EKONOMICKÁ UNIVERZITA V BRATISLAVE
NÁRODOHOSPODÁRSKA FAKULTA

Evidenčné číslo: 101008/B/2014/3780978269

POISTENIE RIZÍK INFORMAČNÝCH TECHNOLÓGIÍ

Bakalárska práca

2014 **Svetlana Lenická**

EKONOMICKÁ UNIVERZITA V BRATISLAVE
NÁRODOHOSPODÁRSKA FAKULTA

POISTENIE RIZÍK INFORMAČNÝCH TECHNOLÓGIÍ

Bakalárska práca

Študijný program:	Poisťovníctvo
Študijný odbor:	6216700 Poisťovníctvo
Školiace pracovisko:	Katedra poisťovníctva
Vedúci záverečnej práce:	Ing. Peter Marko, PhD.

Bratislava 2014 **Svetlana Lenická**

Čestné vyhlásenie

Čestne vyhlasujem, že záverečnú prácu som vypracovala samostatne a že som uviedla všetku použitú literatúru.

Dátum: 21. 05. 2014 **.....**

Poďakovanie

Chcela by som sa poďakovať vedúcemu mojej bakalárskej práce: Ing. Petrovi Markovi, PhD. za odbornú pomoc, cenné rady a za ochotu, tiež svojej najbližšej rodine, ktorá ma v štúdiu podporuje.

ABSTRAKT

LENICKÁ, Svetlana: *Poistenie rizík informačných technológií*. – Ekonomická univerzita v Bratislave. Národohospodárska fakulta; Katedra poisťovníctva. – Vedúci záverečnej práce: Ing. Peter Marko, PhD. – Bratislava: NHF EU, 2014, 51 s.

Cieľom tejto záverečnej práce je poskytnúť rozhľad o rizikách informačných technológií a možnostiach ich poistenia. Práca je rozdelená do troch kapitol. Obsahuje štyri grafy, päť tabuliek a 0 príloh. Prvá kapitola je venovaná stručnému opísaniu informačných technológií, rizikám ktoré sa s nimi spájajú a tiež som uviedla aj niekoľko základných opatrení k ich predchádzaniu. V ďalšej časti sa zaoberám cieľom svojej práce a jej metodikou. V záverečnej časti rozoberám problematiku poistiteľnosti rizík informačných technológií a možnosti ich poistenia v Spojených štátoch amerických a na Slovensku. Výsledkom riešenia danej problematiky je posúdenie situácie na trhu poistenia rizík informačných technológií.

Kľúčové slová: informácia, informačná technológia, poistenie, poistiteľnosť rizika

ABSTRACT

LENICKÁ, Svetlana: *Information technology risks insurance*. – The University of Economics in Bratislava. The Faculty of National Economy; Department of Insurance. – Supervisor: Ing. Peter Marko, PhD. – Bratislava: NHF EU, 2014, 51 s.

The purpose of this bachelor thesis is to provide a view of information technologies risks and the possibilities of insurance of them. The thesis is divided in three chapters. It contains four charts, five tables and 0 enclosures. The first chapter is devoted to brief exposition of information technologies, the risks related with them and I gave some fundamental arrangements to prevent them, too. In the next part I deal with the purpose of my thesis and its methodics. In the closing time I analyze the information technology insurability issues, the possibilities of insurance of them in the United States of America and in Slovakia. The outcome of solving the issue is consideration of the information technology insurance market situation.

Key words: information, information technology, insurance, insurability of risk

O B S A H str.

Úvod

Význam informačných technológií v prostredí ľudskej spoločnosti z roka na rok narastá geometrickým radom. Informačné technológie sú nezastupiteľné v mnohých významných oblastiach, ako veda, výskum, zdravotníctvo alebo výroba, ale aj pre každodenný život obyčajného človeka. Tento veľmi prudký vývoj a nezastupiteľné miesto má však aj svoje negatíva. Spoločnosť sa stáva závislá na informačných technológiách a tieto so sebou prinášajú i riziká, ktorých je neuveriteľne veľa, a ľudia si ich pomerne často vôbec neuvedomujú.

Dôvodom spracovania mojej témy bakalárskej práce boli predovšetkým výrazné zmeny, ktoré so sebou informačné technológie prinášajú pre ľudí, a tie nie sú iba pozitívne, ale aj negatívne. Poskytnem v nej možnosť bližšie sa oboznámiť s rizikami, ktoré sa sebou informačné technológie prinášajú, ale tiež poskytnem pohľad na možnosti, kde ich poistiť, ktoré riziká sa dajú poistiť a možnosti ich budúceho vývoja informačných technológií.

Cieľom mojej bakalárskej práce preto nie je len oboznámiť čitateľa so základnými znakmi a zložkami počítača a iných informačných technológií. Chcela by som najmä identifikovať hlavné riziká informačných technológií, s ktorými prichádza človek a spoločnosť do kontaktu neustále, niekedy bez toho, aby si to uvedomoval. Tiež uvediem niektoré možnosti, ktoré je možné vykonávať na predchádzanie týmto rizikám alebo zmierňovaniu škôd, ktoré môžu potenciálne spôsobiť.

Hlavným cieľom tejto práce sú však práve súčasné možnosti poistenia týchto rizík tak zo strany ponuky, ako aj dopytu. Najprv rozoberiem poistiteľnosť rizík informačných technológií z pohľadu poisťovní, pretože poistný trh krytia týchto rizík zatiaľ nie je tak dobre rozvinutý ako väčšina ostatných druhov poistenia. Mnohé poisťovne ich nekryjú, pretože ich považujú za veľmi neznáme. Na opačnej strane sa stáva čoraz nástojčivejším a tak mu poisťovne začínajú venovať čoraz väčšiu pozornosť.

Na druhej strane stoja klienti poisťovní. Riziká informačných technológií začínajú vplývať na klientov čím ďalej tým viac, a preto si ich poisťovne začínajú lepšie uvedomovať, tieto riziká sa im postupne dostávajú do povedomia. Keďže bežné bezpečnostné opatrenia pri týchto rizikách často nepostačujú, sú nákladné alebo sa pred nimi z nejakého dôvodu nedá chrániť, klienti majú záujem sa pred nimi poistiť. A to je ešte v súčasnosti u nás problematické. Z ich strany zase poskytnem pohľad na možnosti

poistného krytia takýchto rizík na Slovensku aj v zahraničí, kde je tento trh na oveľa vyššej úrovni.

1 Súčasný stav riešenej problematiky doma a v zahraničí

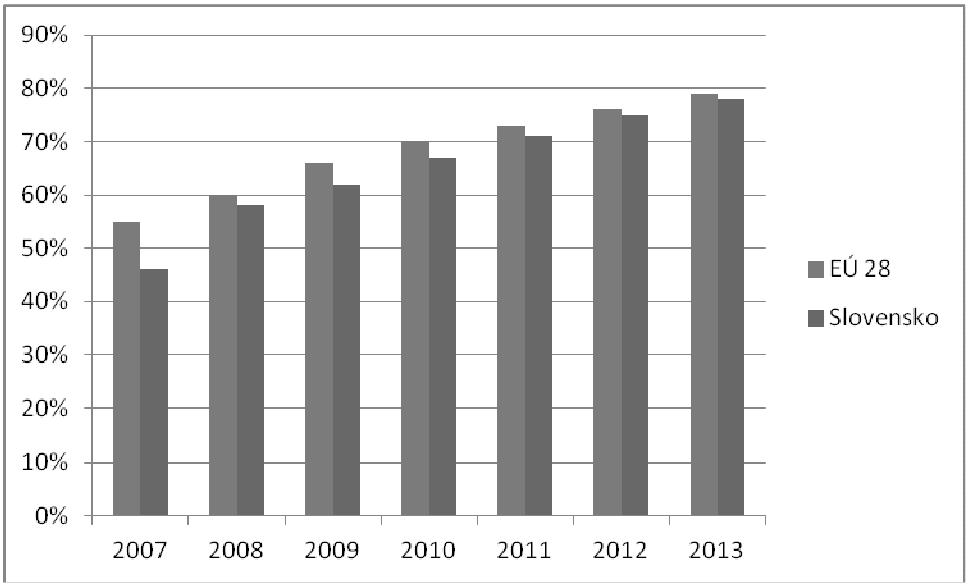
V posledných desaťročiach nastal prudký vývoj v oblasti informačných technológií. (ďalej len IT). To však podnietilo i nárast rizík IT, ktoré sú dnes veľmi vysoké. Preto sa v tejto kapitole budem zaoberať predovšetkým vymedzením pojmu IT a priblížením rizík, ktoré s nimi súvisia.

