, který v případě výpadku el. energie zabezpečí dodávku el. energie	Tajemník FLKŘ / Nákup a instalace doporučeného zařízení	**8**	**4**	**5**	**160**

Objekt: laboratoř GIS Univerzita Tomáše Bati ve Zlíně Fakulta logistiky a krizového řízení										**číslo FMEA: 1**					
Odpovědnost za proces: David Zástřešek, DiS.										**rok výroby modelu / procesu: 2018**					
ANALÝZA HODNOCENÍ SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Funkce / Proces	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (prevence)**	**Stávající řízení procesu (odhalování)**	**Odhalení (O)**	**Rizikové číslo**	**Doporučená opatření**	**Odpovědnost / Provedená opatření**	**Závažnost**	**Výskyt**	**Odhalení**	**RPN**
Objektivní hrozby fyzikální	Elektromagnetické pulsy (EMP)	Poškození HW v laboratoři GIS	**4**	Bouřka	**3**	Žádné	Žádné	**8**	**96**	Zálohování dat z lokálních disků na externí uložiště	Vedoucí laboratoře pan Trojan	**4**	**2**	**6**	**48**
		Ztráta dat při poškození HW	**6**		**3**	Zálohování dat lokálních disků	Žádné	**8**	**144**	Odstínění laboratoře GIS	Tajemník / IT technik	**6**	**2**	**5**	**90**
Objektivní hrozby technické nebo logické	Přepětí el. sítě	Ztráta dat	**9**	Přepětí v přívodní el. sítí 230 V	**5**	Přepěťová ochrana 1 stupně (jističe)	Žádné	**4**	**180**	Instalace přepěťové ochrany 3 stupně (přepěťové zásuvky, prodlužovací kabely)	IT technik (přepěťové prodlužovací kabely dostupné v řadu stovek korun)	**9**	**4**	**3**	**108**
		Poškození či zničení HW	**4**		**5**			**4**	**80**			**3**	**5**	**3**	**45**
	Porucha klimatizace	Nedostupnost dat	**2**	Přehřátí serveru	**2**	Servis klimatizačních jednotek	Teplotní čidla snižující výkon serveru	**1**	**4**	Beze změn	Beze změn	**2**	**2**	**1**	**4**
		Ztráta dat	**3**						**6**			**3**	**2**	**1**	**6**
	Porucha paměti PC	Nefunkčnost PC	**2**	Životnost komponentu / EMP	**4**	Žádné	Provedení testu MemTest64	**7**	**56**	Beze změn	Beze změn	**2**	**4**	**7**	**56**

Objekt: laboratoř GIS Univerzita Tomáše Bati ve Zlíně Fakulta logistiky a krizového řízení										**číslo FMEA: 1**					
Odpovědnost za proces: David Zástřešek, DiS.										**rok výroby modelu / procesu: 2018**					
ANALÝZA HODNOCENÍ SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Funkce / Proces	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (prevence)**	**Stávající řízení procesu (odhalování)**	**Odhalení (O)**	**Rizikové číslo**	**Doporučená opatření**	**Odpovědnost / Provedená opatření**	**Závažnost**	**Výskyt**	**Odhalení**	**RPN**
	Porucha zdroje PC				**5**		Žádné		**70**				**5**		**70**
	Porucha grafické karty PC	Nemožnost zobrazení grafického výstupu	**1**		**4**		Provedení testu Furmark		**28**			**1**	**4**		**28**
	Porucha síťové karty PC	Nedostupnost dat	**3**	Životnost komponentu / EMP	**2**	Žádné	Provedení testu pomocí příkazu „ping“ u operačního systému Windows	**7**	**42**	Beze změn	Beze změn	**3**	**2**	**7**	**42**
	Porucha základní desky PC	Nefunkčnost PC	**3**		**3**		Provedení testů jednotlivých komponent základní desky	**7**	**63**			**3**	**3**	**7**	**63**
	Porucha procesoru PC						Provedení testu pomocí software OCCT								
	Porucha zvukové karty PC	Nedostupnost zvukového výstupu	**1**		**6**		Provedení testu pomocí software SoundCheck	**7**	**42**	Beze změn	Beze změn	**1**	**6**	**7**	**42**

