Návrh algoritmu pro stanovení pojistné hodnoty z pohledu kybernetické bezpečnosti

Ing. Lukáš Pavlík, Ph.D.

Teze disertační práce

Univerzita Tomáše Bati ve Zlíně

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Teze disertační práce

Návrh algoritmu pro stanovení pojistné hodnoty z pohledu kybernetické bezpečnosti

Design of Algorithm for the Determination of Insurance Value from the Perspective of Cyber Security

Autor: **Ing. Lukáš Pavlík, Ph.D.**

Studijní program: Inženýrská informatika, P3902
Studijní obor: Inženýrská informatika, 3902V023

Školitel: doc. Ing. Luděk Lukáš, CSc.

Oponenti: prof. Ing. Zdeněk Dvořák, PhD.
doc. Ing. Petr Hrůza, Ph.D.
prof. Mgr. Roman Jašek, Ph.D.

Zlín, září 2019

Vydala **Univerzita Tomáše Bati ve Zlíně** v edici **Doctoral Thesis Summary.**
Publikace byla vydána v roce 2019

Klíčová slova: *riziko, pojistná hodnota, hrozba, scénář, informační systém, ohrožený prvek, kybernetický incident.*

Key words: *risk, insurance value, threat, scenario, information system, endangered element, cyber incident.*

Plná verze disertační práce je dostupná v Knihovně UTB ve Zlíně.

ISBN 978-80-7454-863-5

ABSTRAKT

Disertační práce je zaměřena na problematiku informační bezpečnosti z pohledu pojištění proti kybernetickým hrozbám. Hlavní částí práce je návrh algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví a jeho následné ověření. Navržený algoritmus je založen na principu ocenění identifikovaných ohrožených prvků organizace a analýzy vybraných scénářů kybernetických hrozeb, včetně určení nejzávažnějšího scénáře. Výstupem tohoto algoritmu je stanovení finančních dopadů na vybrané ohrožené prvky organizace, které mohou být použity pro výpočet pojistné hodnoty. Vyjádření potenciálních dopadů kybernetických hrozeb je také založeno na analýze informačního prostředí organizace, statistických ukazatelích a pravděpodobnostních modelech.

ABSTRACT

The thesis is focused on the issue of information security from the perspective of insurance against cyber threats. The main part of the thesis is a proposal of an algorithm for determining the insurance value resulting from the impact of selected cyber threats on the organization from the perspective of insurance and its subsequent verification. The proposed algorithm is based on the valuation principle of identified vulnerable elements of the organization and analysis of selected cyber threat scenarios, including determining the most serious scenario. The output of this algorithm is to determine the financial impact on selected vulnerable elements of the organization that can be used to calculate the insurance value. The expression of potential impacts of cyber threats is also based on an analysis of the organization's information environment, statistical indicators, and probabilistic models.

OBSAH

1. ÚVOD

Ochrana informačních systémů, dat a organizací je aktuálním problémem kybernetické bezpečnosti především z pohledu společenského a ekonomického dopadu. Vznik a realizace kybernetických incidentů může narušit nejen informační systém a jeho prvky, ale také jiné oblasti organizace, které úzce souvisí se zajištěním její činnosti. K řešení vzniku a dopadů těchto nežádoucích událostí je možné aplikovat pojištění, které je zaměřeno na kompenzaci škod a obnovu související s kybernetickými incidenty. Klíčovou částí celého pojišťovacího procesu je stanovení pojistného plnění, tedy pojistné hodnoty. Pro stanovení výše pojistné hodnoty je nezbytné využít jak přístupů typických pro oblast pojišťovnictví, tak také např. pro oblasti informačních technologií nebo bezpečnosti. A právě tento přístup ke stanovení výše pojistné hodnoty se jeví jako zásadní problém v současné oblasti pojištění.

Pro stanovení výše pojistné hodnoty pro jednotlivé organizace je využíváno především matematického aparátu. Tento přístup je také doplněn o dotazníky, které jsou vyplňovány samotnou organizací, a také statistickými údaji o dané problematice. V disertační práci je navržen a rozvíjen přístup pro stanovení výše pojistné hodnoty, který je koncipován na principu oceňování vybraných prvků organizace. Tyto prvky představují důležité oblasti, jejichž narušení vlivem kybernetického incidentu může způsobit ochromení nebo výrazné narušení informačního systému organizace a dalších významných aktiv. Další částí navrhovaného algoritmu je charakteristika vybraných kybernetických scénářů, které jsou ve vzájemných interakcích porovnávány s identifikovanými ohroženými prvky organizace. Pro tyto účely je využíváno analytických metod, prostřednictvím kterých je prováděno modelování této interakce. Výsledkem celého procesu je identifikace nejzávažnějšího scénáře kybernetické hrozby pro organizaci, a to na základě dopadů na vybrané ohrožené prvky. Posledním krokem je stanovení možné výše finančních škod v případě jeho realizace. Výstupy algoritmu je poté možné aplikovat v procesu stanovení výše pojistné hodnoty pro jednotlivé organizace.

Navržený algoritmus v rámci své funkce propojuje problematiku informačních a komunikačních technologií, oblasti bezpečnosti a ochrany dat a také právních a ekonomických aspektů, které v současné době v oblasti pojištění kybernetických hrozeb absentují. Navrhovaný algoritmus, který je určen primárně pro pojišťovny, lze také využít pro samotné organizace, které mohou pomocí jeho aplikování zjistit svou bezpečnostní úroveň a možný dopad případného kybernetického incidentu. Uplatnění může najít také v agenturách, které poskytují služby v oblasti analýzy informačního prostředí pro pojišťovny a zajišťovny. V neposlední řadě lze práci doporučit akademické a vědecké sféře nebo také laické veřejnosti, která se zajímá o danou problematikou.

2. SOUČASNÝ STAV ŘEŠENÉ PROBLEMATIKY

Kybernetické útoky již v dnešní době nejsou cíleny pouze na internetové firmy. V ohrožení je v podstatě kdokoliv, kdo pracuje s daty. Významnost kybernetické bezpečnosti pro úspěšnost podnikání je srovnatelná s fyzickou bezpečností. Zatímco proti krádeži nebo poškození se firmy mohou pojistit, tak v případě vlastních zákaznických dat je situace složitější (Ponemon study, 2018; Čermák, 2009).

V České republice produkt, týkající se pojištění kybernetických hrozeb, nebyl do roku 2013 nabízen. Od roku 2013 jej začala nabízet pobočka americké pojišťovny AIG v Praze v podobě produktu Cyber Edge. S platností legislativy GDPR (General Data Protection Regulation) byl v České republice zaznamenán nárůst tohoto typu pojištění pro malé a střední organizace (tzv. SME). Mezi pojišťovny, které mají ve svém portfoliu tento typ pojistného produktu na tuzemském trhu, patří také společnosti Renomia nebo Kooperativa (Moláček a Konečný, 2017).