1.1 Informačné technológie

Ľudská spoločnosť prešla mnohými fázami vývoja. Významným zlomom jej bola agrárna revolúcia, neskôr priemyselná, a tak sa ľudstvo dostalo až k dnešnej spoločnosti, ktorá je často označovaná ako „informačná“. Napriek tomu, že toto označenie sa používa veľmi často, nie je jednoznačne charakterizovaná. Možno ju definovať ako prostredie, „v ktorom informácie majú prvoradý význam. Jej nástup urýchľujú možnosti nových informačných a komunikačných technológií. Umožňujú v nebývalom rozsahu rýchlu tvorbu a prenos informácií, vedeckých poznatkov do procesov technologických i sociálnych. To vedie k zmene spôsobu života každého človeka. Ovplyvnené sú všetky obory ľudskej činnosti. Mení sa obchod, služby, výroba, ale hlavne riadenie podnikov i celých štátov. Prekážky dané časom a vzdialenosťou sa postupne úplne odstránia sieťami na prenos informácií (napr. telefónnymi, satelitnými, káblovými), základnými službami pri využívaní sietí (napr. elektronická pošta, Internet) a novými možnosťami (napr. diaľkové, dištančné štúdium, práca na diaľku).“[1] Možno teda povedať, že súčasná spoločnosť, by sa bez internetu a iných informačných technológií.

[1] Citované: Jašková, Ľ. 2014. *Informačná spoločnosť*. [online]. Univerzita Komenského v Bratislave. 2014. [cit. 08.05.2014]. Dostupné na internete: <http://edi.fmph.uniba.sk/~jaskova/InformacneSystemy/tema01/tema01.html>

Graf 1 **Podiel domácností s prístupom na internet**



Zdroj: vlastné spracovanie podľa: EUROSTAT: Level of Internet access – households. [online] [13.05.2014]. Dostupné na internete: <http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00134>

Pod pojem informačné technológie zahŕňame všetky prístroje, metódy a štandardy slúžiace na zber, spracovávanie, uchovávanie, prenos a prezentáciu informácií, ktorými môžu byť rôzne údaje, zvukové stopy, texty, obrázky. „Medzi najvýznamnejšie moderné informačné technológie zahrnujeme:

- Počítače,
- Databázové technológie,
- Expertné systémy,
- Systémy na odporu rozhodovania,
- Automatizácia projektovania informačných systémov,
- Problémovo orientované počítačové systémy,
- Počítačové a terminálové siete,
- Kancelárske systémy,
- Elektronická výmena údajov,
- Elektronická pošta,
- Videokonferencie,
- Multimediálne systémy,
- Telematické služby,
- Elektronické bankovníctvo,

- Robotika,
- Internet, Intranet a iné.“[2]

Pre fyzické uskutočňovanie operácií sú potrebné technické prostriedky. Bývajú nazývané aj hardvér a zahŕňajú technické vybavenie počítačov, komunikačné prostriedky, dátové siete. Hardvér počítača sa skladá zo základnej jednotky a periférnych zariadení, ktoré sa k nej pripájajú. Do základnej jednotky patrí procesor a vnútorná pamäť. Medzi periférne zariadenia patrí napríklad monitor, klávesnica, USB kľúč, reproduktory. Periférne zariadenia možno rozdeliť na vonkajšie pamäte, vstupné a výstupné zariadenia, doplnkové zariadenia.

Pre prácu s údajmi prostredníctvom technických prostriedkov je však potrebné programové vybavenie. Toto je často nazývané softvér a predstavuje súhrn programov a dokumentácie, ktoré umožňujú prevádzku počítača. Zabezpečujú efektívnu činnosť počítača, uľahčujú prácu pri jeho obsluhe a riešia funkčné úlohy. Programové vybavenie počítača sa rozdeľuje na základné programové vybavenie, prostriedky na osobnú informatiku a aplikačné programové vybavenie.[3]

1.2 Význam a budúcnosť IT

Informačné technológie stávajú neodmysliteľnou súčasťou života. Možnosti ich využitia vo vyspelom svete sa stále zvyšujú a rozširujú, na čo má vplyv aj mimoriadny pokrok v tejto oblasti v posledných desaťročiach a množstvá inovácií v oblasti IT. Sú používané takmer každej oblasti, ako napríklad bežná komunikácia, vzdelávanie, podnikanie, zdravotníctvo, veda a výskum. S globalizáciou sa navzájom ovplyvňujú, ale aj podporujú.

IT taktiež prospievajú hospodárstvu krajiny. Ich význam si uvedomujú aj vlády. Napríklad 24. a 25. Októbra 2013 sa konalo zasadnutie EÚ, kde „vedúci predstavitelia EÚ rokovali v rámci tematického zasadnutia o tom, že je potrebné, aby digitálne hospodárstvo EÚ opäť získalo dynamiku, ako aj o význame digitálnej inovácie pre rast a konkurencieschopnosť.“[4] Sektor IT v súčasnosti predstavuje oblasť, ktorý ponúka pracovné miesta a nadpriemerné mzdy, čo viedlo k tomu, že „zamestnanosť v januári 2014

[2] Citované: Kokles, M., Romanová, A. 2010. *Informatika*. 6. vydanie. Bratislava : Sprint dva, 2010. s. 120-121. ISBN 978-80-89393-14-5

[3] Spracované podľa: Kokles, M., Romanová, A. 2010. *Informatika*. 6. vydanie. Bratislava : Sprint dva, 2010. ISBN 978-80-89393-14-5

[4] Citované: Európska rada. 2013. *Európska rada: zaostrené na digitálne hospodárstvo.* [online] 2013. [cit. 13.05.2014]. Dostupné na internete: <http://www.european-council.europa.eu/home-page/highlights/european-council-focus-on-the-the-digital-economy?lang=sk>

v porovnaní s januárom 2013 vzrástla v informačných a komunikačných činnostiach o 4,3 %.“[5]

Svet bez IT si dnes už priemerný bežný človek dokáže predstaviť len ťažko. V budúcnosti však ich význam bude ešte pravdepodobne narastať, na čo budú mať vplyv nielen inovácie a ich prispôsobovanie ľudským potrebám a požiadavkám, ale aj preto, lebo si čoraz lepšie uvedomujeme a objavujeme možnosti ich využitia.

Medzi najvýznamnejšie trendy súčasnosti, ktoré budú v najbližších rokoch pokračovať a rozmáhať sa, patrí najmä cloud computing či big data, ktoré podnikom umožňujú lepší prístup k informáciám, komplexnejšie informácie a zníženie nákladov, využívané sú najmä podnikmi strených veľkostí. Ďalším obrovským trendom sú sociálne médiá, kam patria napríklad blogy, multimédiá, no najväčší potenciál však majú sociálne siete. V posledných obdobiach bol zaznamenaný pokles predaja „klasických“ počítačov, čo je spôsobené najmä tým, že ľudia začínajú uprednostňovať tablety, smartfóny a iné jednoducho prenosné zariadenia, a zatiaľ všetko naznačuje, že tento trend bude pokračovať aj naďalej.