Objekt: laboratoř GIS Univerzita Tomáše Bati ve Zlíně Fakulta logistiky a krizového řízení										**číslo FMEA: 1**					
Odpovědnost za proces: David Zástřešek, DiS.										**rok výroby modelu / procesu: 2018**					
ANALÝZA HODNOCENÍ SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Funkce / Proces	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (prevence)**	**Stávající řízení procesu (odhalování)**	**Odhalení (O)**	**Rizikové číslo**	**Doporučená opatření**	**Odpovědnost / Provedená opatření**	**Závažnost**	**Výskyt**	**Odhalení**	**RPN**
	Porucha Harddisku PC	Ztráta dat	**5**	Životnost	**5**	Zálohová dat	Provedení testu pomocí software HDD Guardian 0.5	**5**	**125**	Vytvoření image disku a jeho pravidelná záloha	IT technik	**3**	**5**	**5**	**75**
Subjektivní hrozby neúmyslné (působením uživatele)	Připojení výměnného média (flash disk) k PC	Infikování PC počítačovým virem	**10**	Uživatel	**8**	Antivirový program ESET	Spuštění antivirového testu programu ESET uživatelem	**5**	**400**	Nastavení automatického spouštění antivirového testu	IT technik	**10**	**5**	**3**	**150**
			10		**8**			**5**	**400**	Bezpečnostní politika, tj. zákaz připojování výměnného média a využívání cloudového uložiště	Vedení FLKŘ / Vyučující v laboratoři GIS	**10**	**4**	**6**	**240**
	Instalace vlastního software na počítače	Infikování PC počítačovým virem	**10**	Uživatel	**4**	Antivirový program ESET	Automatický test instalačního souboru programem ESET	**3**	**120**	Beze změn	Beze změn	**10**	**4**	**3**	**120**

Objekt: laboratoř GIS Univerzita Tomáše Bati ve Zlíně Fakulta logistiky a krizového řízení										**číslo FMEA: 1**					
Odpovědnost za proces: David Zástřešek, DiS.										**rok výroby modelu / procesu: 2018**					
ANALÝZA HODNOCENÍ SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Funkce / Proces	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (prevence)**	**Stávající řízení procesu (odhalování)**	**Odhalení (O)**	**Rizikové číslo**	**Doporučená opatření**	**Odpovědnost / Provedená opatření**	**Závažnost**	**Výskyt**	**Odhalení**	**RPN**
	v laboratoři GIS														
	Používání nejnovějšího software oproti stabilním verzím (LTS)	Nesprávné funkce software s možností úniku dat	**4**	Nestabilní verze software	**4**	Žádné	Žádné	**7**	**112**	Používání stabilních verzí (tzv. LTS verzí) software	Vedoucí laboratoře pan Trojan	**3**	**3**	**6**	**54**
	Nesprávná manipulace s daty	Ztráta dat	**5**	Uživatel	**4**	Autentizace pomocí Active Directory a nastavení uživatelských oprávnění (student, zaměstnanec, správce)	Žádné	**3**	**60**	Beze změn	Beze změn	**5**	**4**	**3**	**60**

Objekt: laboratoř GIS Univerzita Tomáše Bati ve Zlíně Fakulta logistiky a krizového řízení										**číslo FMEA: 1**					
Odpovědnost za proces: David Zástřešek, DiS.										**rok výroby modelu / procesu: 2018**					
ANALÝZA HODNOCENÍ SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Funkce / Proces	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (prevence)**	**Stávající řízení procesu (odhalování)**	**Odhalení (O)**	**Rizikové číslo**	**Doporučená opatření**	**Odpovědnost / Provedená opatření**	**Závažnost**	**Výskyt**	**Odhalení**	**RPN**
Subjektivní hrozby úmyslné (vnější i vnitřní / záleží, zda je hacker zaměstnancem nebo studentem FLKŘ či nikoliv)	Napadení FTP serveru	Nebezpeční stažení a zakódování databází	**7**	Hackerský útok	**6**	Nastavení Firewallu	Nastavení Firewallu	**2**	**84**	Beze změn	Beze změn	**7**	**6**	**2**	**84**
	POP3 pošta	Odposlouchávání	**6**		**4**			**2**	**48**			**6**	**4**	**2**	**48**
	IMAP pošta														
	SMTP pošta	PC funguje jako zdroj spamu	**4**	Hackerský útok	**4**	Nastavení Firewallu	Nastavení Firewallu	**3**	**48**	Beze změn	Beze změn	**4**	**4**	**3**	**48**
	WWW server	Napadení webového serveru (změna dat)	**6**		**5**			**3**	**90**			**6**	**5**	**3**	**90**
	HTTPS WWW	Napadení kódovaného WWW serveru	**6**		**4**			**3**	**72**			**6**	**4**	**3**	**72**
	Trojský kůň Net-Devil Pest	Sledování stisknuté klávesy / Odchytávání hesel / Vzdálený přístup	**9**		**4**	Antivirový program ESET	Antivirový program ESET	**3**	**108**			**9**	**4**	**3**	**108**
	Trojský kůň MscanWorm Ramer	Vzdálený přístup / Spouštění http serveru	**8**		**4**			**3**	**96**			**8**	**4**	**3**	**96**

