Aktiva a současné hrozby v oblasti informačních technologií

Michaela Dubská

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva
akademický rok: 2018/2019

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

Jméno a příjmení:	**Michaela Dubská**
Osobní číslo:	**L16481**
Studijní program:	**B2825 Ochrana obyvatelstva**
Studijní obor:	**Ochrana obyvatelstva**
Forma studia:	**prezenční**

Téma práce: **Aktiva a současné hrozby v oblasti informačních technologií**

Zásady pro vypracování:

1. **Zpracujte rešerši současného stavu vztahující se k dané problematice s důrazem na monografie a analytické materiály.**
2. **Seznamte se s důležitými aktivy v oblasti informačních technologií.**
3. **Seznamte se s významnými hrozbami v oblasti informačních technologií.**
4. **Implementujte identifikovaná aktiva a hrozby do vybraného softwarového nástroje.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

[1] NEZMAR, Luděk. Zákon o kybernetické bezpečnosti pro organizace – Implementace nových povinností do praxe. Grada, 2018. ISBN 978-80-271-0899-2.

[2] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[3] JIRÁSEK, Petr, NOVÁK, Luděk a POŽÁR, Josef. Výkladový slovník Kybernetické bezpečnosti: Třetí doplněné a upravené vydání. 3. Praha: Policejní akademie České republiky v Praze, 2015. ISBN 978-80-7251-436-6

Další odborná literatura dle doporučení vedoucího bakalářské práce.

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

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

V Uherském Hradišti dne 30. listopadu 2018

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

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

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

PROHLÁŠENÍ AUTORA
BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

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

V Uherském Hradišti, dne: 15.5.2019

Jméno a příjmení studenta: Michaela Dubská

.....
podpis studenta

ABSTRAKT

Aktiva a současné hrozby v oblasti informačních technologií je téma, kterému se celá práce věnuje. V úvodní části se seznámíme s tím, co to vlastně jsou aktiva, jaké je jejich možné dělení podle různých kritérií. Pokračujeme informacemi o hrozbách a jejich dělením. Následně se seznámíme s informační bezpečností podle normy ČSN ISO/IEC 27001. Pokračujeme prací v programu Riskan. Je to softwarový program, který slouží pro podporu analýzy rizik. Obsahuje číselníky, které se zabývají aktivy a hrozbami z oblasti informační bezpečnosti. Vzhledem k rychlému vývinu techniku, jsou ale číselníky zastaralé a proto je cílem této práce číselníky aktualizovat a obnovit.

Klíčová slova: Aktiva, hrozby, informační bezpečnost, informační technologie, Riskan,

ABSTRACT

Assets and current threats in the field of information technology is a topic that the whole work is dedicated to. In the introductory part we will learn what assets are, what is their possible division according to different criteria. We continue with information about threats and their division. Subsequently, we will become familiar with information security according to ČSN ISO / IEC 27001. We continue to work with the Riskan program. It is a software program that supports risk analysis. Includes codebooks that deal with information security assets and threats. Due to the rapid development of technology, however, the dials are obsolete and therefore the aim of this work is to update and renew the dials.

Keywords: Assets, Threats, Information Security, Information Technology, Riskan

Ráda bych poděkovala svému vedoucímu práce Ing. Petru Svobodovi za cenné rady, připomínky, jeho ochotu a věnovaný čas. Děkuji Barboře Svorové za pomoc při překladu do anglického jazyka a Martě Horilové za jazykovou korekturu. Velké díky patří také mé rodině, která mi umožnila studovat a také přátelům a známým, kteří mi byli po celou dobu studia velkou oporou.

"Je jenom jedna cesta za štěstím a to přestat se trápit nad tím, co je mimo naši moc."

Epiktétos

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

V Uherském Hradišti, 13. 5. 2019

Michaela Dubská

OBSAH

ÚVOD

Když se v dnešní moderní a uspěchané době řekne informační technologie, každý z nás si představí něco jiného. Velmi záleží na tom, koho se na to vlastně vůbec ptáme. Jestli se zeptáme naší mladé generace, která má obrovský přehled o tom jaké jsou nejmodernější, nejlepší a nejúžasnější prostředky moderní doby anebo jestli se zeptáme někoho ze starší generace, kteří toho neznají zas až tak mnoho. A když se to tak vezme naše starší generace je mnohdy ráda, když se dokáže sžít a nějak "skamarádit", se základní věcí jako je obyčejný mobilní telefon, který do kategorie informačních technologií také patří. Ale zpět k informačním technologiím, co to vlastně je a co si pod tímto názvem vůbec představit? Úplně jednoduše je to všechno kolem nás, s čím se dá nějak komunikovat, využít připojení k internetu, nebo nám jakýmkoliv způsobem zjednodušují náš uspěchaný dnešní život. Bez spousty z nich už si ani každodenní život neumíme představit. Do této skupiny můžeme zahrnout ať už zmiňované mobilní telefony, tablety, laptopy, stolní počítače, ale i všechnu další výpočetní techniku. Prostředky, jako je tiskána, kopírky, skenery, faxy, wifi routery a spoustu dalšího příslušenství, které považujeme za standart. Když si koupíme např. notebook a vůbec si neuvědomujeme, že je to další informační technologie. A bohužel tak jako všude, tak i v oblasti informačních technologií se vyskytuje velké množství nebezpečí a hrozeb. Hrozby a rizika se vyskytují opravdu všude a to i tam, kde by nás to vůbec nenapadlo. Stačí jenom obyčejné připojení se k jakékoliv veřejné internetové síti, nebo otevření přílohy v e-mailu a neštěstí je na světě. Nikdy nikdo z nás neví, kde na nás to nebezpečí číhá a je to jenom otázka času a toho, jak velký si dáváme pozor a jaké používáme zabezpečovací prostředky k tomu, abychom předcházeli vzniku možnosti útočníka nám ublížit.

Vzhledem k tomu, že je dnešní moderní doba tak nebezpečná a nevyzpytatelná, jsem se rozhodla zabývat se tímhle, pro mě velmi zajímavým tématem, v mé bakalářské práci a to z důvodu, abych si rozšířila informace, zase v jiném okruhu vědomostí. A také si myslím, že tohle téma bude velmi dlouho aktuální a nikdy člověk neví, kde skončí a co všechno se mu bude anebo taky nebude v budoucím povolání a životě hodit.

V první části je práce zaměřená na právní vymezení problematiky v oblasti informačních technologií a následuje úvodní seznámení se základními pojmy a uvedení do základu problematiky. Následuje krátké zmínění o kybernetické bezpečnosti, která úzce souvisí

s informačními technologiemi. Práce se věnuje základním pojmům z oblasti kybernetiky, následuje krátký úvod do historie, vývoj v ČR a v zahraničí a shrnutí aktuálního stavu.

Druhá kapitola se věnuje bezpečnosti informačních technologií. V jakých právních předpisech je v České republice zakotvena a kde můžeme najít mnoho informací o této problematice. V závěrečné části je uvedena a rozebrána Mezinárodní norma ISO/IEC 27001, která se zaměřuje na informační bezpečnost.

Následuje kapitola pouze a jenom o informačních aktivech, kde je zase uvedená základní definice aktiva. Rozdělení do několika skupin, podle různých hledisek a kritérií.

Pokračujeme informačními hrozbami, vymezením toho co to hrozba je a opět jejich rozdělení z různého druhu pohledu a podle různých možných kritérií a kategorií.

Praktická část práce obsahuje tabulky, které znázorňují současné aktiva a hrozby. Také zde najdeme tabulky s obsahem nových aktiv a hrozeb, které jsou podkladem pro tvorbu nových číselníku v SW programu Riskan. SW Riskan je program, který slouží k vytvoření analýzy rizik. Následuje popis postupu aktualizace číselníků, ukázka nových a starých číselníků pro možnost porovnání. Závěr praktické části obsahuje názornou ukázku tvorby analýzy rizik s barevným vymezením pravděpodobnosti rizika.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ TECHNOLOGIE

Informační technologie (dále ICT) tvoří velkou skupinu informačních technologií, které se používají pro komunikaci a práci s informacemi. [1]

1.1 Právní předpisy

Základním právním předpisem, který se zabývá problematikou v oblasti bezpečnosti informačních technologií, je zákon č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů a o změně souvisejícími vyhláškami:

- 316/2014 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitosti podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).
- 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích.

Dále výše uvedený zákon mění:

- 106/1999 Sb. Zákon o svobodném přístupu k informacím.
- 231/2001 Sb. Zákon o provozování rozhlasového a televizního vysílání.
- 127/2005 Sb. Zákon o elektronických komunikacích.
- 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Při řešení kybernetické bezpečnosti lze také použít zejména zákony (včetně příslušných vyhlášek):

- 101/2000 Sb. Zákon o ochraně osobních údajů.
- 365/2000 Sb. Zákon o informačních systémech veřejné správy.
- 499/2004 Sb. Zákon o archivnictví a spisové službě.
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014.

Zákon o kybernetické bezpečnosti byl zpracován Národním bezpečnostním úřadem, kde návrh byl předložen vládě 31. července 2013. V účinnost vstoupil dne 1. ledna 2015.

Zákon je založen na třech hlavních pilířích:

- Bezpečnostní opatření.
- Hlášení kybernetických bezpečnostních incidentů.

- Opatření Úřadu.

Hlavními zásadami zákona jsou:

- Snaha minimalizovat zásahy do práv soukromých subjektů.
- Individuální odpovědnost každého subjektu za bezpečnost vlastní sítě.
- Technologická neutralita.

Zákon upravuje veškerá práva a povinnosti osob a orgánů veřejné moci. Cílem je stanovit co nejmenší požadavky na zabezpečení kritické infrastruktury, kritické komunikační infrastruktury, významných informačních systémů a významných sítí. [2]

1.2 Základní názvosloví

V následující části se seznámíme se základními pojmy z oblasti informační bezpečnosti, vymezených v zákoně a výkladovém slovníku:

Kybernetický prostor – *"digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací."*

Kritická informační infrastruktura – *"prvek nebo systém prvků kritické infrastruktury v odvětví komunikačních a informačních systémů."*

Významný informační systém – *"informační systém zpracovaný orgánem veřejné moci, který není kritickou infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci."*

Kybernetická kriminalita -– *"trestná činnost, v níž figuruje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponent, případně větší množství počítačů samostatných nebo propojených* do počítačové *sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti"*

Počítačová kriminalita/Kybernetická kriminalita – *"zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě nebo přímo s nimi spojený."*

Správce informačního systému orgán nebo osoba – *"určují účel zpracování informací a podmínky provozování informačního systému."*

Správce komunikačního systému orgán nebo osoba – *"určují účel komunikačního systému a podmínky jeho provozování, prostředků tvořících informační nebo komunikační systém."*

Významná síť – *"síť elektronických komunikací, zajišťující přímé zahraniční propojení do veřejných komunikačních sítí, zajišťující přímé připojení ke kritické informační infrastruktuře."* [3] [4][5]

Aktivum – cokoliv co má hodnotu pro jednotlivce, organizace nebo veřejnou správu. [5][6]

Informační aktivum – znalosti a data, která mají pro organizaci hodnotu (význam). [5]

Hrozba – potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace. [5]

Bezpečnostní hrozba – potenciální příčina nežádoucí události, která může mít za následek poškození systému a jeho aktiv, např. zničení, nežádoucí zpřístupnění (kompromitaci), modifikaci dat nebo nedostupnost služeb. [5]

1.3 Kybernetická bezpečnost

Vzhledem k tomu, že kybernetické útoky a různá kybernetická napadení patří mezi docela významné hrozby v oblasti informačních technologií a nejenom této oblasti, je dobré se o nich dozvědět pár základních informací.

1.3.1 Vymezení základních pojmů

Základní pojmy jsou stanovený prostřednictvím zákona č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně některých souvisejících zákonů a souvisejícími vyhláškami.

Kybernetická bezpečnost – souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.

Kybernetická kriminalita – trestná činnost, v níž funguje určitým způsobem počítač jako souhrn technického a programového vybavení (včetně dat), nebo pouze některá z jeho komponentů, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět zájmu této trestné činnosti (s výjimkou té trestné

činnosti, jejímž předmětem jsou popsána zařízení jako věci movité) nebo jako prostředí (objekt) nebo jako nástroj trestné činnosti.

Kybernetický prostor – digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací.

Kybernetický útok – útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.

Kyberterorismus – trestná činnost páchána za primárního využití či cílení prostředků IT s cílem vyvolat strach, či neadekvátní reakci. Používá se nejčastěji v kontextu extremisticky, nacionalisticky a politicky motivovaných útoků. [5] [4]

1.3.2 Historie vývoje kybernetiky

Kybernetika patří mezi jeden z nejmladších vědních oborů. Začala vznikat ve čtyřicátých letech dvacátého století. Vznik je velmi úzce spojen s vývojem mnoha jiných vědních oborů, jako je matematická logika, neurofyziologie a rozvoj některých technických oborů - elektronika, výpočetní technika a řídící technika. Kybernetika není pouze o tom, že by přebírala poznatky jiných věd, ale snaží se hledat to, co jednotlivé vědní obory spojuje. Postihuje určité společné rysy různých vědních oborů, čímž přispívá k jejich propojení.