Predpokladá sa tiež rozšírenie bezdotykových zariadení, ktoré sa budú ovládať napríklad gestami či hlasom. Niektorí odhadujú, že sa na trh za pár rokov dostanú napríklad „produkty, ktoré umožnia bezdrôtovo dobíjať zariadenia.“[6] Mnohí sa zhodujú v tom, že IT budú vo väčšine bežných vecí, ako napríklad autá či oblečenie. Virtuálna realita bude tiež realistickejšia, napríklad sa už niektorým vedcom podarilo vytvoriť ultrazvukové vlny, vďaka ktorým získava človek pocit, že sa veci dotýka.[7]

1.3 Riziká informačných technológií

Napriek mnohým výhodám, ktoré so sebou prinášajú, sa s IT spájajú mnohé riziká. Na jednej strane napomáhajú či dokonca umožňujú predchádzať niektorým rizikám, znižovať ich alebo ich kvantifikovať. Na druhej strane však so sebou prinášajú nové riziká a iné zase prostredníctvom nich nadobúdajú väčšie rozmery, v niektorých prípadoch doposiaľ nevídané, rozmery, ako napríklad kyberterorizmus. Treba si však uvedomiť, že

[5] Citované: TASR. 2014. V IT činnostiach stúpla v januári zamestnanosť medziročne o 4,3%. [online] 2014. [cit. 13.05.2014]. Dostupné na internete: < http://www.zive.sk/clanok/72951/v-it-cinnostiach-stupla-v-januari-zamestnanost-medzirocne-o-4-3>

[6] Citované: Valášek, M. 2011. Blízka a vzdialená budúcnosť IT. In *TRENDsk.* [online] 2011. [cit. 13.05.2014]. Dostupné na internete: <http://technologie.etrend.sk/it-biznis/blizka-a-vzdialena-buducnost-it-2.html>

[7] Spracované podľa: IT NEWS: 2014. Ďalší krok k realistickejšej virtuálnej realite. Technológia Ultragraphics umožní „dotknúť“ sa virtuálnych predmetov. In *IT NEWS.I.* [online] 2014. [cit. 14.05.2014]. Dostupné na internete: <http://www.itnews.sk/spravy/startupy/2014-05-02/c162970-dalsi-krok-k-realistickejsej-virtualnej-realite.-technologia-ultrahaptics-umozni-dotknut-sa-virtualnych-predmetov>

veľkosť rizík spájajúcich sa s IT ovplyvňujeme i my a paradoxne tieto riziká narastajú s rozvojom IT. Je to dané najmä tým, že s ich rozvojom sa síce rozširujú možnosti ich využívania, ale tým narastá aj ich komplexnosť a tá má za následok rozmáhanie sa rizík IT. V dnešnej spoločnosti sa IT využívajú hromadne, a tým tiež rastú aj možnosti prenášania a rozširovania týchto rizík aj ich dôsledkov. Problematika IT rizík sa zvyšuje aj tým, že sa stávajú čoraz viac systémovými.

Pojem riziko má rôzne definície, ktoré závisia najmä od pohľadu, z akého ho vnímame. Vo všeobecnosti je najčastejšie uvádzané ako možnosť odchýlky od očakávanej či strednej hodnoty alebo pravdepodobnosť nastania nejakej udalosti a jej možných alternatív. „V poistení sa riziko zvyčajne chápe ako pravdepodobnosť vzniku náhodnej udalosti s negatívnymi vplyvmi na ekonomický subjekt, teda ako funkcia pravdepodobnosti výskytu a veľkosti škodových následkov, ako súčin pravdepodobnosti vzniku nežiaducej udalosti a jej následkov.“[8]

V podnikoch sú informačné technológie veľmi dôležité. Možno povedať, že IT vytvárajú informačné systémy. Tie tvoria podstatnú časť informačno-komunikačných systémov, nehovoriac o tom, že dnes sú komunikačné systémy závislé od informačných. „V súvislosti s informačno-komunikačnými systémami a ich bezpečnosťou je dôležitý pojem informačno-komunikačné aktívum. Je to hmotný alebo nehmotný objekt, ktorý sa podieľa na fungovaní a vytváraní daného ICS. Informačno-komunikačné aktíva je možné rozdeliť do troch hlavných skupín:

- údajové a dokumentačné aktíva, t.j. databázy a dátové súbory, údaje a informácie, systémová dokumentácia, užívateľské manuály, prevádzkové procedúry, dohody o náhradných postupoch používaných v prípade zlyhania poskytovaných služieb alebo systému, archivované informácie. Dátové štruktúry predstavujú najväčšiu hodnotu ICS. Ich strata je ťažko vyčísliteľná, ich hodnota sa môže v závislosti od času výrazne meniť;
- softvérové aktíva, t.j. aplikačný softvér, systémový softvér, vývojové nástroje a pomocné programy, zdrojové knižnice a knižnice vykonateľných programov;
- fyzické aktíva, t.j. počítačové vybavenie (procesory, monitory, modemy, laptopy a pod.), komunikačné vybavenie (routre, faxové zariadenia a pod.) magnetické

[8]Citované: Majtánová, A. a kol. 2006. *Poisťovníctvo*. Bratislava : Iura Edition, 2009. s. 52. ISBN 978-80-8078-2060-3

médiá (pásky, diskety, HDD), iné technické vybavenie (napájacie zdroje, klimatizačné jednotky, UPS), nábytok a podobne.“[9]

IT šetria čas, prácu, náklady, podporujú podnikateľské možnosti, kvalitu služieb poskytovanú zákazníkom. A preto sa čoraz viac spoločností pokúša zavádzať do svojich výrobných procesov. Každá výhoda má však aj svoje nedostatky, a to platí aj pre IT, ktorých riziká narastajú.

Vzhľadom na to, že rizík spájajúcich sa s IT je nespočetne veľa, počnúc zdravotnými, cez environmentálne až po riziká kybeterorizmu, ja sa zameriam na tie riziká, ktoré ohrozujú podnikateľské subjekty a môžu im spôsobiť škody. Takmer všetky tieto hrozby možno rozdeliť do troch kategórií, a to: prírodné živly, technické poruchy a ľudskú činnosť. Do prvej možno zaradiť napríklad zemetrasenie, záplavy či požiar. Ak niektorý z nich nastane, často dochádza strate, tiež k poškodeniu hardvéru, ktorý máva v podnikoch vysokú hodnotu, ale aj strate údajov, ktoré sú na ňom uložené. Hrozbou môže byť napríklad aj slnečná búrka, ktorá môže spôsobovať poruchy elektroniky, výpadky elektrického prúdu.

Medzi technické poruchy, ktoré ohrozujú IT najviac, patrí výpadok elektrického prúdu. Dnes je už mnoho IT zariadení schopných fungovať aj bez dočasného prísunu tejto energie, avšak z dlhodobejšieho hľadiska bez nej nepoužiteľné. Ešte horšie je to vo firmách, ktoré pracujú s vysoko výkonnými aparátmi, pri ktorých aj krátkodobý výpadok prúdu môže narušiť ich činnosť, keďže sú od neho závislé.