Objekt: laboratoř GIS Univerzita Tomáše Bati ve Zlíně Fakulta logistiky a krizového řízení										**číslo FMEA: 1**					
Odpovědnost za proces: David Zástřešek, DiS.										**rok výroby modelu / procesu: 2018**					
ANALÝZA HODNOCENÍ SOUČASNÉHO STAVU										**NÁVRH OPATŘENÍ**		**HODNOCENÍ STAVU PO REALIZACI OPATŘENÍ**			
Funkce / Proces	**Možná chyba**	**Možné následky chyby**	**Závažnost (Z)**	**Možná příčina chyby**	**Výskyt (V)**	**Stávající opatření (prevence)**	**Stávající řízení procesu (odhalování)**	**Odhalení (O)**	**Rizikové číslo**	**Doporučená opatření**	**Odpovědnost / Provedená opatření**	**Závažnost**	**Výskyt**	**Odhalení**	**RPN**
	Trojský kůň CrackDown Oracle Prosiak Swift Remote	Vzdálený přístup / Odchytávání hesla / Spouští FTP a HTTP server / Proxy	**9**	Hackerský útok	**4**	Antivirový program ESET	Antivirový program ESET	**3**	**108**	Beze změn	Beze změn	**9**	**4**	**3**	**108**
	Trojský kůň Cladestine KWM Litmus SubSARI	Vzdálený přístup / Sleduje stisknuté klávesy / Odchytává hesla / Stahuje další trojské koně / Sleduje komunikaci IRC / Spouští FTP server	**9**		**4**	Antivirový program ESET	Antivirový program ESET	**3**	**108**	Beze změn	Beze změn	**9**	**4**	**3**	**108**

4.3 Shrnutí návrhů spojených s eliminací klíčových rizik

Tato část práce obsahuje finanční, časové, organizační, právní nebo technické náklady spojené s eliminací klíčových rizik. Snahou je navrhnout, pokud možno co nejlepší ale zároveň ekonomicky výhodné či únosné řešení:

- Pro výpadek elektrické sítě je doporučena instalace motorgenerátoru, který v případě potřeby zabezpečí dodávku elektrické energie. Cena tohoto řešení se pohybuje v řádu 400 až 900 tisíc korun v závislosti na výrobci a modelu. Z časového, právního a organizačního hlediska by se jednalo o to, že FLKŘ musí vypsat výběrové řízení na dodavatele a samotnou realizaci díla. To je záležitost v řádu několika měsíců. Další překážkou v realizaci může být nedostatek finančních prostředků nutných k nákupu a instalaci zařízení a jeho připojení do stávající elektrické sítě FLKŘ. Výhodou je, že může zabezpečit elektrickou energii nejen pro laboratoř GIS, ale i celou FLKŘ.
- Elektromagnetické pulsy lze řešit odstíněním laboratoře GIS, a to nákupem stínících desek, které se nainstalují v laboratoři, nebo použitím speciální malby. Výmalba nebo instalace desek není nijak časově náročnou. Provoz laboratoře je také v době prázdnin téměř nulový a nebyl by narušen její chod a výuka samotná. I zde je podmínkou vypsat výběrové řízení minimálně na nákup potřebného materiálu. Cenové náklady u levnějších desek se pohybují okolo 200 Kč za kus. Instalace se provádí pomocí lepících pásek. Takovou montáž zvládne bez problémů sám pracovník správy majetku na FLKŘ. U výmalby se jedná o použití nátěru složeného z oxidů železa a hliníku, který vyvinuli vědci z Tokijské univerzity. Cena dosud nebyla stanovena, ale hovoří se o 200 až 300 korunách za metr čtvereční. Otázkou zůstává, jestli se dále zvýší náklady na odborného pracovníka, který nátěr nanese, nebo tyto práce budou provedeny přes pověřené osoby ze strany správy majetku.
- Přepětí elektrické sítě se řeší instalací přepěťové ochrany 3 stupně (přepěťové zásuvky, prodlužovací kabely). Tyto komponenty jsou snadno dostupné a cenová relace se pohybuje okolo 300 korun. Při počtu 25 ks počítačů a dataprojektoru v laboratoři se jedná o náklady do 9000 korun. Z technického hlediska je výhodnější nákup prodlužovacích kabelů, protože jejich montáž nevyžaduje žádné další náklady spojené s odbornou montáží. I tady je podmínka vypsání výběrového řízení. Pokud bereme v úvahu její výší, nejeví se jako překážka pro samotnou realizaci.

Tento způsob řešení také ukazuje, že prevence se vyplácí i ekonomicky. Pokud budeme počítat cenu jednoho PC na 5000 korun, je hodnota HW zařízení laboratoře GIS minimálně 125 000 Kč. Cena preventivního opatření činí maximálně 9000 Kč. Z toho plyne, že neřešení této hrozby by mělo následky nejen v podobě ztráty dat (výzkumná data apod.), ale i ekonomické.

V případě, že by se taková mimořádná událost stala v době plného provozu laboratoře, jednalo by se také o problém zabezpečení kvality výukového programu FLKŘ.