Za zakladatele kybernetiky je považován americký matematik Norbert Wiener (1894 - 1964), který v průběhu 2. světové války spolupracoval s mexickým neurofyziologem Arturem Rosenbluethem. Výsledkem společného výzkumu bylo odhalení určitých společných vlastností v chování jednoduchých částic živého organismu - nervové buňky (animal) a neživého mechanismu - stroje (machine). V roce 1948 vydal Wiener knihu "Cybrnetics or Control and Communication in the Animal and the Machine". Tato kniha je považována za základní kámen vědní disciplíny nazývané Kybernetika. [7]

Název kybernetika má řecký původ a objevuje se např. v Platónově díle Dialogy, kde se tímto názvem označuje "umění řídit lodě a spravovat provincie." V novověku byl název kybernetika použit pro označení budoucí vědy o řízení lidské společnosti.

Nelze tvrdit, že pouze Norbert Wiener a několik jeho kolegů jako jediní vytvořili kybernetiku. Její vznik je potřeba chápat jako výsledek rozvoje duchovních a matematických sil lidské společnosti a rozvoje vědeckého poznávání světa. [8]

1.3.3 Vývoj v ČR

Povědomí o kybernetice mezi veřejnost přišlo do České republiky, v dřívější době Československé republiky, poměrně brzy. V roce 1949 se v Biologických listech od autora prof. Josefa Charváta, dřívějšího přednosty III. interní kliniky LF Univerzity Karlovy, článek *Cybernetismus, nauka o kontrole a spojích v živé hmotě a ve strojích*. Tento článek se ovšem stal na delší dobu pouze jediným článek, kde byl pojem kybernetika uveden.

V Sovětském svazu a tedy i v rámci celého Východního bloku, byla totiž kybernetika označena za nepřijatou vědu a řadu let se o ni nesmělo veřejně psát ani diskutovat.

Příklad definice kybernetiky ze sovětského slovníku - Sovětský filozofický slovník z roku 1954:

"Kybernetika - reakční pavěda, vzniklá v USA po druhé světové válce, která se široce rozšířila i v jiných kapitalistických zemích. Kybernetika jasně vyjadřuje jeden ze základních rysů buržoazního světového názoru - jeho nelidskost, snahu změnit pracující jako doplněk zdroje stroje, změnit je na stroj výroby a na nástroj války. Společně s tím je pro kybernetiku charakteristická imperialistická utopie nahradit živého myslícího člověka, bojujícího za své zájmy strojem, jak ve výrobě, tak i ve válce. Ti, kdož připravují novou světovou vojnu, používají kybernetiku ve svých hrozných praktických činech…"

"…. Kybernetika se proto jeví, nejenom ideologickou zbraní imperialistické reakce, ale prostředkem k uskutečnění jejich agresivních válečných plánů." [9]

Pohled na kybernetiku se začal v zemích se železnou oponou postupně měnit až od poloviny 50. let. Roku 1955 vyšel v sovětském časopise Voprosy filosofie článek "Co je to kybernetika". Autorem tohoto článku byl český marxistický filozof Arnošt Kolman, který žil několik let v Sovětském svazu, kde působil na funkci ředitele moskevského filozofického ústavu. V roce 1956 pak v Moskvě Kolman vydal velmi útlou knížku nazvanou Kybernetika, ve které velmi stručně vysvětluje obecné principy vznikající nové vědy. [10]

1.3.4 Vývoj v zahraničí

Počátky vývoje kybernetiky ve světě sahají až do roku 1948, kdy souběžně v USA a ve Francii vyšla kniha od amerického matematika Norberta Wienera (1894 - 1964). *"Cybernetics o Control and Communication in the Animal and the Machine"* [9]. Tato kniha se stala výchozím dílem pro nově se utvářející vědeckou disciplínu. Na počátcích

rozvoje pracoval Norbert Wiener spolu s mexickým neurofyziologem A. S. Rossenbluethem (1900 - 1970) a skupinou několika dalších spolupracovníků již od začátku 2. světové války.

Pokud se podíváme zpět do minulosti, zjistíme, že slovo kybernetika není nijak novodobým odborným termínem, ale pochází ze starověké řečtiny, **kde kybernetes znamená kormidelník nebo také lodivod.**

Jako první použil takové označení antický filozof Platón (427 - 347 př. n. l.) a to ve smyslu "vědy o řízení lodí". V první polovině 19. stol. francouzský matematik a fyzik A. M. Ampere (1775 - 1836) nazval kybernetikou "cybernetique" v tehdejší době neexistující vědu, která se zabývala řízením společenských a ekonomických soustav. Wiener jej pak poprvé použil v jedné ze svých prací v roce 1947.

V době, po vydání Wienerovy knihy, docházelo k příznivým i nepříznivým kritikám. Na jedné straně docházelo k úplnému zatracování a tvrdému odmítání kybernetiky a na druhé straně docházelo k obdivu a propagaci a někdy až překotnému zavádění do různých technických či společenských oblastí, např. biologie, medicíny, energetického hospodářství, ekologie nebo také výzkumu jazyků a hudby. [10]

1.3.5 Aktuální stav v ČR

V současné době se kybernetickou bezpečností v České republice (dále ČR) zabývá Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).

Národní úřad pro kybernetickou a informačních bezpečnost byl založen 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se měnil zákon č. 181/2014 SB., o kybernetické bezpečnosti a o změně souvisejících zákonů.

Mezi hlavní činnosti NÚKIB:

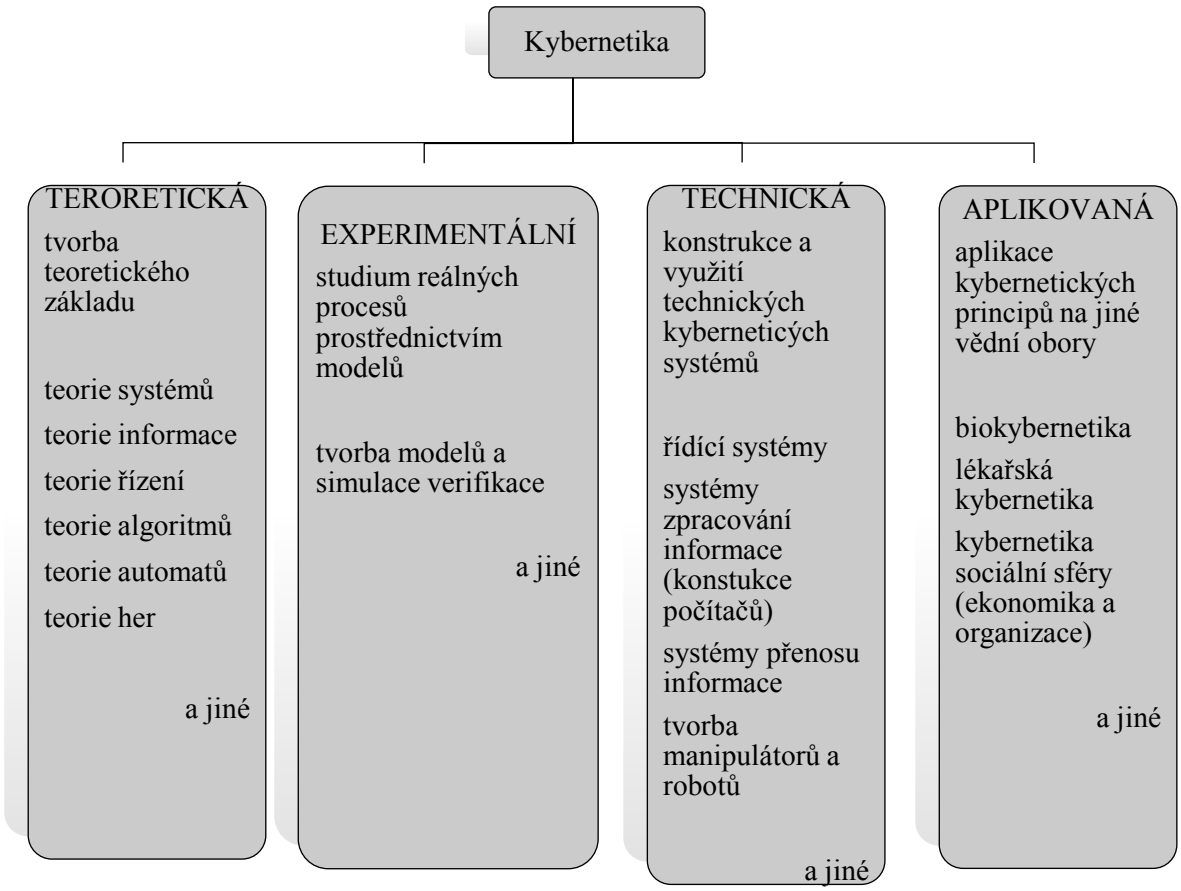
- Provozovat Vládní CERT (Computer Emergency Response Team) České republiky.
- Spolupráce s ostatními národními CERT týmy a CSIRT (Computer Security Incedent Response Team) týmy.
- Spolupráce s mezinárodními CERT týmy a CSIRT týmy.
- Příprava bezpečnostních standardů pro informační systémy KII (kritická informační infrastruktura) a VIS (veřejná informační služba).

- Osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti.
- Výzkum a vývoj v oblasti kybernetické bezpečnosti.
- Ochrana utajovaných informací v oblasti informačních komunikačních systémů.
- Kryptografická ochrana.
- Národní centrum PRS (NCPRS) - jedna ze služeb evropského satelitního systému Galileon. [11]

1.3.6 Klasifikace kybernetiky

Jako nově vzniklý a stále se rozvíjející obor, nemá kybernetika úplně přesně vymezenou působnost a také členění na dílčí obory nebývá úplně jasné.

Na obrázku je uvedená nejčastěji prezentovaná klasifikace kybernetiky s uvedením dílčích oborů. V současné době, podle rozvoje kybernetiky, představuje technická kybernetika jednu z nejrozvinutějších částí. Z teoretického základu využívá poznatků všech vědních disciplín, které patří do teoretické kybernetiky. Proto na následujícím obrázku můžeme vidět ty nejdůležitější. [8]



Obrázek 1 - Klasifikace kybernetiky [8]

2 BEZPEČNOST INFORMAČNÍCH TECHNOLOGIÍ

Vývoj informační bezpečnosti je úzce spojen s vývojem a rozvojem informačních technologií. Informační technologie z pohledu bezpečnosti obsahují:

- Technické prostředky (hardware, paměťová média a prostředky pro komunikaci).
- Programové prostředky (software).
- Data.

Data, programové prostředky a technické prostředky tvoří **systémové části informačních technologií**. Každá z částí je potenciálním rizikem možného útoku, tj. bezpečnost informačních technologií musí být na všech úrovních a ve všech částech. Jako bezpečnost můžeme považovat ochranu informací, systémů a služeb proti nehodám, chybám, zneužití a manipulaci, která snižuje riziko pravděpodobnosti a účinku.

Mezi základní stavební kameny bezpečnosti v oblasti informačních technologií patří:

- **Důvěrnost** – (Confidentality) přístup k důvěrným informacím pouze pro osoby, které mají oprávnění.
- **Integrita** – (Integrity) důležitá je kontrola nad veškerými změnami důvěrných informací a procesů, proto se nesmí zapomenout na správné a úplné zajištění těchto změn.
- **Dostupnost** – (Availability) představuje zabezpečení informací v okamžiku, kdy by se k nim chtěla dostat neoprávněná osoba. [12] [13] [14]

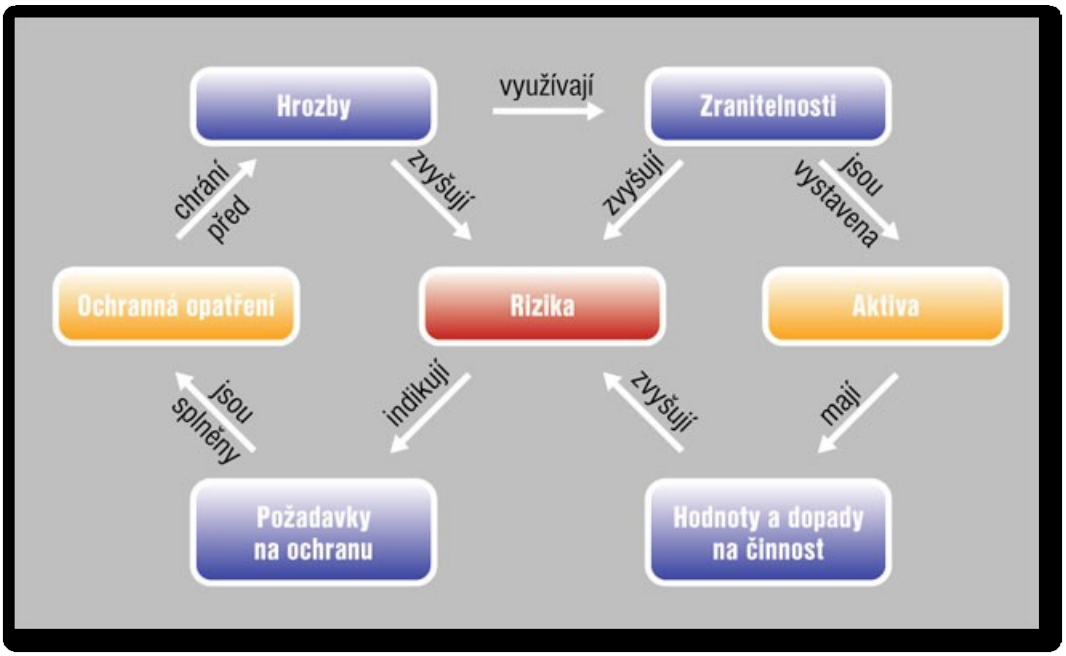
Obrázek 2 - Životní cyklus základních atributů bezpečnosti [15]

Z výše uvedených vlastností lze obecně říci, že bezpečnost informačních technologií je vlastnost systému popisující míru ochrany důvěrných objektů (jednotlivých částí informačních technologií).