Najväčšiu skupinu ohrození súvisiacich s IT tvorí ľudská činnosť. Tá môže byť úmyselná alebo neúmyselná. Neúmyselná ľudská činnosť je vo väčšine prípadov spôsobená ich nedbalosťou, patrí sem napríklad neúmyselné poškodenie hardvéru či jeho strata, ale aj vymazanie údajov alebo ich poskytnutie nežiadanej osobe či osobám, umožnenie vniknutiu malvéru do zariadenia, chyby pri výrobe alebo inštalácii, etc.

Do úmyselnej činnosti človeka patrí počítačová kriminalita, niekedy označovaná aj ako kybernetická kriminaliata. Počítačovou kriminalitou sa zvyčajne rozumejú trestné činy, ktoré sú páchané prostredníctvom IT, najmä počítačov, alebo sú proti nim zamerané. „Patria sem najmä trestné činy ekonomickej povahy (hospodárska kriminalita), ako sú napríklad podvody, krádeže, počítačová sabotáž alebo nedovolený prienik do počítačových sietí ak chráneným údajom (penetrácie). Rovnako sem zaraďujeme aj trestné činy útočiace

[9] Citované: Krátka, Z. 2007. Poistiteľnosť rizika informačných a komunikačných systémov. [online] 2007. [cit. 08.05.2014]. Dostupné na internete: <http://maag.euba.sk/documents/PoistitelnostrizikaICS_konferenciaKPOI2007.pdf>

na súkromie jednotlivca (pozmenenie osobných údajov, použitie nepravdivých údajov, nelegálny zber alebo zneužitie osobných údajov).“[10]

1.4 Vybrané riziká informačných technológií

Riziká spájajúce sa s IT sú veľmi početné, sú ovplyvnené mnohými faktormi, a bude ich ešte viac. Ja preto v tejto časti budem charakterizovať práve tie, ktoré sú najväčšie a špecifické pre túto oblasť.

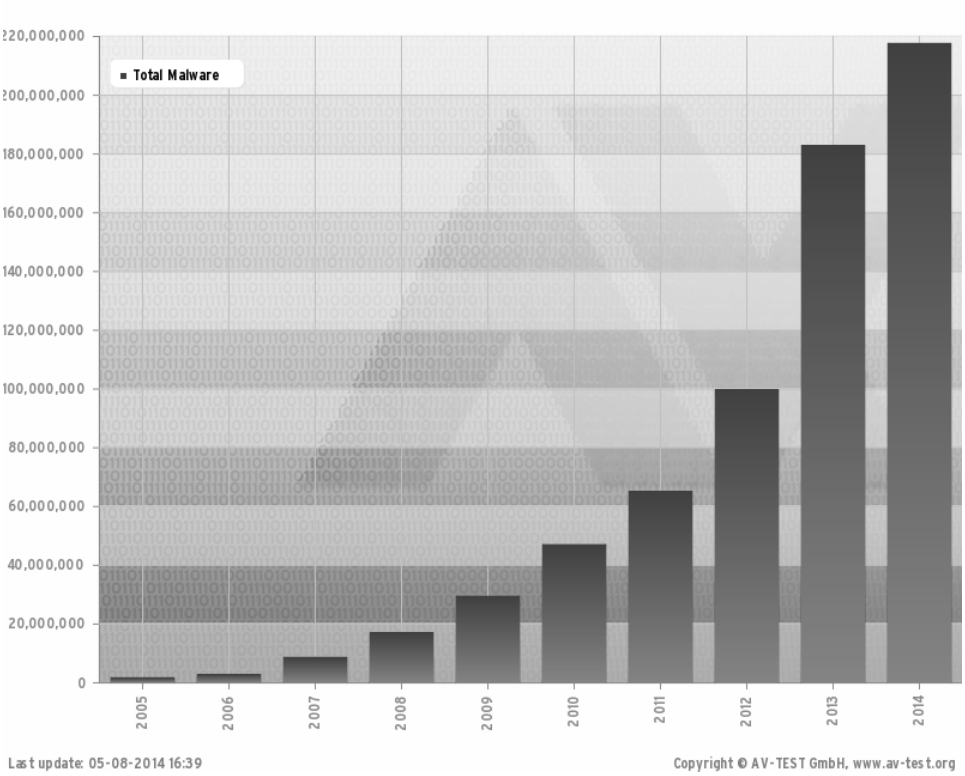
K najväčším rizikám možno zahrnúť kybernetické útoky. Pod pojmom kybernetický útok môžeme chápať útok prostredníctvom informačných technológií, predovšetkým na informačné systémy, počítačové siete či osobné prístroje (napr. notebook). Dôvody konania sú rôzneho charakteru, môžu to byť náboženské motívy, vízia zisku, politické účely, teroristické účely, krádež údajov, pomsta, dokazovanie vlastných schopností, poukazovanie na nedostatky alebo chyby v systémov, etc.[11]

Kybernetické útoky spôsobujú najmä malvéry. Malvér (angl. malicious software, čiže škodlivý softvér) môže byť program alebo kód, ktorý sa dokáže dostať do informačného systému, aby tam spôsoboval škody alebo vykonával či iné činnosti, ktoré nie sú v záujme používateľa. Dnes existuje veľa druhov malvéru, patria sem napríklad vírusy, červy a Trójske kone.

[10] Citované: Ördögh, P. 2014. Čo je to: Počítačová kriminalita a počítačové pirátstvo na Slovensku. In *PENonline.* [online] 2014. [14.05.2014]. Dostupné na internete: <http://www.penonline.sk/analyzy/co-je-co-pocitacova-kriminalita-a-pocitacove-piratstvo-na-slovensku#edn6>

[11] Zuzčák, M. 2011. Kybernetickí útočníci, ich motívy a filozofia. In *SecIT.sk* [online]. 2011. Dostupné na internete: <http://www.secit.sk/sk/content/kyberneticki-utocnici-ich-motivy-filozofia>

Graf 2 **Celkový počet malvérov**



Zdroj: The Independent IT-Security Institute. 2014. Malware. [online] 2014. [cit 09.05.2014] <http://www.av-test.org/en/statistics/malware/>

K najstarším druhom malvéru patria vírusy. „Počítačový vírus je malý softvérový program, ktorý sa šíri medzi počítačmi a ovplyvňuje ich činnosť. Počítačový vírus môže poškodiť alebo odstrániť údaje z počítača, použiť e-mailový program na vlastné šírenie do iných počítačov alebo dokonca odstrániť všetky údaje na pevnom disku.“[12] Dôležitým znakom týchto vírusov je, že podobne ako biologické vírusy tiež potrebujú na šírenie „hostiteľa“, ktorým môže byť nejaký program či dokument. Šíria sa prostredníctvom internetu, pamäťových zariadení, emailov, etc.

Červy sú malvéry podobné vírusom. Za hlavný rozdiel sa pokladá to, že červy sa dokážu šíriť a rozmnožovať bez toho, aby sa museli pripájať na nejaký hostiteľský program. V ich prípade ide v mnohých prípadoch o necielenú infiltráciu. Červy sa šíria cez siete, v ktorých využívajú ich nedokonalosti na to, aby posielali svoje kópie do iných systémov.