V zahraniční je ale situace jiná. V USA, Německu a Velké Británii je množství takových nabízených pojistných produktů vyšší a stejně tak i počet firem, které si jej sjednají. Poměrně velkým problémem je nepoměr částek, ve kterých se vyplácí pojistné krytí. Dohromady tato částka v USA činí 2,45 mld. dolarů, což je 68,2 mld. korun. I tato částka je ale ve skutečnosti nedostatečná. Podle poradenské společnosti PWC, totiž 90 % pojistného připadá na americké firmy. Přitom má pojištění proti škodám jen třetina firem v USA (PWC – Insurance 2020 & beyond, 2015; Franke, 2017).

Pojištění kybernetických hrozeb je ve své podstatě kombinací **majetkového** pojištění (tzn. poskytování pojistného plnění za škody způsobené pojištěnému) a pojištění **odpovědnosti za škodu**, kdy jsou hrazeny škody, způsobené třetím osobám.

Pojištění poskytuje pojistnou ochranu před:

- únikem osobních údajů, informací a dat z informačního systému firmy, ať již náhodného charakteru nebo z nedbalosti,
- cíleným napadnutím informačního systému třetími osobami nebo zaměstnanci za účelem získání přístupu k citlivým informacím (Smejkal, 2018. AIG 2018).

Škody, které lze z pojištění proti kybernetickým hrozbám hradit

Současné pojistné produkty jsou nastaveny na krytí následujících škod:

- škody pojištěného způsobené únikem citlivých korporátních dat a informací,

- náklady pojištěného na oznámení úniku osobních údajů, informací a dat dozorovým orgánům a veřejnosti a komunikace s postiženými klienty, sloužící k ochraně dobré pověsti společnosti,
- náklady pojištěného na identifikaci úniku osobních údajů a informací, zabezpečení běžného provozu informačního systému firmy a realizace opatření k nápravě nedostatků, které způsobily únik,
- škody třetích stran v souvislosti s únikem,
- náklady pojištěného na jednání s dozorovými orgány a jimi udělené pokuty,
- ztráty zisku pojištěného v důsledku webových nebo síťových služeb a úniku osobních údajů a dat (Smejkal, 2018; AIG, 2018).

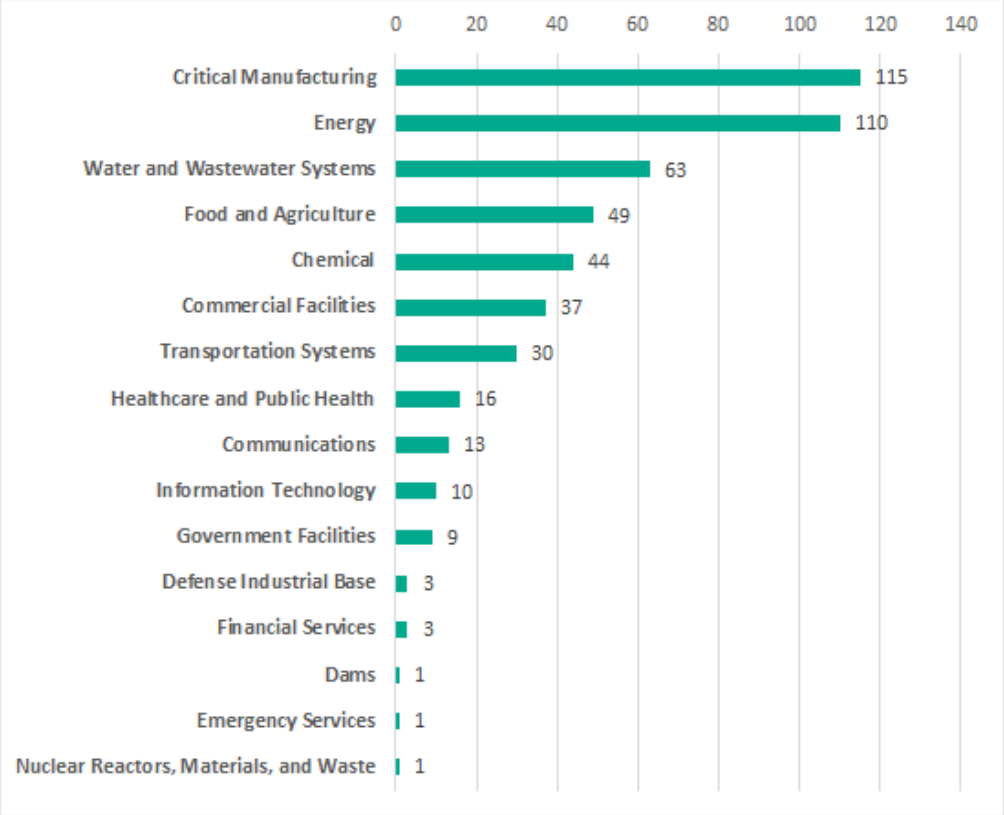
Pojištění proti kybernetickým hrozbám je řešeno pojistnou smlouvou, stejně jako jiné druhy pojištění, ve které jsou stanoveny podmínky a rozsah pojistného krytí. Podle přání pojistníka je možné sjednat i smluvní ujednání, které se liší od pojistných podmínek tak, aby pojistné krytí reagovalo na konkrétní situaci a jeho potřeby. Při sjednání pojištění je samozřejmě klíčové rozpoznání hrozeb, se kterými se zájemci o pojištění kybernetických hrozeb mohou setkat (AIG, 2018).

Velmi důležitou roli hraje dotazník pojistitele, který zájemce o pojištění vyplňuje. V dotazníku jsou uvedeny informace týkající se oboru činnosti pojistníka, údajů a typů dat, se kterými společnost pracuje a které shromažďuje o svých klientech. Pojistitel také úzce spolupracuje s IT společností, která přispívá k vyjasňování určitých specifik na straně zájemce o pojištění (AIG, 2018).

Pojistit společnost proti kybernetickým hrozbám je v současné době velmi riskantní. Zatímco potenciálně vzniklé škody jsou podle pojišťoven a jejich měřítek srovnatelné s velkými přírodními katastrofami, výskyt kybernetických incidentů je v tomto případě mnohem vyšší. V České republice se této skutečnosti pojišťovny obávají, tudíž zde není nabídka tohoto typu pojištění na trhu tak velká. Na druhou stranu lze konstatovat, že jistý zájem ze strany firem zde existuje, ale obvykle k němu dochází až po zveřejnění nějaké mediální kauzy spojené s únikem nebo zneužitím dat. Organizace si uvědomují, že je zde určitá hrozba v podobě cíleného kybernetického útoku, ale většinou pod nátlakem další operativy tuto skutečnost odsouvají na neurčito. Danou oblast většinou řeší až tehdy, když nastane vážný bezpečnostní problém (AIG, 2018; Moláček a Konečný, 2018).

Pojištění proti kybernetickým hrozbám lze poskytnout jakékoliv organizaci, bez ohledu na obor jejího podnikání nebo fungování. Nechat si pojistit svá data tedy může jak výrobní podnik, tak např. univerzita nebo krajský úřad. Je důležité poznamenat, že pojištění proti kybernetickým hrozbám se vztahuje na pojištění dat třetích stran. Tato skutečnost znamená, že mohou být pojištěna data týkající se např. osobních údajů o zákaznících nebo studentech, nikoliv samotné „know-how“ organizace (Ponemon study, 2018).