Základní pojmy v oblasti informační bezpečnosti:

- **Riziko** – nebezpečí, možnost škody, ztráta, nezdaru. Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu.
- **Zranitelnost** – slabé místo aktiva nebo opatření, které může být zneužito jednou nebo více hrozbami.
- **Ohrožení systému** – okolnosti, které mohou vést ke ztrátám nebo škodám.
- **Napadení** – činnost, která vede ke způsobení škod nebo ztrát.
- **Kontrola** – ochranná opatření, která vedou k minimalizaci ohrožení systému. [5] [16] [15]

Na následujícím obrázku jsou vyobrazeny vztahy v rámci informační bezpečnosti. Je zde zachyceno, jakým způsobem jsou ovlivněny všechny prvky informační bezpečnosti = silné a slabé stránky bezpečnostních rizik.



Obrázek 3 – Návaznosti v informační bezpečnosti [17]

2.1 General Data Protection Regulation /GDPR

Nařízení Evropského Parlamentu a Rady Evropské Unie 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46ES (obecné nařízení o ochraně osobních údajů).

Nařízení představuje nový právní rámec ochrany osobních údajů v rámci Evropské unie, kdy cílem je hájit co nejvíce práva občanů proti neoprávněnému zacházení s jejich osobními údaji. General Data Protection Regulation (dále jen GDPR) se týká veškerých firem, institucí, ale i jednotlivců, kteří zpracovávají data uživatelů. Se zavedením GDPR přišlo i zavedení vysokých pokut při porušování pravidel.

Aplikace GDPR v České republice

Obecné nařízení na ochranu osobních údajů, anglická zkratka GDPR, je nejvíce ucelený soubor pravidel na ochranu dat na světě. GDPR se týká společností a institucí mimo území EU, ale působí na evropském trhu. Hlavním cílem GDPR je chránit digitální práva občanů EU.

25. května 2018 začala účinnost GDPR v celé Evropské unii. V České republice tak došlo k nahrazení dosud platné právní normy na ochranu osobních údajů v podobě směrnice 95/46/ES a související zákon č. 101/2000 Sb., o ochraně osobních údajů. Do roku 2018 působil v oblasti ochrany osobních údajů český Úřad pro ochranu osobních údajů (ÚOOÚ), který zůstal i nadále ve své funkci. [18] [19]

2.2 ČSN ISO/IEC 27001

Mezinárodní norma ČSN ISO/IEC 27001 upřesňuje požadavky na implementování, udržování, ustavení a neustálé zlepšování systému řízení bezpečnosti informací v rámci kontextu rizik činnosti organizace. Obsahuje taky požadavky na ošetření a posouzení rizik bezpečnosti informací, přizpůsobené potřebám organizace.

Požadavky normy jsou použitelné a aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu jejich činností.

Obsah normy:

- Předmět normy.
- Normativní odkazy.

- Termíny a definice.
- Kontext organizace.
- Leadership.
- Plánování.
- Podpora.
- Provoz.
- Vyhodnocování výkonnosti.
- Zlepšování.
- Příloha a - cíle opatření a jednotlivá bezpečnostní opatření.

2.2.1 Předmět normy

Norma specifikuje požadavky pro budování implementaci, řízení, monitorování, přezkoumání, údržbu a zlepšování dokumentovaného ISMS s ohledem na celková podnikatelská rizika organizace.

Požadavky normy jsou použitelné a aplikovatelné ve všech organizacích bez ohledu na jejich typ, velikost a povahu jejich činností.

2.2.2 Normativní odkazy

Pro použití standardu ČSN ISO/IEC 27001 jsou nezbytné odkazy na následující dokumenty:

- ČSN ISO/IEC 27002:2014 (36 9798) Informační technologie – *Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací.*
- ČSN ISO/IEC 27003 (36 9790) Informační technologie – *Bezpečnostní techniky – směrnice pro implementaci systému řízení bezpečnosti informací.*
- ČSN ISO/IEC 27004 (36 9790) Informační technologie – *Bezpečnostní techniky – Řízení bezpečnosti informací – Měření.*
- ČSN ISO/IEC 27005 (36 9790) Informační technologie – *Bezpečnostní techniky – Řízení rizik bezpečnosti informací.*
- ČSN ISO 31000:2010 (01 0351) Management rizik – *Principy a směrnice.* [20]

2.2.3 Termíny a definice

Dostupnost – přístupnost a použitelnost na žádost oprávněné entity.

Důvěrnost – informace není dostupná nebo není odhalena neoprávněným jednotlivcům.

Integrita – přesnost a úplnost.

Bezpečnost informací – zachování dostupnosti, důvěrnosti a integrity informací. [5]

2.2.4 Kontext organizace

Porozumění organizaci a jejímu kontextu – určit vnější a vnitřní problematiku ovlivňující ISMS.

Porozumění potřebám a očekáváním zainteresovaných stran – určení zájmových skupin podstatných pro ISMS a určení požadavků těchto skupin na ISMS.

Určení rozsahu ISMS – zohlednění otázek a požadavků organizace a závislosti na podpůrné organizace.

Systém managementu bezpečnosti informací – organizace musí stanovit, zavést, udržovat a neustále zlepšovat ISMS.

2.2.5 Leadership

Vrcholové vedení organizace musí s ohledem na systém řízení bezpečnosti informací:

- Demonstrovat vůdčí roli a závazek:
  - Stanovení politiky a cílů bezpečnosti informací.
  - Zajištění začlenění do procesů organizace.
  - Zajištění dostupnosti zdrojů.
  - Podpora dalších manažerských rolí.
- Stanovit politiku bezpečnosti informací:
  - Přiměřená potřebám organizace.
  - Obsahuje cíle bezpečnosti informací.
  - Obsahuje závazek naplnit požadavky na bezpečnosti informací.
  - Obsahuje závazek neustálé zlepšování ISMS.
- Zajistit odpovědnost a pravomoc - vedení musí přidělit role, pravomoci a odpovědnosti spojené s bezpečností informací.

2.2.6 Plánování

Činnost na pokrytí rizik a příležitostí

Organizace by při plánování ISMS měla zohlednit rozsah ISMS a určit rizika a příležitosti zabývající se:

- Jak ISMS zajistí naplnění stanovených výsledků.
- Jak předcházet nebo snižovat nepředvídatelné jevy.
- Dosahováním neustálého zlepšování.

Organizace by měla plánovat:

- Činnosti reagující na rizika a příležitosti.
- Jak tyto činnosti přizpůsobit do procesů ISMS a jak je hodnotit.

Hodnocení rizik bezpečnosti informací

Organizace musí určit a využít proces pro hodnocení rizik, který:

- Ustanoví a udržuje kritéria po rizika bezpečnosti informací.
- Zajistí, že opakovaní, poskytne shodné, platné a porovnatelné výsledky.
- Identifikuje rizika bezpečnosti informací - ztráta důvěrnosti, integrity, a dostupnosti informací v rozsahu ISMS + určení vlastníka rizika.
- Analyzuje rizika bezpečnosti informací - hodnocení dopadů + hodnocení pravděpodobnosti výskytu + určení úrovně rizika.
- Hodnocení rizika bezpečnosti informací - srovnání výsledků s kritérii + určení priorit pro zvládání rizika.

Organizace musí udržovat dokumentované informace o procesu pro hodnocení rizik.

Zvládání rizik bezpečnosti informací

Organizace musí určit a využívat proces pro zvládání rizik, který:

- Vybírá vhodnou formu zvládání rizik.
- Určuje všechna opatření pro zvládání rizik.
- Srovnává vybraná opatření s přílohou A.
- Vytvoří prohlášení o aplikovatelnosti - zdůvodnění výběru i vyloučení.
- Formuluje plán zvládání rizik.
- Získá souhlas vlastníka rizika se zvládáním rizik a přijetím zbytkových rizik.

Organizace musí udržovat dokumentované informace o procesu pro zvládání rizik.

Cíle informační bezpečnosti a plánování jejich dosažení

Organizace musí stanovit cíle bezpečnosti informací, které musí:

- Být v souladu s politikou bezpečnosti informací.
- Být měřitelné (pokud je to možné).
- Zohlednit aplikovatelné požadavky bezpečnosti informací a zohlednit výsledky z hodnocení rizik a jejich ošetření.
- Být aktualizované, pokud je to zapotřebí.

Organizace musí při plánování cílů určit:

- Co má být provedeno.
- Které zdroje jsou potřebné.
- Kdo je odpovědný.
- Kdy má být splněno.
- Jak budou hodnoceny výsledky.

2.2.7 Podpora

Zdroje – organizace musí určit a poskytnout zdroje pro ISMS.

Kompetence – organizace musí určit potřebnou kompetenci osob, zajistit činnosti spojené se vzděláváním a připravováním, hodnotit účinnosti činností a udržovat důkazy o kompetenci.

Povědomí – osoby si musí uvědomovat politiku bezpečnosti informací, svůj přínos k efektivnosti ISMS, dopad nesouladu s požadavky ISMS.

Komunikace – organizace musí určit potřeby pro vnitřní a vnější komunikaci související s ISMS včetně toho, co komunikovat, kdy, komu, kdo bude komunikovat, procesy efektivní komunikace.

Dokumentované informace

Všeobecně – ISMS musí obsahovat dokumentované informace vyžadované normou a organizací pro účinný ISMS.

Vytváření a aktualizování – organizace musí určit identifikaci a popis, formát a médium, přezkoumání vhodnosti a dostatečnosti.

Řízení dokumentovaných informací – dokumentovaná informace musí být dostupná a vhodná pro použití a také přiměřeně chráněná. Z pohledu ISMS jsou vyžadovány následující dokumentované informace:

- Politika bezpečnosti informací.
- Analýza rizik.
- Prohlášení o aplikovatelnosti.
- Plán zvládání rizik.
- Cíle ISMS.
- Kompetence, výcvik.
- Program IS a výsledek hodnocení IS.
- Řízení neshod.
- Nápravná opatření.

2.2.8 Provoz

Plánování a řízení provozu

Organizace musí plánovat, zavést a řídit procesy potřebné pro ISMS a činnosti pro zvládání rizik, naplnění cílů a udržovat dokumentované informace v potřebném rozsahu. Musí řídit změny a přezkoumat dopady nechtěných změn.

Ohodnocení rizik bezpečnosti informací

Organizace musí v plánovaných intervalech (minimálně 1x za rok) a po významných změnách provést hodnocení rizik, a udržovat dokumentované informace o výsledcích hodnocení rizik.

Zvládání rizik bezpečnosti informací

Organizace musí zavést plán zvládání rizik a musí udržovat dokumentované informace o výsledcích zvládání rizik.

2.2.9 Vyhodnocení výkonnosti

Monitorování, měření, analýza a hodnocení

Organizace musí hodnotit výkonnost bezpečnosti informací a účinnost ISMS a musí určit:

- Jaké jsou potřeby monitorování a měření.

- Metody monitorování a měření.
- Kdy má být monitorování a měření prováděno.
- Kdo má monitorovat a měřit.
- Kdy výsledky analyzovat a hodnotit.
- Kdo má analyzovat a hodnotit.

Organizace musí udržovat dokumentované informace o výsledcích.

Interní audit

Organizace musí v plánovaných intervalech provádět interní audity pro získání informací o souladu s vlastními požadavky i požadavky normy a o účinnosti zavedení a údržby.

Organizace musí určit:

- Kritéria a rozsah každého auditu.
- Vybrat auditory a provádět audit objektivně a nestranně.
- Zajistit předání výsledků auditu.
- Udržovat dokumentované informace o programu auditů a výsledcích auditů.

Přezkoumání vedení

Vedení organizace musí v plánovaných intervalech přezkoumat ISMS z hlediska vhodnosti, přiměřenosti a účinnosti. Přezkoumání musí obsahovat:

- Stav činností z předchozího přezkoumání.
- Vnější a vnitřní změny ovlivňující ISMS.
- Zpětnou vazbu o výkonnosti bezpečnosti informací - neshody a nápravná opatření, výsledky měření a monitorování, výsledky auditů, naplnění cílů bezpečnosti informací.
- Zpětnou vazbu zainteresovaných stran (výstupy kontrol).
- Výsledky hodnocení rizik a stavu plánu zvládání rizik.
- Příležitosti pro neustálé zlepšování. Výstupy musí obsahovat rozhodnutí o zlepšování a změnách ISMS. Organizace musí udržovat dokumentované informace.