Trójske kone sú najpočetnejšie malvéry a na rozdiel od vírusov a červov sa sami nešíria. Trójsky kôň je program, ktorý sa maskuje za obyčajný nevinný program. Úlohou

[12] Citované: Microsoft. 2013. Prevencia a odstraňovanie vírusov a ďalšieho malvéru. [online] 2013. [cit. 09.05.2014]. Dostupné na internete: <http://support.microsoft.com/kb/129972/sk>

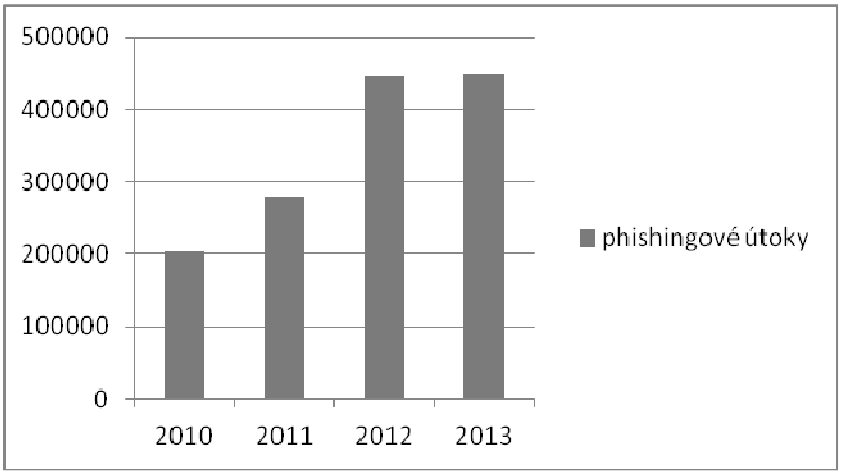
býva väčšinou dostať sa do systému, kam si ich nič netušiaci používateľ stiahne, aby tam spôsobili škodu alebo získavali osobné či tajné informácie. Existuje mnoho typov trójskych koní. Najrozšírenejšie a najnebezpečnejšie sú Remote access trojans, ktoré umožňujú útočníkovi získať úplnú kontrolu nad napadnutým prístrojom. Ten tak má voľný prístup ku všetkým súborom, finančným účtom, súkromným konverzáciám, etc. K tomuto typu patria aj tzv. zadné vrátka. Ďalšou skupinou sú deštruktívne trójske kone, v napadnutom systéme vymazávajú a ničia súbory. Do tejto skupiny patria aj tzv. logické bomby, ktoré sú natavené tak, aby sa spustili v určitom čase. Niektoré trójske kone môžu znefunkčňovať ochranné systémy či byť zdrojom ďalších malvérov. Data-sending trójske kone tvoria skupinu, ktorá posiela útočníkovi heslá k účtom, rôzne dôverné informácie. Niektoré trójske spôsobujú DoS (denial of service) útoky.[13]

Podobné DoS útokom sú DDoS (distributed denial of service), čiže distribuované útoky na odmietnutie služieb. Základný rozdiel medzi DoS a DDoS spočíva v tom, že DoS útoky vyvoláva jeden počítač, kým DDoS sú útoky spôsobované botnetmi. Botnety sú siete „botov“, čo sú „nakazené“ počítače, ktoré na diaľku ovláda jeden centrálny server. Takéto útoky znefunkčňujú servery tým, že posielajú obrovské množstvá požiadaviek, ktoré preťažia sieť. Zabraňujú oprávneným osobám k službám či informáciám, zvyčajne je to inernetbanking, email, internet, etc.[14]

Jednou z jeho v súčasnosti najznámejších foriem sociálneho inžinierstva je phishing. Voľne sa často prekladá ako rybárčenie. „Phishing je druh internetového podvodu, ktorým sa podvodníci snažia získať prístupové údaje k cudziemu internetovému bankovníctvu s cieľom zneužiť ich pre svoje vlastné obohatenie. Podvodník sa môže snažiť vylákať napríklad informácie ako číslo karty, kód nad magnetickým prúžkom, tzv. CVV/CVC ochranný kód, ďalej napríklad prístupové údaje do internetového bankovníctva (identifikačné číslo, heslo či iné bezpečnostné údaje). K získaniu týchto dôverných informácií využívajú podvodné e-maily, ktoré na prvý pohľad vzbudzujú dojem, že sú odosielané priamo z e-mailovej adresy vašej banky. Správa obsahuje odkaz na internetové stránky, kde od vás budú požadované osobné bezpečnostné údaje.“[15]

[13] Spracované podľa: GFI Software. 2011. *The corporate threat posed by email trojans.* [online] [08.05.2014]. Dostupné na: <http://www.gfi.com/whitepapers/network-protection-against-trojans.pdf>
[14] Spracované podľa: Prolexic. *What is denial of service*. In PLXportal [online] [13.05.2014]. Dostuné na internete: <http://www.prolexic.com/knowledge-center-what-is-ddos-denial-of-service.html>
[15] Citované: Šenkýřová, L. 2013. *Čo je PHISHING alebo ako sa nestať obeťou podvodníkov.* In *Financesk* [online] 2013. [cit. 12.05.2014]. Dostupné na internete: <http://www.finance.sk/spravy/finance/109628-co-je-phishing-alebo-ako-sa-nestat-obetou-podvodnikov/>

Graf 3 **Medziročný nárast phishingu**



Zdroj: EMC Corporation. 2014. RSA Monthly Online Fraud Report. [online] 2014. [12.05.2014] <http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf>

Pharming, čiže „farmárčenie“, možno považovať za vylepšenú formu phishingu. Je to tiež spôsob na získanie citlivých informácií. „Pharming je založený na zmene DNS (Domain Name System) položiek. Užívateľ navštívi web stránky, ktoré nie sú originálnymi, ale falošnými stránkami banky. Tie vytvorili hackeri, ktorí chcú získať dôverné údaje. Dizajn stránok je podobný alebo skoro rovnaký ako oficiálna stránka banky. Návštevník stránky preto ani nemusí zistiť, že má otvorenú falošnú web stránku.“[16]

Ďalšou významnou hrozbou je únik a strata informácií. Informácie sú dnes v oblasti podnikania najvýznamnejším aktívom, a tak je ich bezpečnosť mimoriadne dôležitá. Ich strata či poškodenie môže mať na podniky veľmi ničivé dôsledky, pretože okrem nákladov na opätovné získanie informácií spôsobuje aj zníženie produktivity, ušlý zisk, únik ohrozuje povesť firmy, duševné vlastníctvo, spôsobuje pokles cien akcií, etc., ba v horších prípadoch môže viesť dokonca ku koncu podnikania. „Príkladom zo začiatku marca je obchodný reťazec Morrison Supermarkets, ktorý patrí medzi štyri najväčšie v Británii. Išlo o interný únik, došlo k odcudzeniu dát o viac ako 100 000 zamestnancoch, boli to informácie o mzdách, adresy a čísla bankových účtov. Spoločnosť musí zaplatiť pokutu za zlú ochranu citlivých dát, zamestnanci budú za ujmu finančne odškodnení. Navyše od uverejnenia in-

[16] Citované: Slovenská sporiteľňa. *Chráňte svoje peniaze bezpečným používaním služieb elektronického bankovníctva.* [online] [cit. 12.05.2014]. Dostupné na internete: <http://www.slsp.sk/vseobecne-bezpecnostne-pravidla-pri-praci-s-internetom-a-sluzbou-internetbanking.html>

formácií došlo k poklesu ceny akcií spoločnosti o 11 %. Len jeden zamestnanec tak spôsobil firme obrovskú finančnú stratu.“[17]

K úniku či strate informácií môže dôjsť mnohými spôsobmi. Najčastejším je hacking, ktorý na získanie informácií využíva nedostatky sietí. Niektoré údaje majú organizácie uložené na výmenných pamäťových médiách či v notebookoch, tieto sa môžu napríklad stratiť, zničiť alebo ukradnúť a spolu s nimi aj informácie. Ďalším zdrojom úniku alebo straty sú zamestnanci, tak externí ako aj interní. Dôvody ich konania sú rôzne, veľakrát je to finančné obohatenie, pomsta alebo i neúmyselné vyzradenie či odoslanie senzitívnych informácií. Ďalšími, i keď zriedkavejšími, príčinami dôvodu straty údajov sú softvérové chyby, ktoré môžu byť spôsobené napríklad zlou inštaláciou, zlým programom, ale aj zlyhanie pamäťových médií, najmä ak sú zastarané.[18]

1.5 Reakcia na riziko

Všetky subjekty patriace do ekonomickej sféry sú ohrozované rizikami IT. Množstvo týchto rizík svet ešte nepozná, avšak pri známych rizikách by sa mala správne posúdiť pravdepodobnosť ich nastania a ich potenciálne dôsledky, aby bolo možné určiť vhodný postup reakcie.