Tento typ pojištění nachází své uplatnění také ve veřejném sektoru. Na Obr. 2.1 jsou uvedeny sektory, seřazené podle počtu zranitelných prvků z hlediska napadení kybernetickými hrozbami. Jak můžeme vidět, oblast výroby, energetiky nebo vodohospodářství patří mezi nejvíce zranitelné cíle vůči kybernetickým útokům, a proto pojištění proti kybernetickým hrozbám může pomoci dopady těchto nežádoucích událostí snížit (Kaspersky Lab ICS CERT, 2019).



Graf 2.1: Počet zranitelných prvků, používaných v různých průmyslových odvětvích (Kaspersky Lab ICS CERT, 2019)

3. CÍLE DISERTAČNÍ PRÁCE

Cíle disertační práce vychází z kritického zhodnocení současného stavu v oblasti pojištění proti kybernetickým hrozbám. Na základě provedených analýz dostupných odborných materiálů, legislativního rámce a ICT, nástrojů autor dospěl k názoru, že ve zkoumané oblasti absentuje ucelený metodický postup a algoritmus, jehož aplikace v oblasti pojišťovnictví by umožňovala stanovení výše pojistné hodnoty pro organizaci vůči kybernetickým hrozbám. Tento metodický postup nebo algoritmus by měl umožnit stanovení výše potenciálních finančních škod v informačním prostředí organizace s ohledem na problematiku bezpečnosti, ekonomiky, legislativy a informačních technologií.

Pro vytvoření takového algoritmu musí autor disertační práce vyřešit tyto otázky:

a) Jaké oblasti organizace mohou být nejvíce zasaženy dopadem kybernetických hrozeb?
b) Jak stanovit finanční škody ve sledovaných oblastech ve vztahu ke kybernetickým hrozbám, které mohou organizaci ohrozit?
c) Jak vyjádřit pojistnou hodnotu, která by reflektovala dopady kybernetických hrozeb na dané oblasti?
d) Je navržený algoritmus aplikovatelný pro praxi?

Vyřešením těchto otázek je autor schopen splnit hlavní cíl disertační práce, tedy **vytvoření algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví.**

K dosažení hlavního cíle, bude nutné splnit tyto dílčí cíle:

- identifikace kybernetických hrozeb, které mohou být součástí pojištění proti kybernetickým hrozbám,
- specifikace ohrožených prvků, které jsou ovlivněny dopadem kybernetických hrozeb a ve kterých mohou organizaci vznikat finanční náklady,
- definování způsobu ocenění specifikovaných ohrožených prvků v organizaci,
- stanovení výše finančních dopadů vybraných kybernetických hrozeb na jednotlivé ohrožené prvky na základě jejich vzájemné interakce,
- vytvoření algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví a jeho ověření na vybraných referenčních objektech.

Omezení disertační práce:

- z důvodu rozsahu bude navrhovaný algoritmus aplikován pouze na organizace, které se nacházejí v soukromém sektoru,
- z důvodu rozsahu řešeného tématu, bude výsledkem navrhovaného algoritmu stanovení pojistné hodnoty, tzn. že nebude stanoven konečný pojistný limit pro organizaci.

4. ZVOLENÉ METODY ZPRACOVÁNÍ

Pro zjištění aktuálního stavu řešené problematiky byla provedena rešerše zahraničních i tuzemských informačních zdrojů, které jsou v této problematice klíčovým zdrojem informací. K řešení disertační práce bylo použito vědeckých metod, které jsou obvyklou součástí vědeckých prací.

Využity byly především tyto metody:

- metoda analýzy a syntézy,
- metoda indukce a dedukce,
- metoda srovnávání (komparace),
- metoda analogie,
- metoda modelování,
- metody multikriteriálního hodnocení.

a) Metoda analýzy

Analýza je jednou ze základních metod poznání, pomocí níž je konkrétní objekt rozložen na dílčí části a jsou zjišťovány vazby mezi jednotlivými částmi a celkem. Na základě analýzy můžeme vyslovit obecné závěry o určitém objektu nebo jevu. Metoda analýzy byla aplikována při identifikaci ohrožených prvků organizace.

b) Metoda syntézy

Syntéza spojuje jednotlivé části daného objektu, jevu nebo systému do jednoho celku. Jedná se o proces, kdy je vytvářen strukturovaný objekt z jeho jednotlivých prvků a jejich vzájemných vazeb. Metoda syntézy byla v disertační práci využita pro spojování jednotlivých oblastí organizace do celku, který bude dále systematicky posuzován. Tato metoda byla dále využita k vytvoření uceleného algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví.

c) Metoda indukce

Tuto vědeckou metodu lze rovněž označit jako párovou a patří rovněž do kategorie logických metod. Pomocí indukce jsou vytvářeny obecné závěry na základě zjištěných poznatků o jednotlivých objektech nebo jevech. Induktivní úsudky umožňují dojít k podstatě zkoumaných jevů a stanovit jejich zákonitosti. Tato metoda byla v disertační práci využita především pro stanovení ohrožených prvků organizace na základě provedeného dotazníkového šetření.

d) Metoda dedukce

Prostřednictvím dedukce jsou vyvozována nová tvrzení. Jedná se tedy o opak indukce. Tyto metody byly v disertační práci použity pro stanovení závěrů na základě provedeného výzkumu a dosažených výsledků.

e) Metoda srovnávání

Tato metoda patří mezi empirické metody. Při porovnávání se posuzují shodné nebo rozdílné stránky zkoumaných objektů nebo jevů a na základě zjištěných výsledků se provádějí korekce. Tato metoda byla aplikována v disertační práci ve fázi modelování a stanovení výše pojistné hodnoty.

f) Metoda analogie

Jedná se o myšlenkový postup, při němž jsou zjišťovány shody vybraných znaků objektu nebo jevu zkoumaného celku. Tato vědecká metoda byla v disertační práci aplikována při porovnávání scénářů kybernetických hrozeb a ohrožených prvků organizace.

g) Metoda modelování

Modelování je metodou často používanou ve vědecké praxi v mnoha oborech. Cílem použití této metody je napodobit chování zkoumaného systému a ovlivnit jeho chování požadovaným způsobem. Model je vždy pouze přiblížením reálnému objektu, který může být na rozdíl od modelu mnohem složitější. Metoda modelování byla v disertační práci aplikována ve fázi porovnávání scénářů kybernetických hrozeb s ohroženými prvky organizace.

h) Metoda multikriteriálního hodnocení

Multikriteriální hodnocení je metoda, která se používá pro rozhodování mezi více variantami, přičemž se nepřipouští existence více variant řešení. Výsledkem by měla být pouze jedna varianta řešení. Předpokladem použití této metody je větší počet kvantifikovatelných kritérií, která jsou zahrnuta do hodnocení. Tato metoda byla použita pro stanovení vah u nejzávažnějších kybernetických hrozeb v organizaci.