2.2.10 Zlepšování

Neshody a nápravná opatření

Když se objeví neshoda, musí organizace:

- Reagovat na neshody.
- Hodnotit.
- Zavést potřebná opatření.
- Přezkoumat účinnost nápravných opatření.
- Provést změny ISMS, když je to potřeba.

Nápravná opatření musí být přiměřená neshodě. Organizace musí udržovat dokumentované informace o příčinách neshod a o výsledcích nápravných opatření.

Neustálé zlepšování

Organizace musí neustále zlepšovat vhodnost, přiměřenost a účinnost ISMS. [21]

3 INFORMAČNÍ AKTIVA A JEJICH DRUHY

Aktivum – všechno, co má jakoukoliv hodnotu pro jednotlivce, organizaci nebo veřejnou správu. . [5] [6]

Informační aktivum – jedná se o veškerý nemovitý majetek podniku nebo organizace, který slouží k provozu a usnadnění práce a spolupráce v organizaci i mezi organizacemi. Jedná se o veškerá data a znalosti, která mají pro organizace ať už menší či větší význam. [5]

3.1 Základní rozdělení aktiv

Informačních aktiv je velké množství, proto není vůbec jednoduché je rozdělit do kategorií. Pro rozdělení do kategorií, slouží mnoho vzorů a dokumentů, které nám udávají podle čeho a jak aktiva rozdělit. Já jsem si vybrala rozdělení na hmotné a nehmotné, což lze považovat za úplně základní rozdělení a dále rozdělení podle ISMS, které je velmi podobné předchozímu rozdělení.

Rozdělení aktiv na hmotná a nehmotná

Hmotná aktiva

Do kategorie hmotných aktiv lze zařadit technické prostředky výpočetní techniky - modemy, počítače, další aktivní prvky počítačových sítí, tiskárny, kabelové rozvody a ostatní technická zařízení.

Nehmotná aktiva

a) Pracovní postupy – ty, které se využívají v organizace v oblasti IS/ICT.
b) Data – důležité pro rozvoj organizace, které si organizace vytvoří sama nebo je převezme.
c) Programové vybavení – operační systémy počítačů, programové vybavení potřebné pro provoz počítačových sítí, aplikační programové vybavení (textové editory, tabulkové kalkulátory…).
d) Služby – počítačové a komunikační služby, základní služby (zajištění světla, topení, klimatizace…). [6]

Rozdělení aktiv podle systému řízení bezpečnosti informací

Primární aktiva

Zejména nehmotná aktiva – informace, které organizace využívá, veškeré funkční procesy a aktivity organizace, znalosti a know-how, které mají pro ISMS nějaký význam (je potřeba nějakým způsobem zajistit jejich bezpečnost)

Sekundární aktiva

Zejména hmotná aktiva – vybavení komunikační prostředky, programové vybavení a také pracovníci, kteří se zapojují do chodu organizace a mají podíl na jejím organizačním uspořádání, prostory, které organizace využívá a v kterých funguje apod. [6]

4 INFORMAČNÍ HROZBY

Hrozba – jakákoliv příčina, která vznikne neúmyslně, kdy důsledkem je poškození nebo znehodnocení systému nebo organizace [5]

Bezpečnostní hrozba – možná příčina vzniku nežádoucí události, která může vést k poškození systému a aktiv, např. zničení, znehodnocení, nežádoucí zpřístupnění, nedostupnost služeb. [5]

4.1 Základní rozdělení hrozeb

Hrozby můžou vznikat z několika příčin. Základní rozdělení je na přírodní (zemětřesení, blesk) nebo zapříčiněné lidským faktorem (odposlech, chyba uživatele apod.). Další dělení hrozeb je na náhodné (vymazání souboru) a úmyslné (krádež). Z hlediska bezpečnosti je žádoucí, aby jak náhodné, tak úmyslné hrozby, byly identifikovány a měla by být odhadnuta jejich úroveň a pravděpodobnost.

Podle zdroje působení:

- Hrozby vnitřní vycházející ze samotného aktiva (např. výrobní vada).
- Hrozby vnější, jejichž zdroj je mimo vlastní aktivum.

Podle úmyslu:

- Náhodné hrozby (přírodní katastrofa, výpadek proudu).
- Neúmyslné hrozby (omylem vymazaný soubor).
- Úmyslné hrozby (úmyslné poškození, odcizení, síťový útok).

Podle původu:

- Přírodní hrozby (blesk, zemětřesení).
- Hrozby způsobené člověkem (odposlech, chyba uživatele).

Podle směrování na bezpečnostní atributy:

- Hrozby dostupnosti (požár).
- Hrozby integrity (chyba v databázové transakci).
- Hrozby důvěrnosti (krádež notebooku).

Podle toho, na jaký druh aktiva působí:

- Hrozby pro hardware.

- Hrozby pro síť.
- Hrozby pro operační systém.
- Hrozby pro aplikace.
- Hrozby pro informace.
- Hrozby pro uživatele.

Podle motivace útočníka:

- Hrozby za účelem získání finančního prospěchu.
- Hrozby za účelem získání konkurenční převahy.
- Hrozby za účelem dokázání svých schopností.
- Hrozby za účelem odplaty.
- Hrozby z důvodu neplnění povinností. [22]

Tabulka 1: Rozdělení hrozeb - příklady *[Zdroj: 22]*

Lidské hrozby		**Hrozby přírodní**
Úmyslné	**Neúmyslné**	
odposlech	chyba uživatele	blesk
krádež	vymazání	povodeň
hacking	fyzická nehoda	požár

Hacking - často se používá ve smyslu hesla ***Crack***. Druhé obvyklé použití je ve smyslu podařeného, neobvyklého, nápaditého, či rychlého vyřešení programátorského či administrátorského problému. [5]

4.2 Posouzení hrozeb

Posouzení hrozeb provádíme vždy v závislosti na následujících otázkách:

- **Ztráta důvěrnosti** – může vést např. ke ztrátě důvěry vůči zákazníkům, právní odpovědnosti, ohrožení osobní bezpečnosti nebo finanční ztrátě.
- **Ztráta integrity** – může vést např. k přijetí nesprávných rozhodnutí, rozpadu funkčnosti organizace.
- **Ztráta dostupnosti** – může vést např. k neschopnosti vykonávat kritické činnosti organizace.
- **Ztráta individuální odpovědnosti** – může vést např. k podvodu, špionáži, krádeži

- **Ztráta autentičnosti** – může vést např. k použití neplatných dat, která vedou k neplatným výsledkům.
- **Ztráta spolehlivosti** – může vést např. k nespolehlivým dodavatelům, demotivace zaměstnanců. [23]

Důvěrnost – vlastnost, informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům.

Integrita – vlastnost přesnosti a úplnosti.

Dostupnost – vlastnost přístupnosti a použitelnosti na žádost oprávněné entity. [5]

4.3 Nejčastější hrozby

Standardizovaný seznam možných hrozeb pro informační systém čítá několik mnoho položek, zde je však uvedeno jen několik, včetně popisu.

Selhání dodávky energie

Selhání dodávky energie může způsobit problémy z hlediska integrity a následně může způsobit i další poruchy (selhání HW apod.). Selhání dodávky se samozřejmě netýká jen vlastního HW, ale také klimatizace, celého síťového prostředí, zálohování a podobně.

Škodlivý software

Škodlivý software může být použit ke zmaření autentizace a všech souvisejících služeb a bezpečnostních funkcí. Ve svém důsledku může vést ke ztrátě dostupnosti, jestliže jsou např. data nebo soubory zničeny osobou, která získala neautorizovaný přístup pomocí škodlivého programového kódu, nebo vlastním škodlivým programovým kódem.

Selhání hardwaru

Technické poruchy, např. v síti, mohou zničit dostupnost informace, která je uchovávána nebo zpracovávána v této síti. Mezi nejčastější příčiny selhání hardwaru patří např. nedostatečná údržba, nejasné postupy při údržbě HW, nevhodné prostředí umístění HW (vlhkost, prach, výkyvy teploty apod.)

Selhání komunikačních služeb

Chyby a poruchy komunikačních zařízení a služeb ohrožují dostupnost informací přenášených prostřednictvím těchto služeb. V závislosti na příčině chyby nebo poruchy.[8]

5 CÍLE A ZVOLENÉ METODY ZPRACOVÁNÍ

Tato kapitola obsahuje popis cíle práce, a jaké odborné metody byly použity při zpracování bakalářské práce.

5.1 Cíle bakalářské práce

Cílem teoretické části bylo seznámení se základními pojmy v oblasti informačních technologií, co to vůbec informačních technologie jsou a jak se rozdělují. Vymezení základních druhů aktiv a hrozeb podle různých kritérií a skupin, které můžou ohrožovat informační technologie. V poslední části je práce zaměřena na normy a předpisy, které se velmi dobře věnují oblasti problematiky informačních technologií a ovlivňují jejich fungování, kvalitu a zabezpečení.

Cílem praktické části je identifikace, ohodnocení a následné aktualizování číselníku informačních aktiv a hrozeb, který se nachází v programu Riskan. Aktualizovaný seznam, bude sloužit k následné výuce a budou s ním moci dále studenti pracovat při výuce informatiky a dalších informačních předmětů.

5.2 Metody použité při zpracování bakalářské práci

Při psaní bakalářské práce byla použita metoda literární rešerše. Cílem literární rešerše bylo sesbírání informací a seznámení se základními pojmy z oblasti informačních technologií. Dále byly využity metody:

- Deskripce – slouží k uspořádání sesbíraných informací a utřídění si jich dle svých potřeb.
- Analýza rizik – slouží k vyhodnocení nebezpečí, která mohou nastat. Tato metoda je využita v praktické části.
- Syntéza – myšlenkové spojení získaných poznatků. Slouží k vzájemnému pochopení souvislostí.
- Analogie – srovnávání. Jedná se o metodu, která srovnává dříve získané údaje s nově získanými údaji.

Také jsem využívala učebnu IT na Fakultě logistiky a krizového řízení v Uherském Hradišti, kde jsem zapracovala své sesbírané informace do SW programu Riskan.

II. PRAKTICKÁ ČÁST

6 AKTIVA A HROZBY PRO POTŘEBU ANALÝZY ZA VYUŽITÍ NÁSTROJE RISKAN

Kapitola obsahuje tabulky, ve kterých jsou původní aktiva a hrozby a následně nová aktiva a hrozby.

6.1 Současný stav

V následující tabulce je dosavadní přehled informačních aktiv a hrozeb, která se nachází v programu Riskan a slouží jako základ pro aktualizaci.

Tabulka 2 - Přehled aktiv v programu Riskan *[Zdroj: vlastní]*

<table>
<tr><th colspan="14">AKTIVA</th></tr>
<tr><th colspan="4">Informace</th><th colspan="10">Osoby</th></tr>
<tr><td>Strategické informace</td><td>Osobní údaje</td><td>Obchodní tajemství</td><td>Ostatní citlivé informace</td><td>Vrcholové vedení společnosti</td><td>Vedoucí pracovníci</td><td>Bezpečnostní ředitel</td><td>Architekt bezpečnosti</td><td>Bezpečnostní pracovníci</td><td>Administrátoři OS</td><td>Administrátoři aplikací</td><td>Administrátoři komunikací</td><td>Vývojový pracovníci</td><td>Uživatelé IS</td></tr>
<tr><th colspan="8">Prostory a objekty</th><th colspan="6">Technická zařízení</th></tr>
<tr><td>Hranice celku</td><td>Pro umístění serveru</td><td>S komunikačními prvky</td><td>Pro ukládání dat a kopií</td><td>Sklady náhradních dílů a spotřebního materiálu</td><td>Archivy</td><td>Pro vývoj</td><td>Pro administrátory</td><td>Pro uživatele IS</td><td>Kancelářská technika</td><td>UPS</td><td>Náhradní zdroj</td><td>Silová kabeláž</td><td>Skartovací zařízení</td></tr>
</table>

HW										**Datová média**			
Servery			Koncové stanice	Mob. výpočetní prostředky	Tiskárny	Kopírky	Skenery	Zálohovací zařízení	Kryptografické moduly	Záložní média	Archivní média	Instalační médie	
Aplikační	Poštovní	Veřejný web											
Komunikační zařízení a linky													
Komunikační linky externí - modemové spojení	Komunikační linky externí - telefonní	Komunikační linky externí - připojení k Internetu	Internet	LAN	Kabelář datová	Aktivní síťové prvky	Datové rozvaděče	Wifi zařízení	Fire Wall	Modemy	Telefony	Faxy	Záznamníky
SW													
OS - Windows	OS - Unix, Linux	Databáze - Oracle, DB2	Databáze - SQL	Kancelářský SW	Poštovní SW	Komunikační SW	Antivirový SW	IDS, IPS	Kryptografické moduly	SW pro management sítí	Zálohovací SW	Podpůrný SW	Vyvíjený SW
Aplikace		**Vývojové prostředky**					**Zásoby**						
Elektronická pošta	Veřejný web	HW	SW	Databáze	Komunikační média	Testovací data	Náhradní díly	Spotřební materiál	Vyřazené datové nosič	Externí disk			