Niektoré riziká IT sú dostatočne malé na to, aby ich subjekty prijali a znášali bez nákladnejších opatrení. Ak napríklad v podniku dôjde k strate USB kľúča, na ktorom neboli uložené citlivé informácie, alebo sa pokazí tlačiareň, tak to môže spôsobiť škody, ale nie dostatočne veľké na to, aby podnik zanikol, mal závažné finančné problémy či ujmu na svojom mene. Pravdepodobnosť nastania takýchto udalostí je tiež dostatočne malá a na jej prevenciu zvyčajne postačuje vhodná opatrnosť a pravidelné kontroly.

Iné riziká sú väčšie a môžu spôsobovať podnikom vážne škody a problémy, ba dokonca môže dôjsť ku krachu podniku a koncu jeho podnikania, a preto na ne musia reagovať v dostatočnej miere. Proti krádeži hardvéru to môžu byť napríklad bezpečnostné zámky, kamerové systémy, v niektorých i kontrola zamestnancov, prípadne sa na trhu ponúkajú aj rôzne softvéry na ich vypátranie.

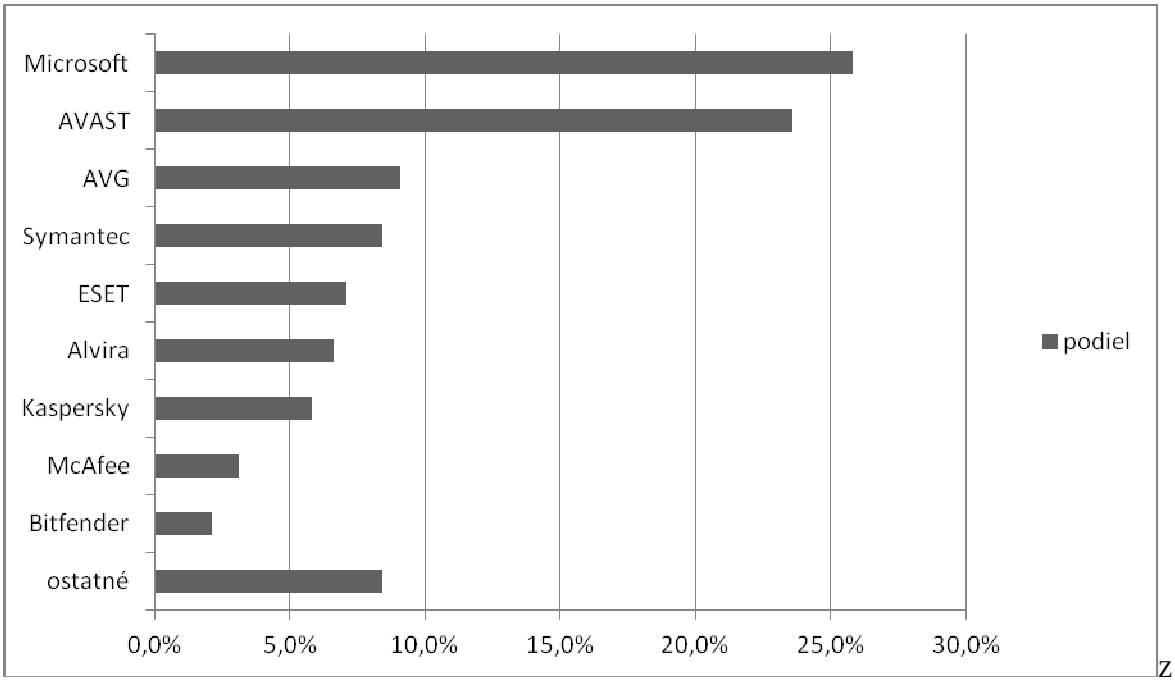
[17] Citované: Ryba, A. 2014. *Únik firemných dát môže spôsobiť prepad cien akcií.*[online] 2014. [cit. 13.05.2014]. Dostupné na internete: <http://www.itnews.sk/spravy/bezpecnost/2014-03-31/c162377-unik-firemnych-dat-moze-sposobit-prepad-cien-akcii>

[18] Spracované podľa: 2014. Ochrana osobných údajov: Ďalší strašiak pre firmy. In *Revue Priemyslu.* [online] 2014. [16.05.2014]. Dostupné na internete: <http://www.revuepriemyslu.sk/stories/clanok/aid/22956/Ochrana_osobn%C3%BDch_%C3%BAdajov/%C4%8Eal%C5%A1%C3%AD_stra%C5%A1iak_pre_firmy>

Ochrana voči výpadkom elektrickej energie je komplikovanejšia, napríklad záložné zdroje elektrickej energie ako generátory pre pokračovanie v prevádzke či pravidelné ukladanie spracovaných dát, aby sa predišlo k ich strate.

Na ochranu pred kybernetickými útokmi sa odporúča vyhýbať sa rizikovým serverom, používať iba overené a licencované softvéry a aktualizovať ich, nepoužívať cudzie pamäťové nosiče, pretože na nich môže byť malvér, používať firewall. Častým prostriedkom sú aj antivírusové programy, ktoré dnes ponúka mnoho spoločností.

Graf 4 **Globálny trh výrobcov antivírusových programov**



Zdroj: The Statistics Portal. 2014. Global market share held by the leading Windows antivirus application vendors in August 2013. [online] [cit. 16.05.2014]. Dostupné na internete: <http://www.statista.com/statistics/271048/market-share-held-by-antivirus

Antivírusové programy však poskytujú iba pasívnu formu ochrany a dnes už nepostačujú. Bezpečnosť by mala byť proaktívna, a tak mnoho firiem vyvíja nové produkty. „Pre firmy by sa potom mali výrazne rozšíriť služby „etického hackovania", kde by im bezpečnostné firmy ponúkali vlastné tímy fingovaných útočníkov, ktorí by sa pokúsili napadnúť firemné siete a odhaliť tak možné diery. Najmä úniky dát spôsobené prelo-

mením ochrany siete sú v posledných rokoch postrachom prakticky všetkých firiem, ktoré podnikajú na internete. A straty spojené s takýmto únikom sú astronomické.“[19]

Avšak sú aj riziká, ako napríklad zemetrasenie, pred ktorými sa nedá efektívne chrániť. Ich pravdepodobnosť býva malá, škody veľké a náklady na prevenciu vysoké. Na ochranu pred takýmito rizikami je najvýhodnejší ich prenos na iný subjekt, ktorého najfrekventovanejšia forma je poistenie.

[19] Citované: Ryba, A. 2014. *Klasické antivírusy sú už odpísané a neplnia svoj účel.* [online] 2014. [cit. 14.05.2014]. Dostupné na internete: <http://www.itnews.sk/spravy/bezpecnost/2014-05-07/c163053-symantec-klasicke-antivirusy-su-uz-odpisane-a-neplnia-svoj-ucel>

2 Cieľ práce, metódy práce a metodika skúmania

Informačné technológie ovplyvňujú prostredie ľudí z roka na rok čoraz viac a prinášajú so sebou mnohé riziká, a preto hlavným cieľom mojej bakalárskej práce je identifikovať súčasné riziká, ktoré súvisia s informačnými technológiami a najmä poskytnúť čitateľovi prehľad o možnostiach ich poistenia v Slovenskej republike aj v zahraničí.