5. HLAVNÍ VÝSLEDKY PRÁCE

5.1 Návrh algoritmu pro stanovení pojistné hodnoty z hlediska pojištění proti kybernetickým hrozbám

Hlavním účelem **algoritmu pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví** (dále jen algoritmus) je poskytnout rámec pro vyjádření potenciálních finančních škod, které mohou v organizaci nastat vlivem realizace kybernetické hrozby. Nástroj nebo postup, který by umožňoval dosáhnout tohoto cíle, v současné době absentuje a přitom je zřejmé, že v nejbližších letech bude potřeba. Algoritmus sjednocuje různé pohledy a oblasti, které jsou pro vyjádření pojistné hodnoty v oblasti pojištění proti kybernetickým hrozbám nezbytné. Jedná se především o hlediska ekonomická a informaticko-bezpečnostní.

Navržený algoritmus je rozdělen do následujících fází:

a) Fáze 1: Definování ohrožených prvků organizace a jejich ocenění
b) Fáze 2: Hodnocení významnosti jednotlivých ohrožených prvků organizace
c) Fáze 3: Hodnocení závažnosti vybraných kybernetických hrozeb
d) Fáze 4: Modelování interakce mezi vybranými kybernetickými hrozbami a definovanými ohroženými prvky
e) Fáze 5: Identifikace nejzávažnější kybernetické hrozby
f) Fáze 6: Určení pojistné hodnoty

Na základě Fáze 1 jsou určeny tzv. ohrožené prvky organizace, které představují oblasti, které mohou být zasaženy dopadem kybernetických hrozeb. Finanční škody, které mohou v těchto oblastech vzniknout, mohou významným způsobem zatížit fungování organizace.

Fáze 2 je zaměřena na stanovení významnosti jednotlivých ohrožených prvků pro organizaci. Toto ohodnocení je prováděno na základě semikvantitativní stupnice.

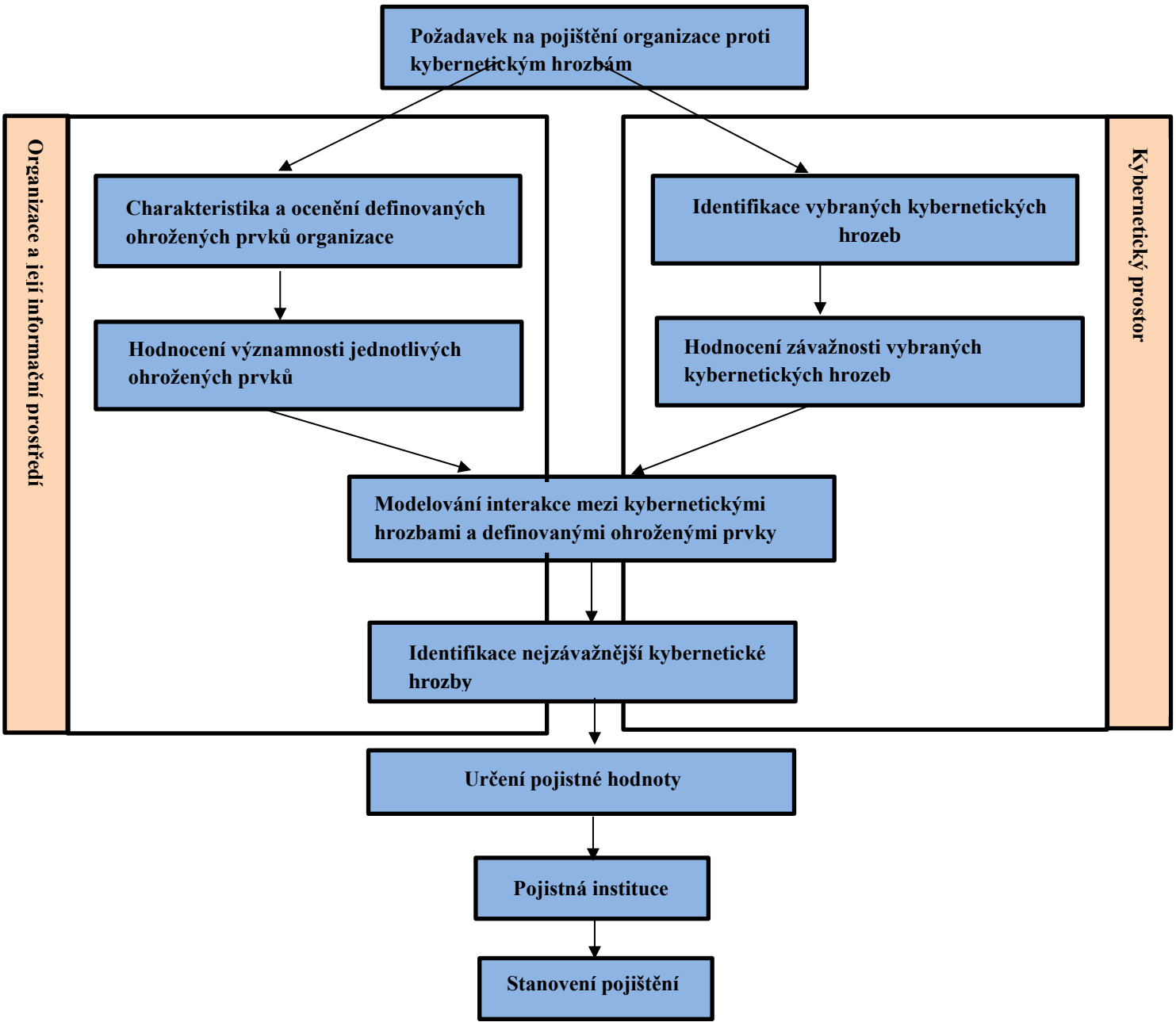
Fáze 3 je určena ke stanovení významnosti uvažovaných kybernetických hrozeb, které mohou být uvažovány v rámci pojištění organizace. Stanovení významnosti těchto kybernetických hrozeb je prováděno na základě semikvantitativní stupnice.

Fáze 4 představuje modelování interakce mezi vybranými kybernetickými hrozbami a ohroženými prvky. Pro tyto účely je zde použito vybraných metod analýzy rizik, které slouží pro vyjádření dopadu jednotlivých kybernetických hrozeb na dané ohrožené prvky.

Fáze 5 je zaměřena na určení nejzávažnější kybernetické hrozby pro organizaci na základě pořadí zjištěných rizik. Tato skutečnost je zjištěna jednak na základě výsledků provedené analýzy rizik, ale také prostřednictvím Saatyho metody.

Fáze 6 pak představuje stanovení pojistné hodnoty na základě navržené semikvantitativní stupnice, pomocí které lze odvodit možné finanční dopady na organizaci a její informační prostředí.

Návrh algoritmu a jeho fází je uveden na následujícím schématu.