- Poruchu harddisku u PC je možné vyřešit snadno softwarovou cestou. Existují na to prostředky přímo pod systémem Windows, ale i další s licencí opensource. Jde o to, že v pravidelném časovém intervalu bude vytvořena image disku. Při poruše či zničení harddisku tak nemůže dojít ke kompletní ztrátě dat.
- Používáním nejnovějších verzí software oproti stabilním verzím (takzvaným LTS) se zvyšuje možnost pádu software a ztráta dat. Je samozřejmě pochopitelné, že je snaha výuku provádět na co nejnovějším softwaru s řadou novinek, ale v tomto případě jedinou možností, jak tomuto riziku zamezit je užití LTS verzí. Tyto verze sice neobsahují nejnovější možnosti, ale jsou odzkoušené samotnými uživateli. Případná rizika v podobě neodzkoušených možností zde nehrozí.

ZÁVĚR

Závěrem lze konstatovat, že problematika IT infrastruktury a kybernetické bezpečnosti je velice širokým tématem, které jen stěží obsáhne jedna bakalářská práce. Kybernetika se dostává v rámci naší civilizace stále více do popředí. Stačí se jen podívat do nedávné minulosti a uvědomit si, kde se lidstvo pohybovalo na začátku 20. století a jakého pokroku za posledních 100 let dosáhlo. Počítače zabírali celé místnosti, o výkonu nemluvě. Jen málokdo si uměl přestavit, kam se vývoj v této oblasti posune. Osobní počítače, notebooky nebo chytré telefony jste mohli spatřit pouze ve sci-fi filmech. Dnes jsou vzhledem k postupu vědy a techniky pro nás naprostou samozřejmostí. Neumíme si bez nich přestavit denní život, a nebojím se konstatovat, že se na nich stáváme až závislými.

Provedená analýza rizik na konkrétním příkladu laboratoře GIS jasně dokazuje, jaké hrozby či problémy se mohou vyskytovat a jak je lze odstranit či minimálně eliminovat na nejnižší možnou míru.

Při zpětném hodnocení výstupů je zřejmé, že analyzované hrozby mohou mít vliv na bezpečnost nejen dat (jedince či celé organizace), ale i kompletní IT infrastruktury. Při počtu potenciálně možných útočníků, kteří jsou schopni se do laboratoře dostat fyzicky, tak i možné hrozbě útoků zvenčí. Také se nemusí jednat pouze o data, ale hovoříme i o ekonomickém dopadu na technickém vybavení laboratoře GIS. Takové přepětí v elektrické síti nás dokáže připravit nejen o informace, ale i hardware, který se v laboratoři GIS používá. Pokud se podíváme na objektivní příčiny přírodního charakteru, zde by se zřejmě škody dostali do řádů statisíc korun. Přitom ne vždy musí být řešení hrozeb finančně, technicky, časové, organizačně či jinak náročné. To ukazuje samotná analýza v případech používání nejnovějšího software oproti stabilním verzím (LTS), připojení výměnného média (flash disku) a poruše harddisku. Vyplývá z ní, že se jedná pouze o systémové záležitosti. Lze je řešit bez finančních nákladů, za pomoci bezpečnostní politiky v laboratoři GIS. Tato bezpečností politika by jasně určila, že nelze připojovat výměnná média a doporučila by využití cloudových uložišť. Pro případ poruchy harddisku by určovala frekvenci záloh a osoby pověřené jejich provedením a kontrolou.

Jsem si vědom skutečnosti, že laboratoř GIS je konkrétní specializované pracoviště a neposkytuje komplexní obrázek o IT infrastruktuře celé organizace. Zpracování komplexní analýzy rizik IT infrastruktury pro celou fakultu by bylo náročné z časového i odborného hle-

diska. Vzhledem k vytíženosti lidských zdrojů by bylo zpracování natolik složité, že překračuje rámec bakalářské práce. I přesto se domnívám, že provedená analýza rizik postihuje hrozby, rizika a problémy, které se dají v praxi aplikovat i na ostatní laboratoře, kanceláře či posluchárny náležející k IT infrastruktuře Fakulty logistiky a krizového řízení. Z tohoto pohledu se domnívám, že cíl práce byl naplněn.

SEZNAM POUŽITÉ LITERATURY

1) *Analýza možných způsobů a důsledků poruch (FMEA): referenční příručka*. 4. vyd. Přeložil Ivana PETRAŠOVÁ. Praha: Česká společnost pro jakost, 2008. ISBN 9788002021018.
2) ČERMÁK, Miroslav. Analýza rizik: Jemný úvod do analýzy rizik. *CLEVER AND SMART* [online]. 2013 [cit. 2018-04-08]. Dostupné z: http://www.cleverand-smart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/
3) ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009. Knihovnicka.cz. ISBN 978-80-7399-731-1.
4) DOHNAL, Jan a Jan POUR. *IT v řízení podniku: MBI*. Praha: Professional Publishing, 2016. ISBN 9788074311604.
5) DRASTICH, Martin. *Systém managementu bezpečnosti informací*. První vydání. Praha: Grada Publishing, a.s., 2011. ISBN 978-80-247-4251-9.
6) FMEA Analýza příčin a důsledků. *SVĚT PRODUKTIVITY Beta* [online]. c2012 [cit. 2018-04-14]. Dostupné z: http://www.svetproduktivity.cz/slovnik/FMEA-Analyza-pricin-a-dusledku.htm
7) GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 9788024754574.
8) Historie univerzity. *Univerzita Tomáše Bati ve Zlíně* [online]. Zlín, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/o-univerzite/historie-univerzity
9) HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5., aktualiz. vyd. Brno: Computer Press, 2011. ISBN 9788025131763.
10) JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů* [online]. Vyd.1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 9788074543128. Dostupné také z: http://hdl.handle.net/10563/25821
11) KADLČÍKOVÁ, Nela. *Analýza zdrojů rizik možného ohrožení prvku kritické infrastruktury* [online]. Uherské Hradiště, 2016 [cit. 2018-04-14]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/38736/kadl%c4%8d%c3%ad-kov%c3%a1_2016_dp.pdf?sequence=1&isAllowed=y. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a krizového řízení. Vedoucí práce Ing. Slavomíra Vargová, Ph.D.