Bezpečnost - řízení, dokumentace, záznamy											
Řízení bezpečnosti (ISMS)	Bezpečnostní politika	Analýza rizik	Prohlášení o aplikovatelnosti	Plán zvládání rizik	Havarijní plán	Evidence bezpečnostních incidentů	Dokumentace bezpečnostních systémů	Dokumentace bezpečnostní správců	Bezpečnostní směrnice pro uživatele	Auditní zprávy	Auditní logy, žurnály
Ostatní											
Šifrovací materiál	Klíče od místností, trezorů	Přístupová hesla a kódy administrátorů	Přístupová hesla a kódy běžných pracovníků	Autentizační předměty	Papírová dokumentace	Systémová (administrátorská) dokumentace	Programátorská dokumentace	Provozní dokumentace	Uživatelská dokumentace		

Tabulka 3 - Přehled hrozeb v programu Riskan *[Zdroj: vlastní]*

HROZBY													
Lidské neúmyslné – selhání													
Ztráta důvěrnosti/integrity dat v důsledku chyby uživatele IT	Zničení počítačového vybavení nebo dat v důsledku nedbalosti	Nedodržení bezpečnostních opatření	Nepřípustné spojení kabelů	Neúmyslné poškození kabeláže	Škody způsobené personálem pro úklid a lidmi zvenčí	Nevhodné užívání IT systému	Nesprávná správa IT systému	Chybná administrace přístupových práv k IT systému, aplikacím a datům	Nesprávná výměna uživatelů PC	Neúmyslná manipulace s daty	Nesprávná/žádná časová synchronizace v síti	Nesprávná konfigurace aktivních časových komponentů	Nesprávná/nehodná členění sítě
Nestrukturovaná organizace dat	Porušení zákonných podmínek pro používání šifrovacích procedur	Nesprávné používání šifrovacích modulů	Nevhodná konfigurace systému správy sítě	Zablokování serveru během provozu	Neproduktivní surfování po Internetu	Nesprávná administrace systému pro vzdálený přístup	Nevhodné používání autentizačních služeb pro vzdálených přístup	Nezabezpečená konfigurace klientů systému pro vzdálený přístup	Nedbalost při zacházení s informacemi	Nevhodné zacházení s hesly			

Lidské neúmyslné - organizační nedostatky													
Nedostatečná/nevhodná bezpečnostní pravidla	Nedostatečná bezpečnostní povědomí	Chybějící nebo nedostatečný bezpečnostní management IT	Ztráta/úbytek zaměstnanců	Nedostatečný/chybějící školení bezpečnosti	Nedostatečné monitorování bezpečnostních oprávnění IT	Chybějící/nedostatečné monitorování činnosti uživatelů	Nedostatečná admin. přístupových práv	Porušení autorských práv	Chybějící klasifikace aktiv	Nedostatečné schvalování nového vybavení IT	Nekontrolované využívání zdrojů	Používání neregistrovaných prvků v IT systému	Neautorizované stahování a užívání SW
Nedostatečné přizpůsobení používání IT novým změním	Nedostatečná správa klíčů pro šifrování	Nedostatečné/neodpovídající zásoby spotřeb. mat	Nedostatečná organizace výměny uživatelů	Nedostatečné hodnocení auditních záznamů	Umístění serveru v nechráněném prostoru	Nevhodná práce s nosiči dat a dokumenty při práci doma	Nedostatečné přezkoumání bez. politiky s provozem	Chybějící/nedostatečné havarijní plány	Nedostatečná procedura pro příjem pracovníků	Neautorizované zpracování osobních dat	Neexistující dohoda o důvěrnosti s třetími stranami		
Technické selhání													
Přerušení dodávky elektrické energie	Výpadek interních rozvodů a zdrojů	Kolísání napětí - přepětí, podpětí	Vadné nosiče dat	Bezpečnostní díry v SW	Otevřená hesla na síti při přihlašování	Ztráta uložených dat	Nedostatky a chyby SW	Chyba v databázi	Ztráta dat v databázi	Ztráta dat vlivem malého úl. prostoru	Ztráta integrity/konzistence databází	Chybná funkce síťových komponentů	Poruch a odeslání zprávy

Nekvalitní / chybějící autentizace	Chyba šifrovacího modulu	Nedostatečně bezpečné šifrovací algoritmy	Chyby v zašifrovaných datech	Chybějící časová totožnost v e-mailech	Porucha komponentů systémů pro správu sítě nebo systému	Chyby v koncepci SW	Nevhodné provozní prostředí klienta	Nedokumentované provozní prostředí klienta pro vzdálený přístup	Překročení kapacity paměťových médií	Porušení integrity databáze	Nechráněné přenosy dat (LAN, WAN, e-mail)	Poruchy /chyby/ nedostatečná kapacita přenosu dat	Ztráta služeb přenosu dat
Lidské úmyslné – poškození													
Záměrná manipulace nebo destrukce systému IT	Záměrná manipulace s daty nebo softwarem	Neoprávněný vstup do budovy	krádež	vandalismus	útok	Odposlech v síti LAN/ WAN	Manipulace s dat. linkami	Neoprávněné/neautorizované užití systému IT	Zneužití portů pro vzdálenou správu	Odposlech telefonních hovorů nebo přenosu dat	Zvědavý zaměstnanci	Hrozby představované vlastními zaměstnanci při údržbě, správě	Hrozby představované cizími zaměstnanci pro údržbu úklid

Zkoušení přístupových hesel	Zneužití uživatelských práv	Zneužití administrativních práv	Trojské koně	Počítačové viry, makroviry	Maškaráda (předstírání identity)	Nepřevzetí/odmítnutí zprávy	Odmítnutí služeb - DOS	Neoprávněné pořízení kopie dat, média při transportu	IP/DNS/ Web spoofing	Zneužití protokolu pro směřování dat5 Působení vyšší moci

Přírodní události									
Bouře, hurikán	Blesk	Oheň	Voda - záplavy, povodeň	Voda - havárie rozvodů vody	Vzplanutí kabeláže	Nepřípustná teplota	Nepřípustná vlhkost	Prach, špína	Ztráta dat působením intenzivního magnetického pole

6.2 Aktuální aktiva a hrozby

V následujících tabulkách můžeme vidět návrh nových aktiv a hrozeb. Aktiva a hrozby jsou rozděleny do jiných kategorií, než původně byly. Budou sloužit k aktualizaci číselníků v programu Riskan. Pro sbírání těchto dat, byly využity internetové stránky, české i zahraniční.

Tabulka 4 - Přehled nových aktiv *[Zdroj: vlastní]*

AKTIVA										
Hmotná					**Nehmotná**					
Komunikační zařízení	**Hardware**	**Software**	**Záznamová média**	**Další technické vybavení**	**Ostatní**	**Bezpečnostní prvky**	**Informace**	**Prostory**	**Textové, tabulkové a komunikační prostředky**	**Personál**
Internet	Tiskárna	Kancelářský	Flash disky	Náhradní zdroj	Šifrovací materiál	ISMS	Strategické informace	Archivy	Datová schránka	Vrcholové vedení
LAN	Kopírka	Poštovní	Externí disky	Skart	uživatelské dokumenty	Bezpečnostní politika	Osobní údaje	Vývojárna	e-mail	Ředitel bezpečnosti
Datová kabeláž	Skener	Komunikační	CD	UPS	Provozní dokumenty	Analýza rizik	Obchodní tajemství	Sklady náhradních dílů	Word	Bezpečnostní pracovníci
Wifi zařízení	Monitor	Antivirový	DVD	Náhradní díly	programátorská dokumentace	Plán zvládání rizik	Ost. citlivé údaje	Serverovny	Excel	administrátoři
FireWall	Klávesnice	IDP, IPS	Paměťové karty	Spotřební materiál	Systémová dokumentace	Havarijní plán	GDPR	Uživatelské místnosti	Open office	Vývojový pracovníci

Modemy	Myš	OS - Windows			Papírová dokumentace	Audit			Outlook	Uživatelé
Telefony	El. zdroj	OS - Unix, Linex			Přístupová hesla	Dokumentace bezpečnosti				
Záznamníky	Základní deska	Zálohovací				Bezpečnostní směrnice				
Datové rozvaděče	Operační paměť	Podpůrný								
	Grafická karta	Vyvíjený								
	Zvuková karta	Síť PPP								
	Síťová karta	Síť VPN								
	Pevný disk	Síť IPsec								
		DNSSEC doména								

Tabulka 5 - Přehled nových hrozeb *[Zdroj: vlastní]*

HROZBY				
Technické a technologické	**Přírodní**	**Způsobené lidským faktorem**		
		Úmyslné		**Neúmyslné**
		z vnějšího prostředí	Z vnitřního prostředí	
Přerušení dodávky el. energie	Povodně	Odposlech	Vandalismus	Neoprávněné aktualizace
Výpadek interní sítě	Bouře	Krádež	Úmyslná manipulace s daty	Jednoduchá, lehce napadnutelná hesla
Špatné napětí sítě	Hurikán	Neoprávněný vstup do budovy	Neoprávněné užití systému IT	Zavádění cloudu
Poškození nosiče dat	Blesk	Útok, napadení DNS serveru	Zvědaví zaměstnanci	Nešifrování dat
Špatné zabezpečení SW	Oheň	Cizí osoby (uklízečka s úklidové služby)	Zneužiti oprávnění	BYOD
Uložená hesla při přihlašování	Prach, špína	Falšování PDF podpisů		BYOPC
Porucha odeslání zprávy	Vlhkost	Cílený phishing		Minimální bezpečnostní povědomí
Chyba přenosu dat	Špatná teplota	DMA útoky		Nedostatečná kvalifikace zaměstnanců
Nechráněné přenosy		DDOS útoky		Malý počet zaměstnanců
Nevyhovující provozní prostředí		DOS útoky		Porušení autorských práv
Nedostatečné zabezpečení		Šifrování SSL		Nedostatečný/chybějící bezpečnostní management
Chyba šifrovacího modulu		Vyděračský SW		Neoprávněné stahování a užívání SW
Chyba v databázi		Útoky na IoT		Špatné umístění serveru (nevyhovující prostředí)
		WannaCry		Malé zásoby spotřebního materiálu
		Kybergrooming		Špatná správa klíčů pro šifrování
		Ransomware		Nepřizpůsobení IT modernizaci

		Viry (trojský kůň)		Porušení předpisů
		Darring		Poškození kabeláže
				Poškození v důsledku nedbalosti
				Malé zabezpečení pro vzdálený přístup
				Neproduktivní surfování po Internetu

7 AKTUALIZACE ČÍSELNÍKŮ V NÁSTROJI RISKAN

SW nástroj Riskan je určen jak pro orientační, tak i detailní podporu tvorby analýzy rizik. V rámci samotného procesu analýzy rizik pracuje SW Riskan s tzv. profily ve vztahu k analyzovanému objektu (předmětu). V každém profilu jsou hodnoceny tři základní bezpečnostní prvky: aktivum, hrozba a zranitelnost, s možností hodnotit zranitelnost jednotlivých aktiv vůči jednotlivým hrozbám. Základem pro zpracování analýzy rizik představuje přehled aktiv a hrozeb hodnoceného subjektu, kde aktiva a hrozby podobného charakteru mohou být sdruženy do jednotlivých skupin. Při hodnocení lze tedy pracovat jak na úrovni celých skupin, tak na úrovni podskupin až jednotlivých prvků těchto uvedených skupin. Hodnocení probíhá podle předem nadefinované stupnice hodnot pro aktiva, hrozby a zranitelnost.

Nástroj podporuje výpočet rizika pro každou dvojici aktivum x hrozba na všech úrovních skupin. Při jakékoliv změně hodnot parametrů aktiv, hrozeb nebo zranitelnosti dochází k automatickému přepočtení výsledných rizik, takže je možné provádět simulace dopadů navrhovaných protiopatření nebo simulace dopadů při změně úrovní hrozeb.

SW Riskan umožňuje určit si až tři úrovně výsledného rizika pro roztřídění do kategorií podle stupně rizika (např. riziko nízké, střední, vysoké). Nástroj podporuje i barevné rozlišení výsledných rizik včetně přehledného grafického zobrazení. Nedílnou součástí interpretace výsledků je i zpracování ve formě jednotlivých grafů.