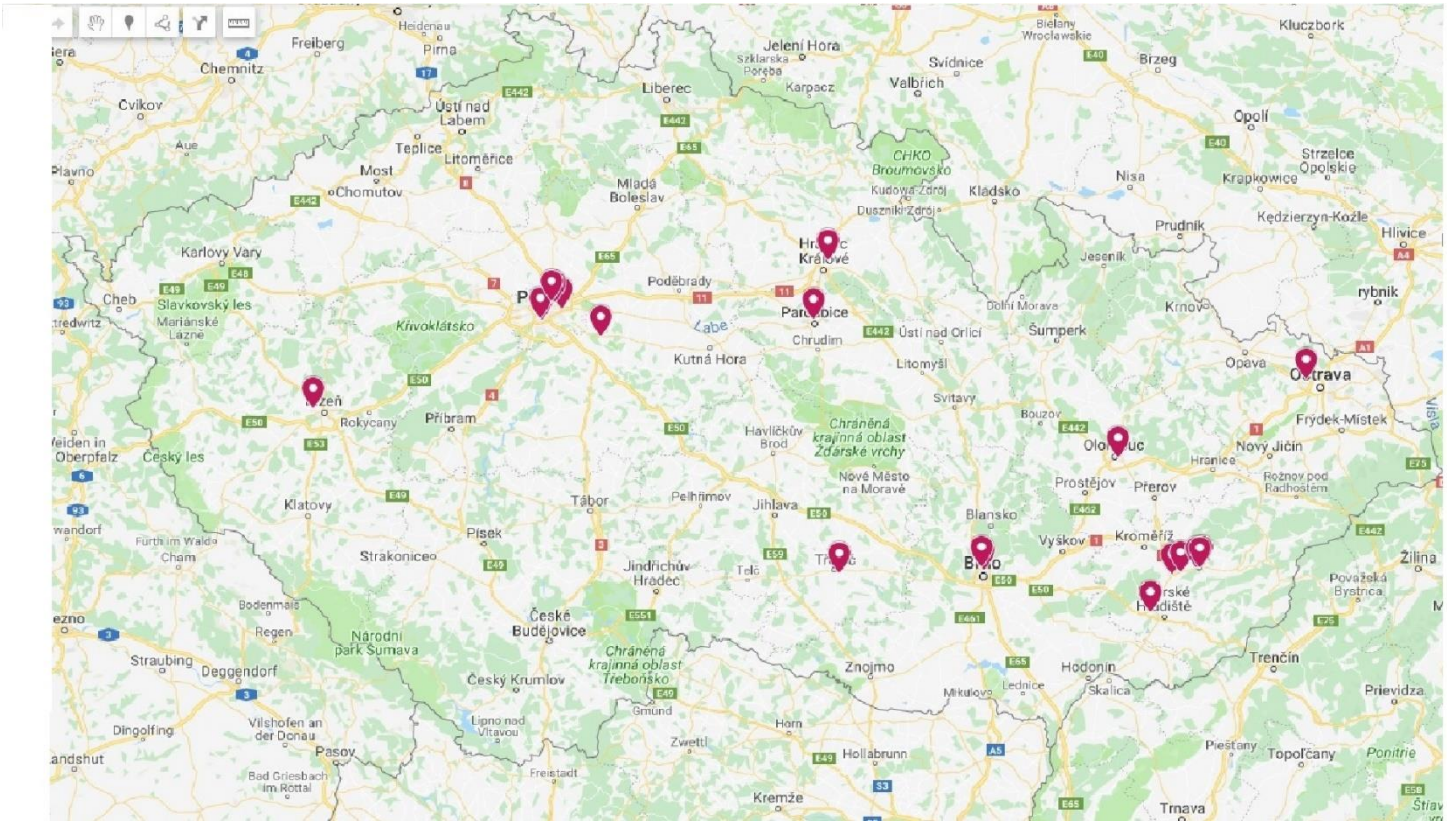
Obr. 5.1: Schéma navrhovaného algoritmu

5.2 Návrh a zpřesnění ohrožených prvků organizace

Nástrojem pro ověření hlavního cíle disertační práce, bylo dotazníkové šetření, jehož cílem je zmapovat a ověřit stav organizací z pohledu pojištění proti kybernetickým hrozbám. Cílem dotazníkového šetření k disertační práci byla především **analýza referenčních objektů a dále ověření stanovených cílů, které jsou předpokladem pro návrh algoritmu.** Vzhledem k tomu, že v oblasti pojištění proti kybernetickým hrozbám není doposud zpracováno dostatečné množství odborné literatury nebo vědeckých prací, je tento dotazník unikátním nástrojem pro sběr požadovaných dat.

Dotazníkové šetření probíhalo ve 20 organizacích na území České republiky. Tyto organizace lze vzhledem k jejich velikosti a počtu zaměstnanců zařadit mezi malé, popř. střední podniky. Jednalo se výhradně o organizace ze soukromé sféry, které se liší svou podstatou podnikání i informačním prostředím.

Na obr. 5.2 je uvedena mapa, ve které je vyznačeno umístění dotazovaných referenčních objektů.



Obr. 5.2: Mapa umístění organizací, které byly předmětem dotazníkového šetření (vlastní zdroj)

Hlavní výsledky disertační práce představují ohrožené prvky organizace, které jsou klíčovými oblastmi informačního prostředí organizace z pohledu kybernetického pojištění. Každý prvek organizace je doplněn vývojovým diagramem, který slouží pro znázornění průběhu a dopadu kybernetických hrozeb na vybrané ohrožené prvky.

Mezi tyto ohrožené prvky lze zařadit:

- hardware,
- software,
- ušlý obrat,
- pokuty,
- dobré jméno organizace,
- náklady na rekonstrukci a obnovu dat,
- náklady na oznámení ztráty nebo úniku dat.

5.2.1 Hardware

Do oblasti hardware lze zařadit v tomto případě nejen počítače a jejich příslušenství, ale také jakékoliv technické vybavení, které souvisí s informačním systémem organizace.

5.2.2 Software

Pro účely této disertační práce bude použita výše nákladů, která by musela být vynaložena na reinstalaci softwaru v případě jeho narušení. Vzhledem k tomu, že organizace vlastní licenci na provoz softwarových nástrojů, není nutné tento software znovu pořizovat za novou cenu. Může také nastat situace, kdy je software pořízen a vázán na hardware, se kterým byl zakoupen, nicméně tato možnost není v případě malých a středních podniků příliš pravděpodobná.

5.2.3 Ušlý obrat

Pokud realizace kybernetické hrozby naruší výrobní proces organizace (pokud v organizaci nějaký probíhá) nebo základní funkce a činnosti podnikání, je nutné v procesu stanovení pojistné hodnoty zohlednit také možný ušlý obrat. Za ušlý obrat se považuje množství finančních prostředků, které jsou přijaty ekonomickým subjektem za určité časové období.

5.2.4 Pokuty

Pro ocenění této kategorie nelze použít předem stanovený vzorec. Výše pokut je individuální záležitostí a záleží na posouzení subjektů, které mohou pokutu dle platné legislativy uložit. Při stanovování výše pokuty je brána v úvahu povaha, závažnost a délka porušení ochrany dat. Dále pak jestli se jedná o ojedinělou

událost, nebo o systematické porušování, jestli došlo k porušení úmyslně, nebo z nedbalosti apod. Všechny skutečnosti, které vstupují do procesu stanovení výše pokuty, jsou definovány v nařízení GDPR, které je pro území České republiky upraveno zákonem č. 110/2019 Sb., o zpracování osobních údajů.