12) Kdo jsme. *Univerzita Tomáše Bati ve Zlíně* [online]. Zlín, c2000-2018 [cit. 2018-04-10]. Dostupné z: http://www.utb.cz/o-univerzite/kdo-jsme

13) KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

14) *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2018-04-10]. Dostupné z: https://www.govcert.cz/

15) O nás. *Univerzita Tomáše Bati ve Zlíně: Fakulta logistiky a krizového řízení* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/struktura/o-nas-8

16) O nás. *Univerzita Tomáše Bati ve Zlíně: Fakulta logistiky a krizového řízení* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/struktura/o-nas-6

17) O nás. *Univerzita Tomáše Bati ve Zlíně: Fakulta logistiky a krizového řízení* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/struktura/o-nas-7

18) O nás. *Univerzita Tomáše Bati ve Zlíně: Fakulta logistiky a krizového řízení* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/struktura/o-nas

19) Profil fakulty. *Univerzita Tomáše Bati ve Zlíně* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/o-fakulte/profil-fakulty-2

20) RAK, Jakub. *Aplikovaná informatika - Základy informatiky a IT* [online]. s. 6 [cit. 2018-02-28]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=6085. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.

21) RAK, Jakub. *Aplikovaná informatika* [online]. 86 s. [cit. 2018-02-28]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.

22) Struktura FLKŘ. *Univerzita Tomáše Bati ve Zlíně: Fakulta logistiky a krizového řízení* [online]. Uherské Hradiště, c2000-2018 [cit. 2018-04-11]. Dostupné z: http://www.utb.cz/flkr/struktura/struktura-flkr-1

23) SVOBODA, Petr. *LARBI Bezpečnost informací* [přednáška]. Uherské Hradiště: LUOO FLKŘ UTB, 4. 3. 2016.

24) ŠAFAŘÍK, Zdeněk. *Analýza rizik* [online]. 170 s. [cit. 2018-01-30]. Dostupné z: http://vyuka.flkr.utb.cz/mod/folder/view.php?id=3744. Studijní texty v rámci projektu OPVK „Inovace a rozvoj výuky bezpečnosti se zaměřením na krizové řízení“ CZ.1.07/2.2.00/28.0185.

25) TICHÝ, Milík. *Ovládání rizika: analýza a management*. V Praze: C.H. Beck, 2006. Beckova edice ekonomie. ISBN 80-7179-415-5.

26) Univerzita Tomáše Bati ve Zlíně. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-04-10]. Dostupné z: https://cs.wikipedia.org/wiki/Univerzita_Tom%C3%A1%C5%A1e_Bati_ve_Zl%C3%ADn%C4%9B

27) VARGOVÁ, Slavomíra. *LBRAR Analýza rizik: FMEA* [přednáška]. Uherské Hradiště: LUKR FLKŘ UTB, 21. 4. 2017.

28) VESELÝ, Milan. *Použití metody FMEA pro prevenci chyb v průmyslové výrobě* [online]. Brno, 2012 [cit. 2018-03-29]. Dostupné z: https://dspace.vutbr.cz/bitstream/handle/11012/4439/2012_DP_Vesel%C3%BD_76060.pdf?sequence=-1. Diplomová práce. Vysoké učení technické v Brně. Vedoucí práce Ing. Luboš Kotek, Ph.D.

29) WOSZCZYNSKI, Amy B. a Andrew GREEN. Learning Outcomes for Cyber Defense Competitions. *Journal of Information Systems Education* [online]. 2017, **28**(1), 21-41 [cit. 2018-03-27]. ISSN 10553096. Dostupné z: http://search.ebscohost.com/login.aspx?direct=true&db=lxh&an=126157286&scope=site

30) ZÁSTŘEŠEK, David. *Národní centrum kybernetické bezpečnosti a CERT*. Zlín, 2016. Semestrální práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Ing. Petr Svoboda.