Pre dosiahnutie hlavného cieľa práce je potrebné splnenie niekoľkých čiastkových cieľov. Prvým čiastkovým cieľom je oboznámenie čitateľa o metódach, ktoré som najviac využívala pri vytváraní tejto práce. Ďalším parciálnym cieľom mojej práce je poskytnúť čitateľovi základné informácie o informačných technológiách súčasnosti. Tiež vytýčim základné typy rizík, ktoré sa s nimi spájajú, ale aj bližšie predstavím tie ohrozenia, ktoré sa najviac prejavujú v súčasnom svete. Čiastkovým cieľom je predstavenie možností ako na riziká informačných technológií, ktoré na svoje prostredie pôsobia, reagovať aj niektoré možnosti prevencie proti nim.

Ďalším parciálnym cieľom bude aj poukázanie na najvýznamnejšie problémy súvisiace s poistiteľnosťou rizík IT, ktoré sú dané najmä ich povahou, a následne je nízka ponuka poistných produktov týchto rizík.

Posledným parciálnym cieľom tejto práce je predstavenie súčasnej situácie na trhu poistenia rizík, ktoré so sebou prinášajú informačné technológie. Najprv uvediem najvýznamnejšie možnosti tohto poistenia v Spojených štátoch amerických, kde je problematika rizík informačných technológií na riešená na oveľa lepšej úrovni než u nás. V poslednej časti poskytnem pohľad na situáciu poistiteľnosti týchto rizík na Slovensku.

Pri vypracovávaní svojej bakalárskej práce som používala rôzne metódy. Patrí k nim predovšetkým štúdium odbornej literatúry, ktorú som získavala predovšetkým z kníh a internetu, odkiaľ som získala mnoho cenných údajov.

Medzi metódy, ktoré som využívala najviac aj patrí pozorovanie. Táto metóda je založená na vnímaní predmetu alebo javu riešeného problému. Mnohokrát sú pri nej využívané získané skúsenosti a empirické poznatky. Často býva súčasťou iných metód, ktoré by bez nej boli nepoužiteľné.

Tiež som využívala indukciu. Ide o metódu, výsledkom ktorej je všeobecne platný záver vyvodený na základe poznatkov o konkrétnych javoch. Indukcia teda umožňuje prechod od jednotlivých úsudkov k všeobecným tvrdeniam.

Metóda indukcie sa často dopĺňa s metódou dedukcie, ktorú som v práci používala tiež. Dedukcia je spôsob, pri ktorom sa od všeobecných tvrdení, úsudkov a hypotéz prechádza k záverom, ktoré sú špecifické, zvláštne. Všeobecne platné, známe a overené závery sú pri tejto metóde aplikované na jednotlivé skúmané prípady.

Ďalšou metódou bola abstrakcia, pri ktorej sa odhliada od nepodstatných znakov rôznych javov pozornosť sa sústreďuje na ich vyčlenené špecifické vlastnosti. Opakom abstrakcie je konkretizácia, ktorú som využívala tiež. Hlavnou výhodou konkretizácie je možné spresnenie, pričom sa prejavuje najmä príkladmi.

Využívala som tiež analýzu a syntézu. Pri analyzovaní javov dochádza k ich rozčleňovaniu na jednotlivé časti, aby sa umožnilo lepšie posudzovanie. Syntéza je zase postup, pri ktorom spájame jednotlivé časti či vzťahy medzi javmi, čím sa zase umožňuje poznávať súvislosti medzi nimi a nahliadnuť na ich vnútornú štruktúru.

3 Výsledky práce a diskusia

Ekonomické subjekty majú záujem o poistenie rôznych rizík, medzi ktoré patria aj riziká súvisiace s IT. Existuje však niekoľko dôvodov, pre ktoré nie sú všetky poisťovne ochotné poskytovať poistné krytie na tieto riziká.

3.1 Poistiteľnosť rizík informačných technológií

„Poistenie je vzťah medzi dvoma zmluvnými stranami, pri ktorom je jedna zmluvná strana, tá, ktorá poisťuje za to, že dostáva poistné ochotná odškodniť druhú zmluvnú stranu (poisteného) v prípade vzniku poistnej udalosti (strata, škoda, dožitie sa veku) v súlade s dohodnutými podmienkami.“[20]

Pre možnosť poistenia rizík IT je teda potrebné, aby bola na trhu aj jeho ponuka, a dopyt po ňom. Najväčší nárast záujmu o poistenie rizík IT boli zaznamenané zo strany podnikateľov, ktorých môžeme rozdeliť na tri skupiny:

- „užívatelia IT, ktorí majú predovšetkým záujem o krytie strát vzniknutých prerušením prevádzky a nákladov na opätovné zabezpečenie dát a pod.,
- poskytovatelia služieb (softwarové firmy, systémoví integrátori, servisné organizácie, outsourcingové firmy), ktorí majú záujem o krytie škôd spôsobených obchodným partnerom a klientom z titulu zodpovednosti za poskytované služby a pod.,
- poskytovatelia služieb na vlastných serveroch, ktorí majú záujem jednak o krytie vlastných škôd, jednak o krytie škôd u tretích osôb (klientov) z titulu zodpovednosti.“[21]

Napriek dopytu po poistení rizík IT bol tento druh poistení dlhý čas ťažko dostupný. Dôvodom bol samotný charakter rizík IT. Poisťovne totiž nepreberajú všetky riziká, ale posudzujú ich podľa kritérií poistiteľnosti. „Aby poisťovne vôbec mohli uvažovať o poistnom krytí niektorých rizík, musia tieto riziká spĺňať určité podmienky, bez splnenia ktorých by boli tieto riziká neprijateľné a teda nepoistiteľné. Poistiteľné riziká musia spĺňať nasledujúce podmienky:

- identifikovateľnosť

[20] Citované: Majtánová, A. a kol. 2006. *Poisťovníctvo*. Bratislava : Iura Edition, 2009. s.35 . ISBN 978-80-8078-2060-3

[21] Citované: Krátka, Z. 2007. *Poistiteľnosť rizika informačných a komunikačných technológií.* [online] 2007. [cit. 11.05.2014]. Dostupné na: <http://maag.euba.sk/documents/PoistitelnostrizikaICS_konferenciaKPOI2007.pdf>

- náhodnosť,
- vyčísliteľnosť,
- ekonomická únosnosť.“[22]

Prvou podmienkou pre poistiteľnosť je identifikovateľnosť. Riziko musí byť presne definované, ohraničené. A to je jeden zo základných problémov pri poistení informačných technológií. Možno povedať, že IT sú záležitosťou len niekoľkých desaťročí, ale ich vývoj je prudký, platí to najmä pre internet a veci s ním súvisiace. Oba tieto fakty vedú k záveru, že dodnes je táto oblasť nedostatočne prebádaná, ťažko ovplyvniteľná, vývoj je tu tiež ťažko predvídateľný, stále sa vynárajú nové a nové riziká. Množstvo rizík je dnes už známe, naďalej sú však ťažko predvídateľné a často sa navzájom podmieňujú a súvisia. Jednou z najpoužívanejších spôsobov, ako sa zbaviť niektorého z týchto „nedostatkov“, sú výluky. Takéto výluky v poistných zmluvách sú však tiež jedným z faktorov, ktoré bránili rozmachu poistenia rizík IT.