5.2.5 Dobré jméno organizace

Pro potřeby finančního vyjádření dobrého jména organizace je nutné charakterizovat, co je pod tímto pojmem uvažováno. V rámci pojištění proti kybernetickým hrozbám je „poškozením dobrého jména“ myšlena budoucí finanční újma, která vznikne realizací kybernetické hrozby v určitých oblastech organizace. Těmito oblastmi jsou dodavatelé, odběratelé, zákazníci a sponzoři. Jedná se tedy o finanční prostředky, o které vlivem nežádoucí události může organizace přijít v určitém časovém rozmezí.

5.2.6 Náklady na rekonstrukci nebo obnovu dat

Náklady na rekonstrukci a obnovu dat lze definovat jako účelně vynaložené náklady na obnovu a znovuzískání dat z hardwarových a softwarových prostředků. Ztráta dat může nastat tedy v případě, že je narušen zdroj nebo nosič, na kterém jsou data uložena nebo zálohována.

5.2.7 Náklady na oznámení ztráty nebo úniku dat

V rámci pojistného krytí by měly být brány v úvahu také náklady na oznámení ztráty nebo úniku dat dozorovým orgánům. Do této kategorie je zahrnuto také informování dalších poškozených stran, které jsou kybernetickým incidentem dotčeny, komunikace s těmito dotčenými subjekty apod.

Pro každý z těchto ohrožených prvků je navržen matematický aparát, prostřednictvím kterého lze vyjádřit jejich finanční cenu, která je součástí stanovení pojistné hodnoty organizace.

5.3 Verifikace algoritmu

Navržený algoritmus byl ověřován na dvou organizacích, které mají rozdílný předmět činnosti a také informační prostředí. Algoritmus byl z důvodu přehlednosti rozdělen na ekonomickou část a na informaticko-bezpečnostní část. V rámci stanovení pojistné hodnoty byla nejprve vyjádřena cena jednotlivých ohrožených prvků organizace. V dalších krocích byla prostřednictvím vybraných metod analýzy rizik stanovena významnost jednotlivých ohrožených prvků a byla rovněž vyjádřena zranitelnost organizace vůči definovaným kybernetickým hrozbám. Výsledkem tohoto procesu bylo vytvoření matice rizik, ve které bylo na základě interakce mezi ohroženými prvky a kybernetickými hrozbami stanoveno pořadí jednotlivých hrozeb. Posledním krokem provedené analýzy bylo

identifikování nejzávažnější kybernetické hrozby pro jednotlivé organizace a vyjádření možné výše pojistné hodnoty.

Na základě návrhu pojistné hodnoty pro každou organizaci, bylo vydáno stanovisko jednotlivých organizací, které tímto potvrdily, že předložené závěry a výsledky aplikace navrženého algoritmu odpovídají možným finančním dopadům vybraných kybernetických hrozeb na informačním prostředí organizace. Výsledky aplikace navrženého algoritmu byly zkoumány odborníkem na oblast informačních technologií v jednotlivých organizací. Výsledné stanovisko je sestaveno a podepsáno vedoucím manažerem každé organizace.

6. PŘÍNOS PRO VĚDU A PRO PRAXI

V rámci této kapitoly je popsán význam a přínos navrhovaného výsledku disertační práce pro vědu a praxi. Jsou zde popsány hlavní výstupy výzkumu, které jsou uvedeny v následujících dvou podkapitolách.

6.1 Přínos pro vědu

Výsledky disertační práce jsou přínosné pro vědeckou komunitu především z pohledu kvantifikace definovaných ohrožených prvků a stanovení možných finančních dopadů na organizaci a její informační systém. Jelikož se jedná o transdisciplinární oblast zájmu, výsledky disertační práce mohou najít své uplatnění především v oblastech, jako je ekonomika, informační a komunikační technologie nebo bezpečnost. Navržený algoritmus může přinést nový pohled do oblasti kybernetické bezpečnosti, a to především pro popis a zkoumání možných dopadů kybernetických hrozeb na organizaci a její informační prostředí. Tento nový pohled může najít své uplatnění ve vědecké komunitě především z důvodu zachycení vzájemných vztahů mezi ohroženými prvky a kybernetickými hrozbami a tím zpřesnění stanovení potenciálních finančních škod v organizaci.

Výsledky výzkumu byly v průběhu řešení disertační práce publikovány v řadě odborných příspěvků v rámci recenzovaných časopisů, mezinárodních konferencí a odborných časopisů, které jsou evidovány v databázích SCOPUS nebo Web of Science.

6.2 Přínos pro praxi

Hlavní výsledky práce bude možné uplatnit především v oblasti pojišťovnictví a kybernetické bezpečnosti jako analytický nástroj pro posouzení bezpečnostní stránky organizace, která má být pojištěna proti dopadům kybernetických hrozeb. Jelikož současné přístupy k řešení této problematiky nezohledňují vždy všechny aspekty, které mohou mít zásadní vliv na výši pojistné hodnoty, může navrhovaný algoritmus poskytnout přehled o možných dopadech v různých oblastech organizace, které jsou ovlivňovány funkcí informačního systému. Z tohoto důvodu je navrhovaný algoritmus velmi přínosný pro odborníky v oblasti kybernetické bezpečnosti, pojistitele, pojistné makléře a také pro analytiky v oboru pojišťovnictví. Využít tento nástroj mohou také ratingové agentury nebo specializované firmy, které zajišťují odborné poradenství pro pojišťovny v oblasti informačních technologií a bezpečnosti.

Velký přínos může tato práce nalézt také v brzké budoucnosti. Vlivem vzrůstající frekvence kybernetických útoků na organizace a jejich informační systémy lze predikovat, že zájem o tento typ pojištění bude narůstat. Vzhledem k legislativě, která souvisí s ochranou osobních dat a sankcemi, které s touto problematikou souvisí, lze rovněž předpokládat, že organizace budou v rámci

ochrany svých aktiv vyvíjet větší zájem o pojištění tohoto typu. Dalším významným aspektem jsou také samotné finanční škody, které v oblastech jako je např. dobré jméno, ušlý obrat nebo náklady na rekonstrukci nebo obnovu dat mohou být pro organizaci likvidační. Finanční částka na obnovu těchto oblastí by mohla být pro poškozenou organizaci rovněž velmi zatěžující, a proto by pojištění proti kybernetickým hrozbám mohlo být vhodným nástrojem, jak tuto negativní událost a její dopady zmírnit a umožnit tak organizaci dosáhnout opět stavu rovnováhy.

7. ZÁVĚR

Současná společnost je čím dál více orientována na informační a komunikační technologie. Komunikační prostředky a nástroje se staly nedílnou součástí nejen lidských životů, ale také pracovního prostředí, ve kterém přispívají ke zkvalitňování podnikových procesů. Je zřejmé, že organizace využívající těchto informačních a komunikačních prostředků mohou být předmětem kybernetických útoků. Tyto útoky mohou mít za cíl nejen organizaci poškodit, ale také zamezit její funkci a obnově činnosti.