31) ZÁSTŘEŠEK, David. *Systémově vyjádřené modely Národního centra kybernetické bezpečnosti a CERT pro prostředí kybernetické bezpečnosti*. Zlín, 2017. Semestrální práce. Univerzita Tomáše Bati ve Zlíně. Vedoucí práce Prof. Ing. Jiří Dvořák, DrSc.

32) ZEMAN, Martin. *Zavedení metody FMEA do podniku Störi Mantel s.r.o.* [online]. Zlín, 2010 [cit. 2018-04-14]. Dostupné z: https://digilib.k.utb.cz/bitstream/handle/10563/11911/zeman_2010_dp.pdf?sequence=1&isAllowed=y. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta technologická. Vedoucí práce Ing. Josef Hrdina.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DNS	Domain Name Server
DoS	Denial of Service
EMP	Elektromagnetické pulsy
FAI	Fakulta aplikované informatiky
FaME	Fakulta managementu a ekonomiky
FHS	Fakulta humanitních studií
FLKŘ	Fakulta logistiky a krizového řízení
FMEA	Failure Mode and Effect Analysis
FMK	Fakulta multimediálních komunikací
FT	Fakulta technologická
FTP	File Transfer Protocol
GIS	Geografický informační systém
GovCERT.CZ	Vládní CERT České republiky
HTTP	Hypertext Transfer Protocol
HTTPS	Nadstavba protokolu HTTP – chráněný přístup k webovým serverům
HW	Hardware
i OS	Operační systéme pro mobilní telefony od firmy Apple
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Message Access Protocol
IoT	Internet of Things
IP adresa	Rozlišení zařízení síťových rozhraní
ISO	International Organization for Standardization

IT	Informační technologie
KII	Kritická informační infrastruktura
LAN	Local area networks
LTS	Long Term Service Agreement
Mac OS	Operační systém pro počítače a notebooky od firmy Apple
MAN	Metropolitan area network
NASA	National Aeronautics and Space Administration
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	Operační systém
PC	Osobní počítač
POP3	Post Office Protocol 3
RPN	Risk priority number
SMTP	Simple Mail Transfer Protocol
SW	Software
TB	Terabyte
UTB	Univerzita Tomáše Bati ve Zlíně
VUT	Vysoké učení technické
WAN	Wide area networks

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: TOPOLOGIE SÍTĚ – SBĚRNICOVÁ

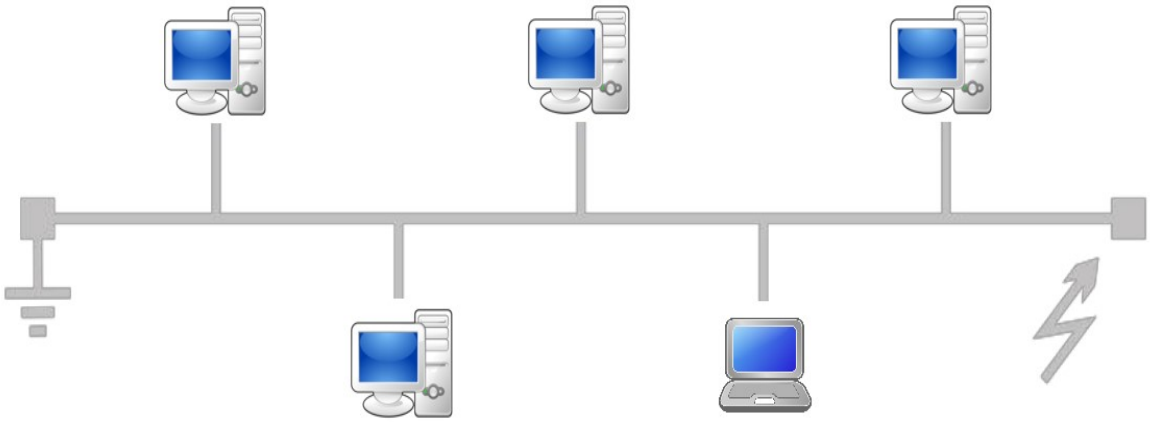


Schéma sběrnice (vodičem je většinou koaxiální kabel).