Základní algoritmus pro rychlé zhodnocení rizik v SW nástroji Riskan zahrnuje:

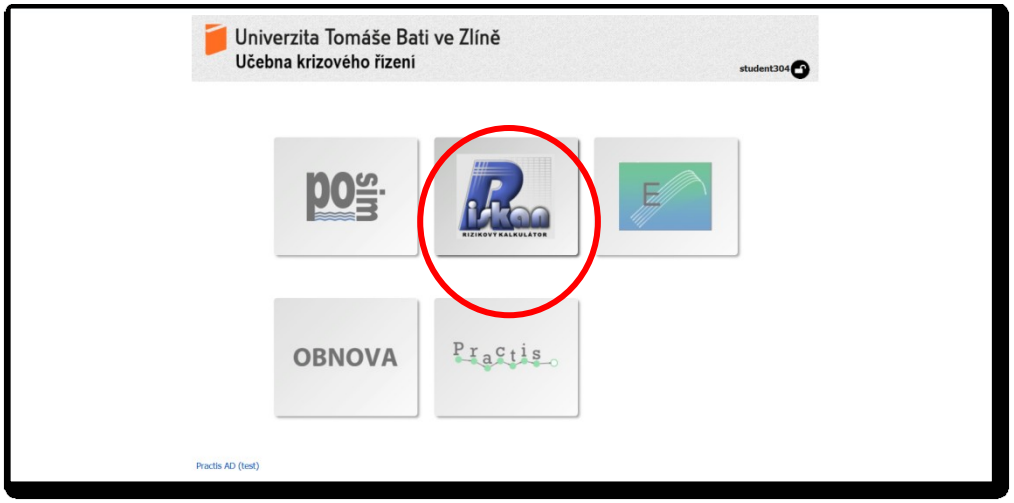
- Identifikace aktiv a jejich hodnocení.
- Identifikace hrozeb a ohodnocení jejich pravděpodobnosti.
- Ohodnocení zranitelnosti aktiv jednotlivými hrozbami.
- Výpočet výsledného rizika pro každou dvojici aktivum-hrozba.
- Roztřídění výsledných rizik na nízká, střední a vysoká dle stanovených kritérií.[24]

7.1 Postup aktualizace číselníků v nástroji Riskan

Následující kapitola popisuje postup při provádění aktualizace číselníků v SW programu Riskan.

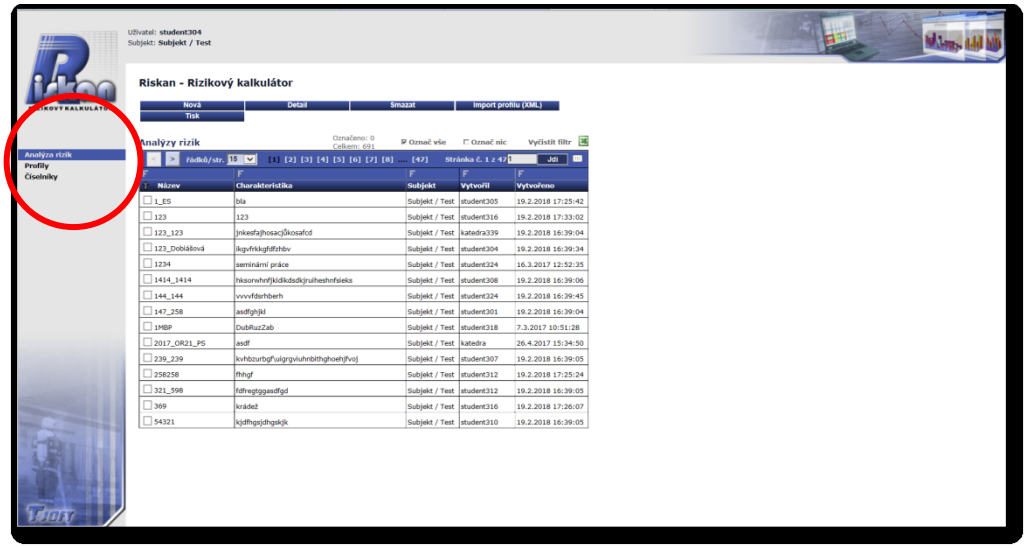
7.1.1 Přihlášení do programu Riskan.

Na obrázku č. 4 můžeme vidět úvodní stránku při spuštění internetových stránek, pomocí které se přihlásíme do programu Riskan.



Obrázek 4 - Úvodní stránka *[Zdroj: Vlastní]*

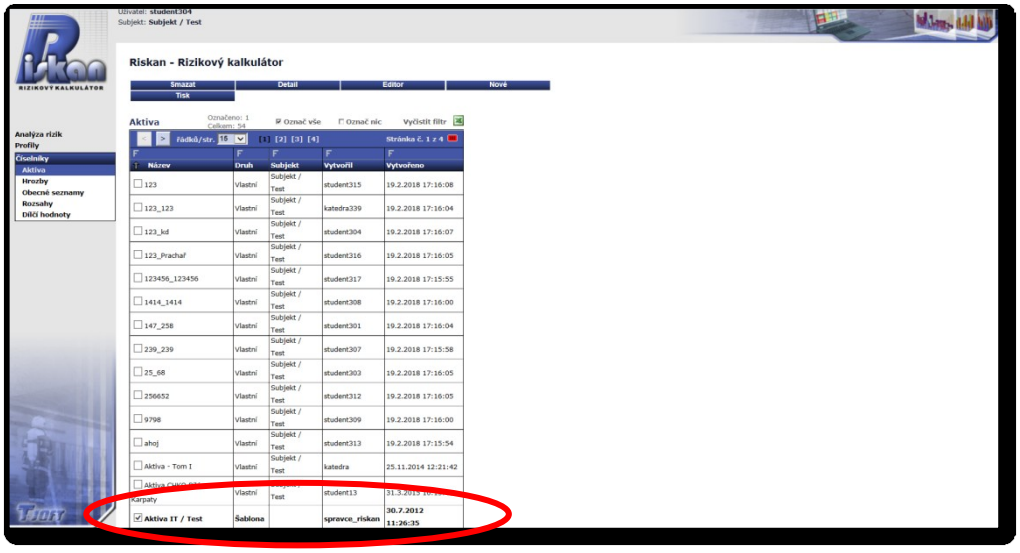
Obrázek č. 5 znázorňuje úvodní stránku, která se nám zobrazí po přihlášení se do programu Riskan. Na pravé straně nám nabízí kategorie, z kterých si můžeme vybrat podle toho, co potřebujeme udělat. Jedná se o kategorie: analýzy rizik, profily nebo číselníky.



Obrázek 5 - Výběr kategorie *[Zdroj: Vlastní]*

V mém případě jsem si nejprve musela jít do kategorie číselníky a najít si stávající aktiva a hrozby, které jsou v programu Riskan zapsaná.

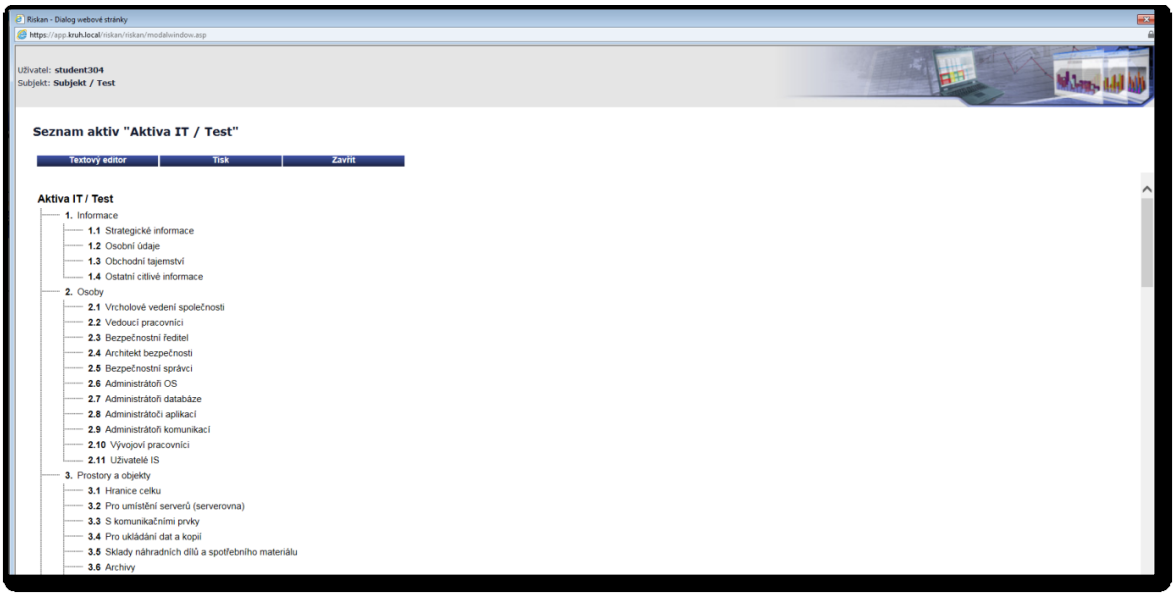
V kategorii aktiva jsem našla číselník z roku 2012, zadaný správcem jak můžeme vidět na obrázku číslo 6.



Obrázek 6 - Aktuální seznamy aktiv *[Zdroj: Vlastní]*

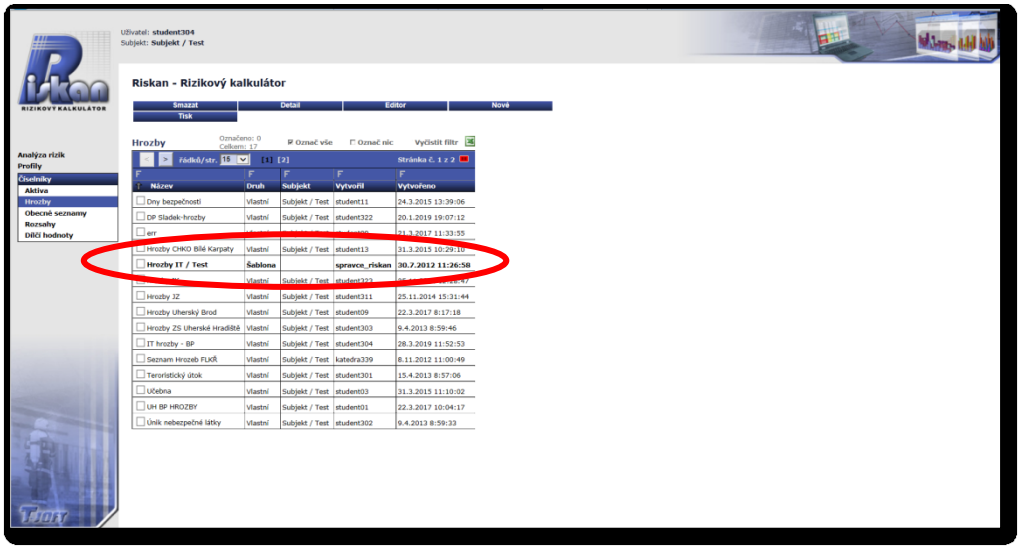
7.1.2 Seznam aktiv a hrozeb v Riskanu

Obrázek č. 7 zobrazuje číselník aktiv, který se zobrazí při otevření složky Aktiva IT / Test. Aktiv je v Riskan velké množství (tabulka č. 2 v předchozí kapitole), proto je zde pouze začátek číselníku.



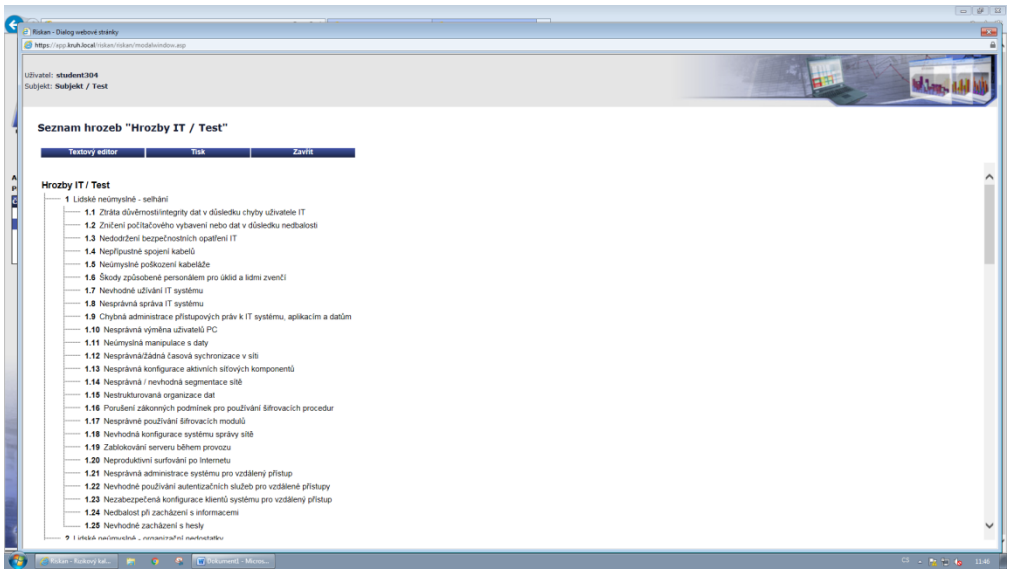
Obrázek 7 - Seznam aktiv *[Zdroj: Vlastní]*

Na obrázku č. 8 můžeme vidět složku Hrozby IT / Test, která obsahuje všechny hrozby, které byly zadané správcem v roce 2012.