Předložená disertační práce je zaměřena na tuto oblast s cílem navrhnout algoritmus pro stanovení pojistné hodnoty plynoucí z dopadů vybraných kybernetických hrozeb na organizaci z pohledu pojišťovnictví. V rámci kompenzace a snižování potenciálních škod, které mohou vlivem některé z kybernetických hrozeb nastat, může být aplikován jako účinný nástroj pojištění organizace proti kybernetickým hrozbám. Navržený algoritmus je výsledkem nejen rešerší dostupných informačních zdrojů z této oblasti, ale také strukturovaných rozhovorů a konzultací se zástupci v oblastech pojišťovnictví, bezpečnosti a informačních a komunikačních technologií. Rešerše a konzultace byly provedeny jak v českém, tak zahraničním prostředí. Disertační práce vychází z předpokladu, že do procesu stanovení pojistné hodnoty organizace, která má být pojištěna proti kybernetickým hrozbám, by měly být zahrnuty také jiné oblasti, jejichž funkce ovlivňuje činnost celé organizace. Výzkum realizovaný v rámci řešení disertační práce tento předpoklad potvrdil. Došlo k identifikaci a zpřesnění ohrožených prvků organizace, které je nutno do stanovení výše pojistné hodnoty zahrnout.

Hlavním přínosem této práce z pohledu novosti je návrh algoritmu pro stanovení pojistné hodnoty, který je založen na definování a ocenění vybraných ohrožených prvků organizace, které představují z pohledu významnosti důležité oblasti organizace. Dále se jedná o stanovení vybraných kybernetických hrozeb včetně vyjádření interakce těchto hrozeb vůči stanoveným ohroženým prvkům, identifikaci nejzávažnější kybernetické hrozby pro danou organizaci a vyjádření potenciálních finančních dopadů na její informační prostředí.

SEZNAM LITERATURY

AIG - Cyber Edge: End-to-End Cyber Risk Management Solutions [online]. USA: AIG, 2015, 12 s. [cit. 2018-11-08]. Dostupné z: https://www.aig.com/content/dam/aig/america.pdf

ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009, 138 s. ISBN 978-80-7399-731-1.

FRANKE, Ulrik. The cyber insurance market in Sweden. *Computers & Security* [online]. USA: Elsevier, 2017, (68), 130 - 144 [cit. 2018-12-02]. ISSN 0167-4048. Dostupné z: https://www.sciencedirect.com

Insurance 2020 & beyond: Necessity is the mother of reinvention [online]. United Kingdom: PWC, 2015, 28 s. [cit. 2019-01-27]. Dostupné z: https://www.pwc.com/gx/en/insurance/publications/assets/pwc-insurance-2020-and-beyond.pdf

KASPERSKY LAB ICS CERT. *Threat landscape for industrial automation systems. H2 2018* [online]. Rusko, 2019 [cit. 2019-05-06]. Dostupné z: https://ics-cert.kaspersky.com/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/#_Toc4416091

MOLÁČEK, Petr a Daniel KONEČNÝ. Kybernetická rizika jsou pro české pojišťovny téma. *Cyberinsurance.cz* [online]. Praha, 2017, 31. 3. 2017 [cit. 2019-04-28]. Dostupné z: http://www.cyberinsurance.cz/?p=534

MOLÁČEK, Petr a Daniel KONEČNÝ. Role pojišťovnictví v kyber prostředí. *Cyberinsurance.cz* [online]. Praha, 2018, 17. 5. 2018 [cit. 2019-03-15]. Dostupné z: http://www.cyberinsurance.cz/?p=698

Ponemon study 2018 [online]. USA: Ponemon Institute, 2018, 47 s. [cit. 2019-04-28]. Dostupné z : https://databreachcalculator.mybluemix/assets/2018

SMEJKAL, Vladimír. *Kybernetická kriminalita*. 2. rozšířené a aktualizované vydání. Praha: Aleš Čeněk, 2018, 936 s. ISBN 978-80-7380-720-7.

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM POUŽITÝCH ZKRATEK

GDPR	General Data Protection Regulation
ICT	Information and Communication Technologies
IT	Informační technologie
SME	Small and Medium Enterprise

PUBLIKAČNÍ ČINNOST AUTORA

Články v recenzovaných časopisech evidovaných v databázi SCOPUS, WoS

PAVLÍK, Lukáš. Modeling the Impact of Cyber Threats on an Organization's Information System in the Framework of Cyber-Risk Insurance. *International Journal of Mathematical Models and Methods in Applied Sciences* [online]. USA: North Atlantic University Union, 2019, 5 s., **13**(13) [cit. 2019-04-26]. ISSN 1998-0140. Dostupné z: http://naun.org/cms.action?id=20232

PAVLÍK, Lukáš. Modeling the Impact of Selected Cyber Threats on the Organization's Parameters in the Framework of Cyber Risk Insurance. WSEAS Transactions on Business and Economics [online]. 2018, 7 s., **10** (Vol. 15) [cit. 2018-11-15]. ISSN 1109-9526. Dostupné z: http://www.wseas.org/multimedia/journals/economics/2018/b025107-669.pdf

Články ve vědeckých nebo odborných časopisech neevidovaných v databázích WoS, SCOPUS

PAVLÍK, Lukáš, Tomáš KLÍMA a Krerk PIROMSOPA. *The Issue of Cyber-Risk Insurance from the Point of View of the Valuation of the Information System in the Organization* [online]. Vol. 11. North Atlantic University Union, 2017, 6 s. [cit. 2017-11-26]. ISSN 1998-4308. Dostupné z: http://naun.org/cms.action?id=16148

PAVLÍK, Lukáš. POSTERUS.SK. *Metrics for Evaluating Information Systems* [online]. Slovensko, 2017, 10 s. [cit. 2017-05-17]. ISSN 1338-0087.

PAVLÍK, Lukáš. Quantitative and Qualitative Assessment Tools for Information Systems Security. Posterus.sk [online]. 2016, 9(5), 8 s. [cit. 2016-06-30]. ISSN 1338-0087. Dostupné z: http://www.posterus.sk/?p=18519

Články ve sborníku konference evidovaných v databázi SCOPUS, WoS

PAVLÍK, Lukáš. Design Methodology for Determining the Financial Damage caused by Cyber Threats in the Field of Insurance. In: *ICMT 2019*. Brno: Univerzita obrany, 2019.

FICEK, Martin, Lukáš PAVLÍK, Rui Miguel SOARES SILVA a Michaela MILKULIČOVÁ. *Influence of distance to depth shot of a CO2-powered airsoft gun with lead shot ammunition and shape of the temporary and permanent cavity in ballistic gelatin*. In: . Athens, Greece: 23 rd INTERNATIONAL CONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC 2019), 2019, 7 s.

Článek je přijat na konferenci, prezentován bude v červenci 2019.