PŘÍLOHA P II: TOPOLOGIE SÍTĚ – KRUHOVÁ

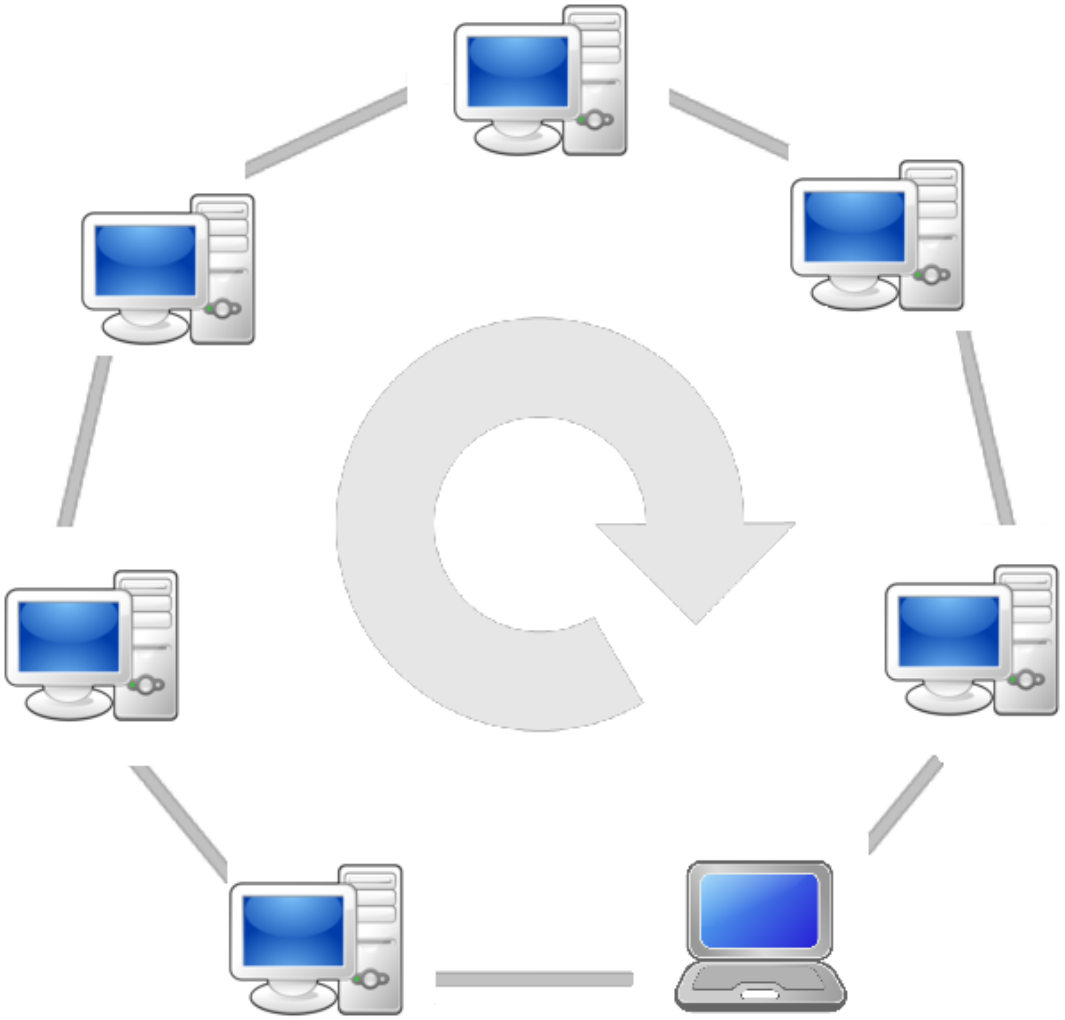


Schéma kruh se směrem toku dat (informace jde od stanice ke stanici).

PŘÍLOHA P III: TOPOLOGIE SÍTĚ – HVĚZDA

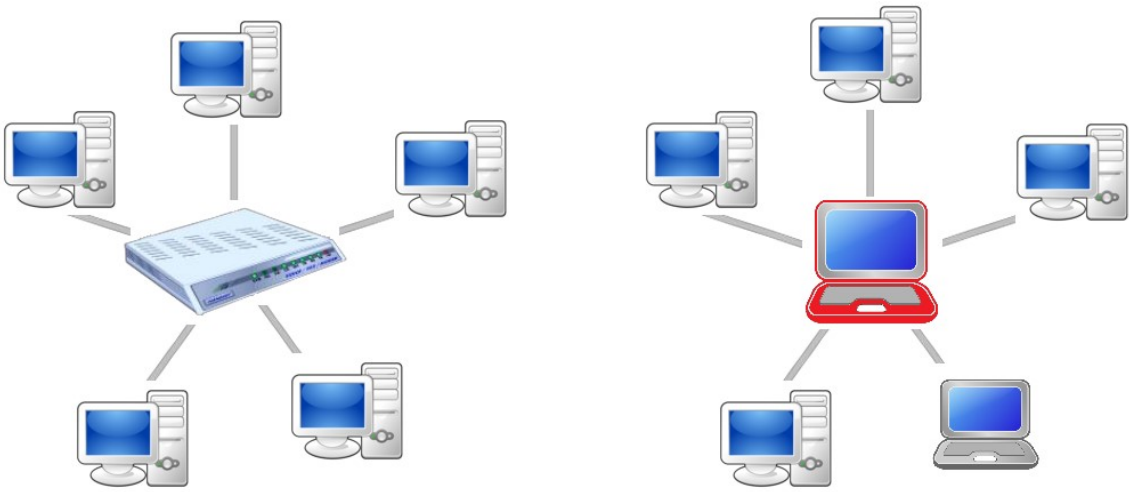


Schéma hvězda, kde jako aktivní prvek je např. rozbočovač, přepínač nebo PC (označeno červeně).