Obrázek 8 - Aktuální seznamy hrozeb *[Zdroj: Vlastní]*

Obrázek č. 9 zobrazuje ukázku hrozeb v programu Riskan. Celý seznam hrozeb jsme viděli v předchozí kapitole v tabulce č. 3

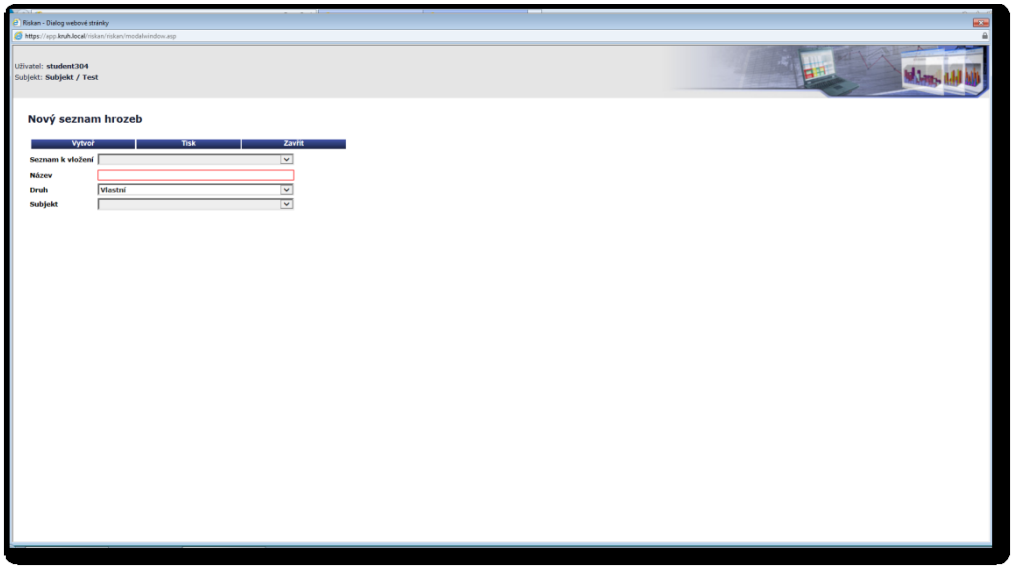


Obrázek 9 - Seznam hrozeb *[Zdroj: vlastní]*

7.1.3 Tvorba nového seznamu

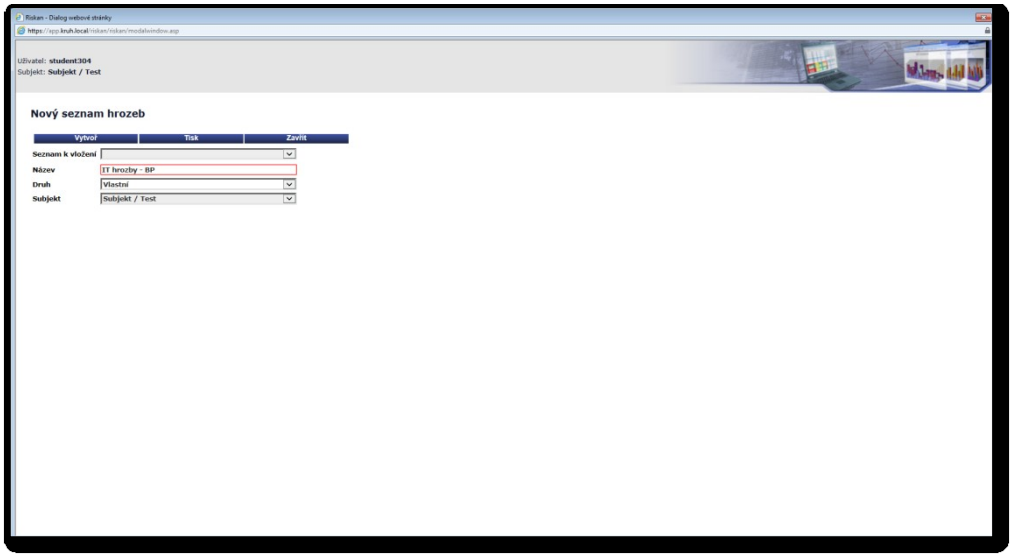
V následující kapitole se seznámíme s postupem, jak pracovat při tvorbě nových číselníků aktiv a hrozeb v programu Riskan.

Obrázek č. 10 nám zobrazuje úvodní stránku, kde si vytvoříme složku pro tvorbu číselníku, který bude obsahovat hrozby.



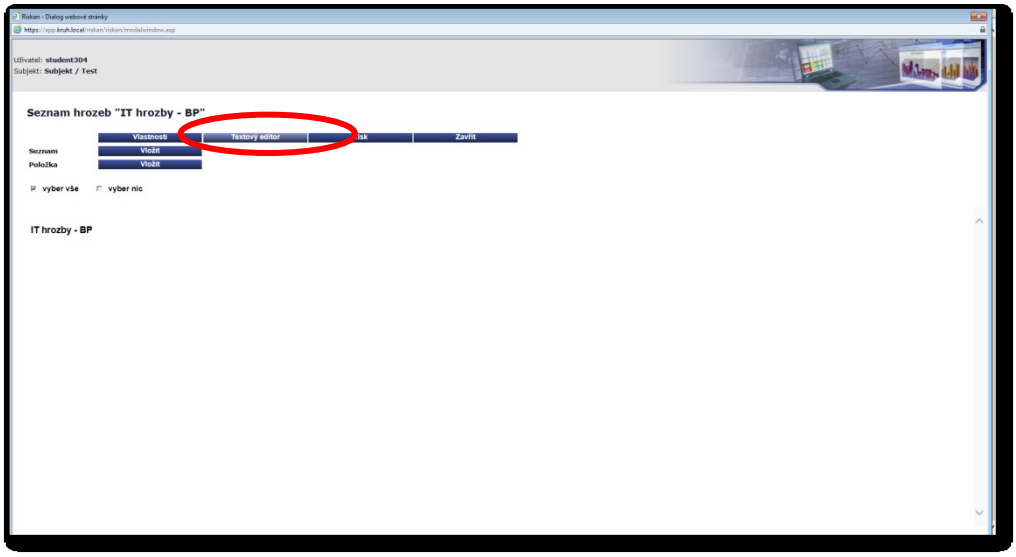
Obrázek 10 - Nový seznam hrozeb *[Zdroj: Vlastní]*

Při tvorbě nových číselníků, musíme vždy vyplnit název souboru, dále druh a subjekt. To můžeme vidět na obrázku č. 11.



Obrázek 11 - Nový seznam hrozeb *[Zdroj: Vlastní]*

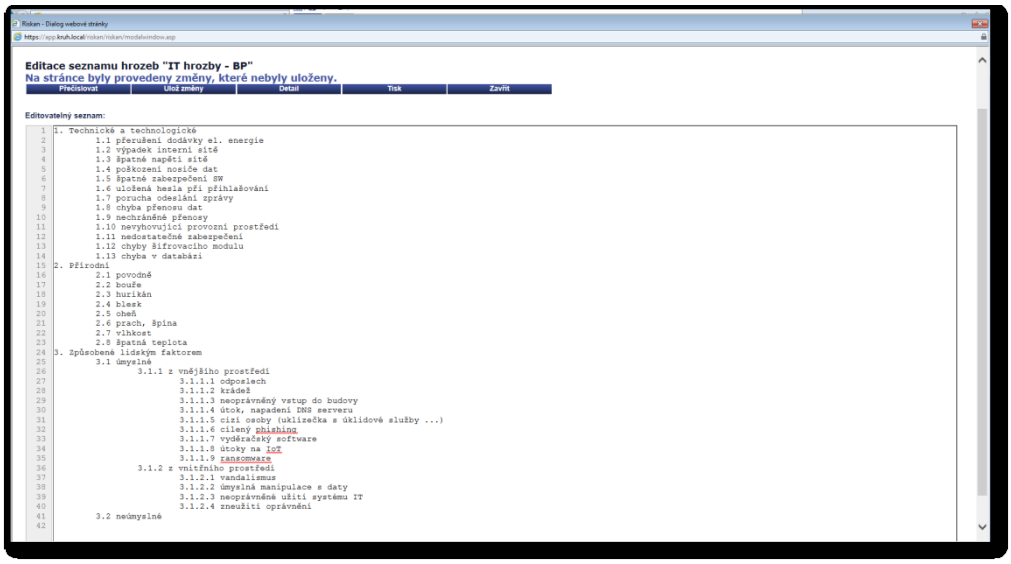
Po vytvoření názvu souboru se přesunujeme k samostatné tvorbě nového číselníku a zapisování aktiv a hrozeb do programu Riskan. Obrázek č. 12 ukazuje, že po vytvoření názvu musíme kliknout na textový editor, abychom mohli začít psát.



Obrázek 12 - Začátek psaní seznamu *[Zdroj: Vlastní]*

Po napsání všech hrozeb, které jsou uvedené v předchozí kapitole v tabulce č. 4. nám vznikne nový číselník, který bude sloužit pro tvorbu relevantní analýzy rizik k roku 2019.

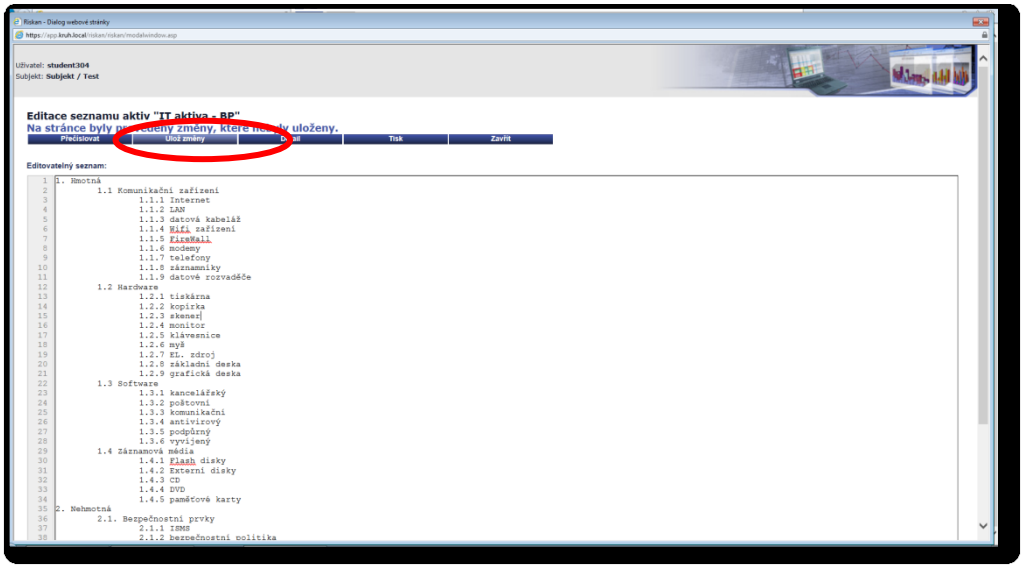
Obrázek č. 13 zobrazuje ukázku při psaní hrozeb do programu Riskan.



Obrázek 13 - Tvorba vlastního seznamu *[Zdroj: Vlastní]*

Obrázek č. 14 ukazuje pokračování při tvorbě nového číselníku. Při zapsání všech požadavků do číselníku, si všechny zapsané údaje zkontrolujeme a klikneme na ikonku "uložit změny". Dojde k uložení námi zapsaných dat a vytvoření nového číselníku hrozeb.

Úplně stejný postup použijeme při tvorbě nového číselníku aktiv. Vzorem pro zapisování nových údajů aktiv mi byla tabulka č. 3 v předchozí kapitole.



Obrázek 14 - Ukládání změn *[Zdroj: Vlastní]*

7.2 Aktualizace číselníků

V následující kapitole uvidíme porovnání starých a aktualizovaných číselníků v SW programu Riskan. Jedná se pouze o ukázku, prvních pár vybraných údajů z číselníků.

Na obrázku č. 15 jsou vyobrazená dočasná aktiva, která se nacházely v Riskan a byla vyexportovaná do Excelu.

	AKTIVA - CELKEM
1.	Informace
1.1	Strategické informace
1.2	Osobní údaje
1.3	Obchodní tajemství
1.4	Ostatní citlivé informace
2.	Osoby
2.1	Vrcholové vedení společnosti
2.2	Vedoucí pracovníci
2.3	Bezpečnostní ředitel
2.4	Architekt bezpečnosti
2.5	Bezpečnostní správci
2.6	Administrátoři OS
2.7	Administrátoři databáze
2.8	Administrátoči aplikací
2.9	Administrátoři komunikací
2.10	Vývojoví pracovníci
2.11	Uživatelé IS

Obrázek 15 - Aktiva *[Zdroj: vlastní]*

Na obrázku č. 16 vidíme nový číselník aktiv. Je také vygenerovaný z programu Riskan do Excelu, kde byla následně provedena analýza rizik.