VEČEŘA, Filip a Lukáš PAVLÍK . *The finding of the queuing theory models for evaluation throughput of the IRS radio network in the Czech Republic*. Athens, Greece: 23 rd INTERNATIONAL CONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC 2019), 2019, 6 s.

Článek je přijat na konferenci, prezentován bude v červenci 2019.

PAVLÍK, Lukáš. *Possibilities of modelling the impact of cyber threats in cyber risk insurance*. 22 nd INTERNATIONAL CONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC 2018). Majorca, Spain, 2018, 4 s.

ŠAUR, David a Lukáš PAVLÍK. *Comparison of accuracy of forecasting methods of convective precipitation*. Majorca, Spain: INTERNATIONAL CONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC 2018), 2018, 6 s.

GRACLA, Michal a Lukáš PAVLÍK. *Preparation of experimental measurements using a firearm.* Majorca, Spain: INTERNATIONAL CONFERENCE ON CIRCUITS, SYSTEMS, COMMUNICATIONS AND COMPUTERS (CSCC 2018), 2018, 6 s.

PAVLÍK Lukáš. *Identifying and Modeling the Impact of Cyber Threats in the Field of Cyber Risk Insurance*. INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN SCIENCES AND INDUSTRY 2018. Corfu, Greece: IEEE, 4 s. [cit. 2018-04-30].

PAVLÍK, Lukáš. *Mathematical Method as a Tool for the Identification of Assets within the Organization Providing Insurance against Cyber Risk.* INTERNATIONAL CONFERENCE KNOWLEDGE FOR MARKET USE 2017. Univerzita Palackého, Filozofická fakulta, Olomouc, 2017, 9 s. ISBN 978-80-244-5233-3

KLÍMA, Tomáš, Krerk PIROMSOPA a Lukáš PAVLÍK. *Designing model for calculating the amount of cyber risk insurance*. INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN SCIENCES AND INDUSTRY 2017. Corfu, Greece: IEEE, 5 s.

PAVLÍK, Lukáš a Luděk LUKÁŠ *Pareto Analysis as a Tool for the Identification of Assets within the Organization Providing Insurance against Cyber Risk*. INTERNATIONAL CONFERENCE ON MILITARY TECHNOLOGIES 2017. Univerzita obrany, Brno, 2017, 5 s. ISBN 978-1-5386-1988-9 [cit. 2017-05-17]

PAVLÍK, Lukáš a Roman JAŠEK. *Possibilities Pricing of the Information System by Providng Insurance against Cyber Risk: International Scientific Conference: Knowledge for Market Use 2016* [online]. Univerzita Palackého, Olomouc, 2016, 8 s. [cit. 2016-10-26]. ISBN 978-80-87533-14-7.

LUKÁŠ, Luděk, Martin HROMADA a Lukáš PAVLÍK. INTERNATIONAL CONFERENCE ON MATHEMATICS AND COMPUTERS IN SCIENCES AND INDUSTRY 2016. *The Key Theoretical Models for the Safety and Security Ensuring* [online]. Chania, Crete: IEEE, 2016, 5 s. [cit. 2017-05-17]

Články ve sborníku konference neevidovaných v databázi SCOPUS, WoS

PAVLÍK, Lukáš a Martin FICEK. *Identifikace aktiv ovlivňujících cenu informačního systému organizace v rámci poskytování pojištění proti kybernetickým hrozbám.* Mezinárodní Konference Bezpečnostní Technologie Systémy a Management. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2017, 6 s. ISBN 978-80-7454-696-9.

PAVLÍK, Lukáš. *Specifikace faktorů ovlivňujících cenu informačního systému v rámci poskytování pojištění proti kybernetickému riziku: XXV. ročník*

mezinárodní konference Požární ochrana 2016. Ostrava, 2016, 7 s. ISBN 978-80-7385-177-4. ISSN 1803-1803.

VEČEŘA, Filip a Lukáš PAVLÍK. *Možnost zvyšování odolnosti radiokomunikační sítě PEGAS jako prvku kritické infrastruktury*. Mezinárodní Konference Bezpečnostní Technologie Systémy a Management. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2015, 8 s. ISBN 978-80-7454-559-7

ŠAUR, David a Lukáš PAVLÍK. *Využití programu SFERA pro účely ochrany kritické infrastruktury*. Mezinárodní Konference Bezpečnostní Technologie Systémy a Management. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, 2015, 7 s. ISBN 978-80-7454-559-7

PROFESNÍ ŽIVOTOPIS AUTORA

Osobní údaje:

Jméno a příjmení, titul:	Ing. Bc. Lukáš Pavlík
Datum narození:	15. 1. 1987
Stav:	svobodný
Adresa:	Třída Tomáše Bati, 1276, 760 01, Zlín
Kontaktní telefon:	724 589 193
E-mail:	lukas.pavlik87@gmail.com

Pracovní zkušenosti, praxe:

Organizace:	Crissis Consulting, s.r.o.
Náplň práce:	zpracovávání povodňových plánů, placená praxe
Doba trvání:	květen 2013 – září 2013
Organizace:	Principal engineering, s.r.o.
Náplň práce:	spolupráce na tvorbě metodických postupů v oblasti analýzy rizik
Doba trvání:	říjen 2016 – září 2018
Organizace:	Moravská vysoká škola Olomouc, o.p.s.
Náplň práce:	zajištění pedagogických a výzkumných činností
Doba trvání:	září 2017 – současnost

Vzdělání:

Škola:	Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, Zlín

Rok nastoupení a ukončení:	2015- současnost
Obor:	Inženýrská informatika – Inženýrská informatika (Ph.D.)
Škola:	Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, Zlín
Rok nastoupení a ukončení:	2013 - 2015
Obor:	Inženýrská informatika – Bezpečnostní technologie, systémy a management (Ing.)
Škola:	Univerzita Tomáše Bati ve Zlíně, Fakulta logistiky a Krizového řízení, Uherské Hradiště
Rok nastoupení a ukončení:	2010 – 2013
Obor:	Procesní inženýrství – Ovládání rizik (Bc.)

Znalosti a dovednosti:

PC:	MS WINDOWS, MS OFFICE, RISKAN, TERREX, INTERNET – úroveň znalostí pokročilá
Jazykové znalosti:	Anglický jazyk – pokročilá znalost
	Německý jazyk – základní úroveň
	Ruský jazyk – mírně pokročilý
Řidičský průkaz:	Skupiny B
Vlastnosti a zájmy:	Zodpovědnost, spolehlivost, preciznost,
	komunikativnost, sport

Lukáš Pavlík

Návrh algoritmu pro stanovení pojistné hodnoty z pohledu kybernetické bezpečnosti

Design of Algorithm for Determination of Insurance Value from the Perspective of Cyber Security

Teze disertační práce

Vydala Univerzita Tomáše Bati ve Zlíně,

nám. T. G. Masaryka 5555, 760 01 Zlín.

Náklad: vyšlo elektronicky

Sazba: autor

Publikace neprošla jazykovou ani redakční úpravou.

Pořadí vydání: první

Rok vydání 2019

ISBN 978-80-7454-863-5