PŘÍLOHA P IV: TOPOLOGIE SÍTĚ – STROM

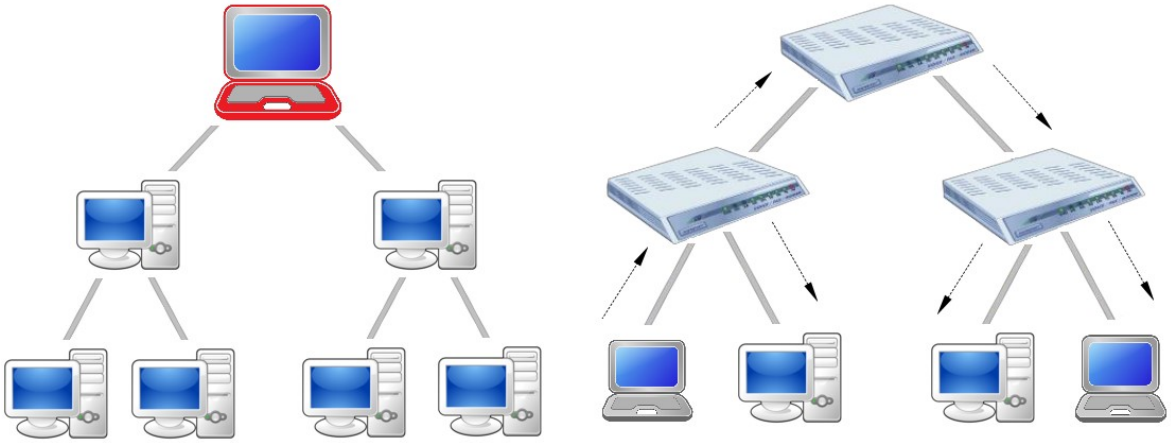


Schéma strom, kde jako aktivní prvek je osobní počítač (označeno červeně) nebo např. přepínače, rozbočovače.

PŘÍLOHA P V: TOPOLOGIE SÍTĚ – PÁTEŘNÍ SÍŤ

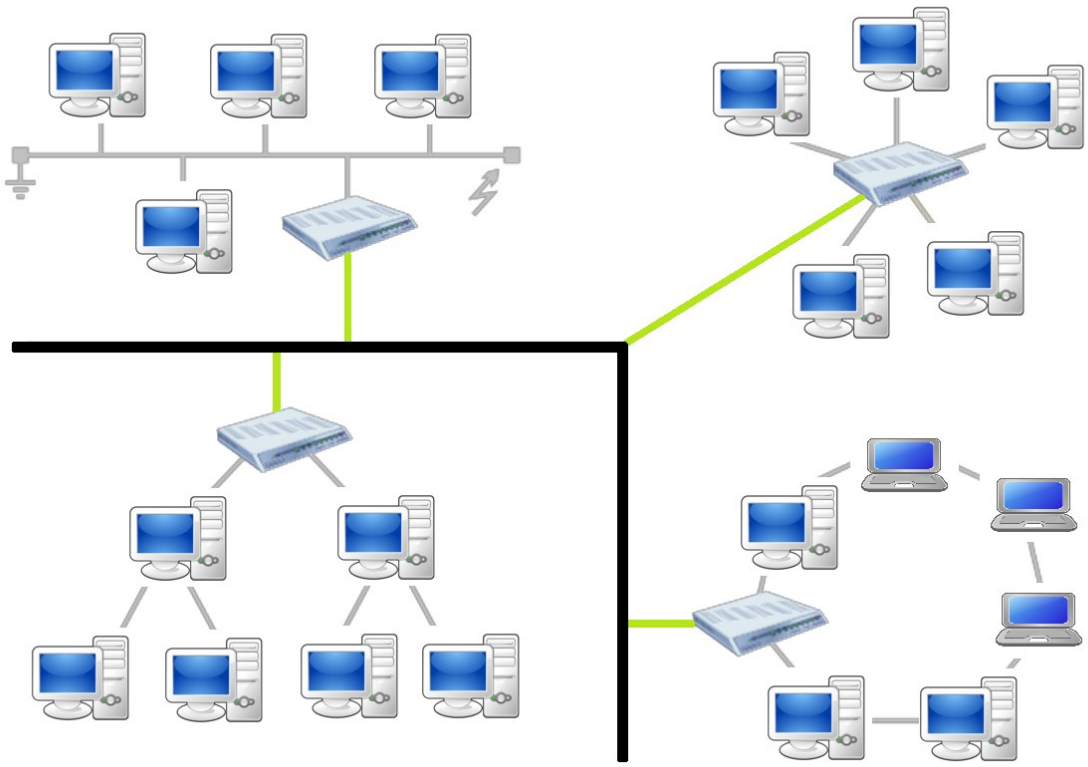


Schéma páteřní sítě (páteřní síť vyznačena černě), kdy ostatní sub-sítě jsou na ni připojeny a vytváří tak jeden celek.