	AKTIVA - CELKEM
1.	Hmotná aktiva
1.1.	Komunikační zařízení
1.1.1	Internet
1.1.2	LAN
1.1.3	Datová kabeláž
1.1.4	Wifi zařízení
1.1.5	FireWall
1.1.6	Modemy
1.1.7	Telefony
1.1.8	Záznamníky
1.1.9	Datové rozvaděče
1.2.	Hardware
1.2.1	Tiskárna
1.2.2	Kopírka
1.2.3	Skener
1.2.4	Monitor
1.2.5	Klávesnice

Obrázek 16 - Aktiva *[Zdroj: vlastní]*

Při porovnání obrázků můžeme hned na úvod vidět, že aktiva jsou rozdělená do jiných skupin a mají více podskupin.

Obrázek č. 17 ukazuje staré hrozby, před aktualizací seznamu.

	HROZBY - CELKEM
1	Lidské neúmyslné - selhání
1.1	Ztráta důvěrnosti/integrity dat v důsledku chyby uživatele IT
1.2	Zničení počítačového vybavení nebo dat v důsledku nedbalosti
1.3	Nedodržení bezpečnostních opatření IT
1.4	Nepřípustné spojení kabelů
1.5	Neúmyslné poškození kabeláže
1.6	Škody způsobené personálem pro úklid a lidmi zvenčí
1.7	Nevhodné užívání IT systému
1.8	Nesprávná správa IT systému
1.9	Chybná administrace přístupových práv k IT systému, aplikacím a datům
1.10	Nesprávná výměna uživatelů PC
1.11	Neúmyslná manipulace s daty
1.12	Nesprávná/žádná časová sychronizace v síti
1.13	Nesprávná konfigurace aktivních síťových komponentů
1.14	Nesprávná / nevhodná segmentace sítě
1.15	Nestrukturovaná organizace dat
1.16	Porušení zákonných podmínek pro používání šifrovacích procedur

Obrázek 17 - Hrozby *[Zdroj: vlastní]*

Na obrázku č. 18 už vidíme nový seznam hrozeb, aktualizovaný podle tabulky. Seznam hrozeb je vyexportovaný do Excelu, kde sloužil k provedení analýzy rizik.

HROZBY - CELKEM	
1.	Technické a technologické
1.1	Přerušení dodávky elektrické energie
1.2	Výpadek interní sítě
1.3	Špatné napětí sítě
1.4	Poškození nosiče dat
1.5	Špatné zabezpečení SW
1.6	Uložená hesla při přihlašování
1.7	Porucha odeslání zprávy
1.8	Chyba přenosu dat
1.9	Nechráněné přenosy
1.10	Nevyhovující provozní prostředí
1.11	Nedostatečné zabezpečení
1.12	Chyba šifrovacího zabezpečení
1.13	Chyba v databázi
2.	Přírodní
2.1	Povodně
2.2	Bouře

Obrázek 18 - Hrozby *[Zdroj: vlastní]*

Opět při porovnání ukázkových obrázků hrozeb, vidíme jiné rozdělení do skupin a podskupin.

7.3 Validace aktualizovaných číselníků

Kapitola validace aktualizovaných číselníků obsahuje názornou ukázku využití nových aktualizovaných číselníků v programu Riskan pro tvorbu analýzy rizik.

RISKAN RIZIKOVÝ KALKULÁTOR — T-SOFT

Generátor grafů | Export do XML

Hrozby		Pravděpodobnost	Aktiva	AKTIVA - CELKEM	1.	1.1.	1.1.1	1.1.2	1.1.3	1.1.4	1.1.5	1.1.6	1.1.7	1.1.8	1.1.9	1.2.	1.2.1	1.2.2	1.2.3	1.2.4	1.2.5	1.2.6	1.2.7	1.2.8	1.2.9	1.2.10	1.2.11	1.2.12	1.2.13	1.3
			Hodnoty aktiv	5	5	4	3	4	4	3	3	2	2	3	5	4	4	2	5	5	4	5	5	5	5	5	5	5	
				velmi vysoká	velmi vysoká	vysoká	vysoká	střední	vysoká	vysoká	střední	střední	nízká	nízká	střední	velmi vysoká	vysoká	vysoká	nízká	velmi vysoká	velmi vysoká	vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	velmi vysoká	
HROZBY - CELKEM		5	velmi vysoká	60	60	48	48	36	48	48	36	36	16	24	36	60	48	48	24	60	0	0	60	60	60	60	60	60	60	
1.	Technické a technologické	5	velmi vysoká	60	60	48	48	36	48	48	36	36	16	24	36	60	48	48	24	60	0	0	60	60	60	60	60	60	60	
1.1	Přerušení dodávky elektrické ener	4	vysoká	60	60	48	48	36	48	48	36	36	16	24	36	60	48	48	24	60	0	0	60	60	60	60	60	60	60	
1.2	Výpadek interní sítě	4	vysoká	40	40	36	0	0	0	0	0	0	0	0	36	40	0	0	0	0	0	0	40	40	40	40	40	40	40	
1.3	Špatné napětí sítě	3	střední	45	45	24	24	18	24	24	18	18	6	12	18	45	24	24	12	30	0	0	45	30	15	15	15	15	15	
1.4	Poškození nosiče dat	4	vysoká	60	60	0	0	0	0	0	0	0	0	0	0	60	0	0	0	0	0	0	0	40	40	40	40	40	60	
1.5	Špatné zabezpečení SW	3	střední	45	45	24	24	18	24	24	18	18	12	12	0	45	0	0	6	0	0	0	0	30	45	30	15	30	45	

Obrázek 19 - Analýza rizik *[Zdroj: vlastní]*

Na obrázku č. 19 vidíme provedenou analýzu rizik v programu Riskan. Nově zadané údaje do číselníků v programu Riskan, jsem vyexportovala do programu Excel. Následně jsem určila hodnoty aktiv, hrozeb a jejich pravděpodobnost zranitelnosti. Po zadání všech těchto údajů do tabulek se nám zobrazí barevně vybarvená políčka, která nám určují závažnost rizika. Zelená barva vyobrazuje nízké riziko, žlutá barva střední riziko a červená barva vysoké riziko.

ZÁVĚR

Cílem mé bakalářské práce v teoretické části bylo seznámit se základními právními dokumenty a předpisy, které se zabývají aktivy, hrozbami a hlavně informační bezpečností. Také jsem se musela seznámit se základními pojmy z oblasti informatiky, informační bezpečnosti, co všechno vlastně to jsou aktiva a co všechno je možné do skupiny aktiv zahrnout. V kapitole hrozeb jsem se zabývala tím, co to hrozba je, jaké jsou různé kategorie a příčiny vzniku hrozeb. Rozdělení hrozeb z různého hlediska, ať už jsou to hrozby, které vzniknou příčinou, která se dá předpovídat anebo hrozby, které vznikají lidským nebo jiným faktorem a nejsou úmyslné. Vznikají neopatrným nebo neprofesionálním zacházením s prostředky informačních technologií. Oblast informační bezpečnosti je velmi živé téma a je velmi složité vytvořit takové dokumenty a prostředky, aby byla zajištěná dostatečná bezpečnostní pravidla, která se budou dát využívat v delším časovém úseku a nebudou se muset neustále aktualizovat. V oblasti bezpečnosti se hlavně věnuji ČSN normě ISO/IEC 27001, která zajišťuje podmínky pro bezpečnosti informačních technologií. Také je zde uvedena problematika, která je velmi aktuální, a to problematika GDPR. Jedná se o zajištění ochrany osobních údajů a to ve všech možných směrech.

Hlavním cílem v praktické části bylo, vyhledání aktuálních aktiv a hrozeb v oblasti informačních technologií. Vyhledané informace si sesbírat a využít je pro další zpracování v programu Riskan. V programu Riskan, jsem našla původní číselníky, které byly z roku 2012. Číselníky je potřeba aktualizovat, protože oblast informatiky se neustále vyvíjí a technologie jdou dopředu mílovými kroky. Po mé asi půlroční práci, kdy jsem se věnovala intenzivnímu studování na různých internetových stránkách, jak českých tak i zahraničních, nových aktiv i hrozeb jsem si určila kategorie, do kterých jsem vyhledané a sesbírané informace rozdělila. Rozdělení jsem zvolila podle svých kritérií a kategorií, které jsem si sama určila, a vyhovovaly mi. Pokračovala jsem prací v programu Riskan, kde došlo k uplatnění sesbíraných informací a vložení je do číselníků. Zapsáním a zveřejněním mých informací se zaktualizovaly základní číselníky aktiv a hrozeb, které program obsahuje. Aktuální číselníky se mohou nyní využít při tvorbě analýzy rizik, která bude adekvátní k roku 2019.

SEZNAM POUŽITÉ LITERATURY

[1] BEZPALEC, Pavel. *Management ICT systémů. Publi cz:: Co je ICT - systém* [online]. b.r. [cit. 2019-02-27]. Dostupné z: https://publi.cz/books/242/01.html

[2] HROMADA, Martin, Petr HRŮZA, Josef KADERKA, Oldřich LUŇÁČEK, Miroslav NEČAS, Bohumil PTÁČEK, Leopold SKORUŠA a Richard SLOŽIL. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint, 2015. ISBN 978-80-87994-72-6.

[3] ČESKO. Zákon č. 181/2014 Sb.: Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů ČR*. 2014, ročník 2014, číslo 181. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

[4] KOLOUCH, Jan. *CyberCrime*. 1. vydání. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[5] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[6] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

[7] WIENER, Norbert. *CYBERNETICS or control and communication in the animal and the machine*. Second edition. Cambridge (Massachuttes), 1948. ISBN 0-262-73009-X.

[8] TŮMA, František. *Kybernetika*. 8. vyd. Plzeň: Západočeská univerzita v Plzni, 2010. ISBN 978-80-7043-945-6.

[9] JUDIN, Pavel, ed. a Mark ROZENTAL', ed. *Kratkij filosofskij slovar'*. Izd. 4., dopolnennoje i ispravlennoje. Moskva: Gos. Izd. Političeskoj lit., 1955.

[10] *Historie výpočetní techniky v československu* [online]. b.r. [cit. 2018-11-28]. Dostupné z: https://www.historiepocitacu.cz/pocatky-kybernetiky-v-csr.html

[11] *Národní úřad pro kybernetickou a informační bezpečnost* [online]. b.r. [cit. 2018-12-05]. Dostupné z: https://www.govcert.cz/cs/

[12] *Managementmania: dostupnost* [online]. b.r. [cit. 2019-02-23]. Dostupné z: https://managementmania.com/cs/dostupnost-availability

[13] *Managementmania: Integrita* [online]. b.r. [cit. 2019-02-23]. Dostupné z: https://managementmania.com/cs/celistvost-integrity

[14] *Managementmania: důvěrnost* [online]. b.r. [cit. 2019-02-23]. Dostupné z: https://managementmania.com/cs/duvernost-confidentiality

[15] *Clever and Smart* [online]. b.r. [cit. 2019-02-03]. Dostupné z: https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/

[16] ČANDÍK, Marek. *Základy informační bezpečnosti*. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-731-8218-1.

[17] *Systém online* [online]. b.r. [cit. 2019-02-03]. Dostupné z: http://m.systemonline.cz/it-security/bezpecnost-informaci-se-netyka-jen-it-firem-1.htm

[18] *Obecné nařízení o ochraně osobních údajů prakticky* [online]. b.r. [cit. 2019-02-03]. Dostupné z: https://www.gdpr.cz/gdpr/

[19] *Úřad pro ochranu osobních údajů* [online]. b.r. [cit. 2019-02-03]. Dostupné z: https://www.uoou.cz/

[20] *Info-iso.cz: oborový internetový portál* [online]. b.r. [cit. 2019-02-17]. Dostupné z: http://www.info-iso.cz/iso-27001/iso-27001-zakladni-informace

[21] *ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky- Systémy řízení bezpečnosti- Požadavky*. b.r.

[22] *KYBEZ: Platforma kybernetické bezpečnosti* [online]. b.r. [cit. 2018-11-18]. Dostupné z: https://www.kybez.cz/bezpecnost/pred-cim-chranit

[23] *Bezpečnost v kostce* [online]. b.r. [cit. 2018-12-06]. Dostupné z: http://www.chrantesidata.cz/cs/art/1153-dil-6/

[24] *RISKAN: uživatelský manuál*. Verze 2.0. Praha: K-SOFT s. r. o., 2012.

[25] NEZMAR, Luděk, *Zákon o kybernetické bezpečnosti pro organizace - Implementace nových povinností do praxe*. Grada, 2018. ISBN 978-80-271-0899-2.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incedent Response Team
ČR	Česká republika
EU	Evropská unie
GDPR	General Data Protection Regulation - Obecné nařízení o ochraně osobních údajů
HW	Hardware
ICT	Information and Comunication Technologies - Informační a komunikačních technologie
IS	Informační systém
ISMS	Systém řízení bezpečnosti informací
IT	Informační technologie
KII	Kritická informační infrastruktura
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
ÚOOÚ	Úřad pro ochranu osobních údajů
VIS	Veřejná informační služba

SEZNAM OBRÁZKŮ

SEZNAM TABULEK