Ďalším dôvodom je aj hmlistosť v oblasti niektorých pojmov, ktoré sa bežne používajú nesprávne. Trendom v tomto smere je postupné objasňovanie aj v tejto oblasti, keďže sa s nimi často pracuje. Problém však predstavuje neexistencia definície niektorých termínov. Okrem čisto technických chýba presné vymedzenie aj celkom bežných výrazov v zákonoch. Celosvetovo je to síce tiež na ceste k lepšiemu, u nás však ešte stále nie je definovaných ani mnoho bežných termínov ako napríklad počítačová kriminalita.

Na to aby riziko spĺňalo podmienku identifikovateľnosti, musí byť analyzovateľné z hľadiska veľkosti frekvencie jeho výskytu. S tým je tiež problém, pretože poisťovne ani rôzne štatistické orgány nie sú schopné sami zistiť či s vysokou presnosťou určiť celkový rozsah a frekvenciu výskytu týchto rizík, a subjekty využívajúce IT často z mnohých dôvodov, napríklad ak podniky nechcú stratiť svoju dôveryhodnosť, nie sú ochotné tieto údaje zverejňovať. Na druhej strane, riziká súvisiace s IT si začínajú viac uvedomovať obe strany, a tak sa prístup k týmto údajom stáva jednoduchším a štatistiky a ich spracovávanie dômyselnejšie. Potrebu takéhoto zaznamenávania si začínajú uvedomovať aj vlády, napríklad v Českej republike začne v roku 2015 platiť zákon, podľa ktorého „firmy, štátna správa a inštitúcie budú musieť povinne hlásiť bezpečnostní incidenty v ich IT

[22] Citované: Littvová, Z. – Marko, P. – Vachálková, I. 2012. *Riziko v poisťovníctve*. Bratislava : Ekonóm. s. 24. ISBN 978-80-225-3385-0

infraštruktúrach jednej centrále (čiže NBÚ).“[23] Tieto informácie sú pre poisťovne dôležité, pretože na ich základe sa tvoria sadzby poistného.

Riziká, ktoré sú predmetom poistenia, musia vyť náhodné. „Aby mohlo byť nejaké riziko poistiteľné, musí sa náhodnosť prejaviť buď v neurčitosti jeho výskytu, teda či daná udalosť vôbec nastane alebo nie, prípadne ak je isté, že daná udalosť nastane, tak sa neurčitosť musí prejaviť v čase.“[24] Zatiaľ sa predpokladá, že riziká IT túto podmienku spĺňajú. Existuje tu síce dosť vysoká asymetria informácií, túto podmienku však spĺňajú. Problém môže byť však v tom, že zatiaľ ešte nie sú veľmi dobre preskúmané podmienky nastania takýchto udalostí, na druhej strane však v poslednom období nastal veľký posun aj v tejto oblasti.

Platí tiež, že škody, ktoré vzniknú subjektom realizáciou nejakého rizika IT, musia byť vyčísliteľné. Napríklad pri krádežiach či poškodení hardvéru ako napríklad tlačiarne či monitory, nie je veľmi problematická vyčísliteľnosti škôd, avšak pri pamäťových médiách s informáciami je to komplikovanejšie. To je ďalší dôvod problematickej poistiteľnosti rizík. IT Straty, ktoré vzniknú nastaním rizík IT, často nemajú fyzický charakter. Ak napríklad dôjde k strate, krádeži či poškodenia prenosného pamäťového média, hlavná strata sa netýka samotného zariadenia, ale informácií, ktoré na ňom boli. V prípade ich straty, krádeže či poškodenia môžu nastať obrovské škody, ktoré sa však nie vždy dajú správne, jednoznačne a objektívne určiť. Ich správny odhad sťažuje aj nedostatok empirických, historických údajov. Problém vyčísliteľnosti strát súvisí aj so vzájomným prepojením informačných systémov. Napríklad „incident v sieti jednej firmy môže negatívne ovplyvniť funkčnosť siete inej spoločnosti. Táto skutočnosť sťažuje definovanie rozsahu poistného krytia v prípade nastania incidentu.“[25]

Jednou z hlavných nevýhod poistenia je aj morálny hazard. Morálny hazard možno charakterizovať ako riziko, že po tom, ako sa poistník poistí, začne sa správať takým spôsobom, ktorý môže viesť k tomu, že vzrastie riziko vzniku danej poistnej udalosti. Pri rizikách súvisiacich s IT predstavuje toto riziko ešte väčšiu hrozbu, pretože dôsledky

[23] Citované: Sedlák, J. 2014. Firmy budou muset hlásit kybernetické útoky. Hrozi jim pokuta. In *E15* [online] 2014. [cit. 12.05.2014]. Dostupné na internete: <http://e-svet.e15.cz/it-byznys/firmy-budou-muset-hlasit-kyberneticke-utoky-hrozi-jim-pokuta-1050153>

[24] Citované: Littvová, Z. – Marko, P. – Vachálková, I. 2012. *Riziko v poisťovníctve*. Bratislava : Ekonóm. s. 24. ISBN 978-80-225-3385-0

[25] Citované: Bálint, T. 2011. Poistenie rizík v oblasti informačných a komunikačných technológií. In: *Mezinárodní vědecká konference : Hradecké ekonomické dny 2011 : Ekonomický rozvoj a management regionů : Sborník recenzovaných příspěvků; Díl I* [online]. Hradec Králové : Univerzita Hradec Králové, 2011 [cit. 12.05.2014]. s. 22. Dostupné na: <https://cisco.uhk.cz/hed/data/sbornik/SBORNIK2011_I.pdf#page=19>

takéhoto konania rastú exponenciálne vo veľkosti aj finančnej náročnosti. To pre poisťovne znamená nielen samotné upisovanie a poisťovanie, ale aj iné aktivity potrebné na to aby sa týmto rizikám dalo predchádzať, teda na seba prenášajú nielen riziko, ale aj nevyhnutnosť výskumu rizík IT a pomoc a vytváranie ochranných opatrení.

„Pri rozhodovaní o poistení rizika zohráva významnú úlohu ekonomická únosnosť rizika. Ekonomická únosnosť poistenia príslušného rizika musí byť splnená tak z pohľadu poisťovne, ako aj z pohľadu klienta.“[26] Práve vysoké poistné bola spočiatku jedným z faktorov, ktoré bránili rýchlemu rozšíreniu kyberpoistenia. Poisťovne neboli schopné správne určiť výšku potenciálnych škôd, čím narastalo riziko pre poisťovne, ktoré sa odrazilo aj na výške poistného. Na druhej strane, často je uvádzaný ako dôvod plného rozvoja takéhoto poistenia aj nedostatok poistného krytia.

Možno konštatovať, že riziká spojené s IT sú ešte stále považované za nové a s ich poistiteľnosťou môžu mať poisťovacie spoločnosti problémy. Tieto riziká však zároveň predstavujú i trhovú príležitosť pre poisťovne a vzhľadom k rastúcemu dopytu po ich poistení, poisťovne musia na ne začať viac a lepšie reagovať. To znamená, že musia získavať poznatky o povahe týchto rizík, hľadať spôsoby, ako ich poistiť, a vytvárať tak nové produkty, čiže inovovať.

3.2 Poistenie rizík informačných technológií v USA

Spojené štáty americké patria medzi krajiny, v ktorých sa ako prvých objavili poistné produkty kryjúce riziká, ktoré so sebou prinášajú IT, a dodnes patria k lídrom v tejto oblasti. Má to mnoho príčin, medzi ktoré môžeme zaradiť napríklad to, že sa USA patria medzi štáty, v ktorých skôr nastalo hromadné rozšírenie IT medzi širokú verejnosť ako aj do výrobných procesov a služieb. Ďalej má obrovskú geografickú rozlohu a počtom obyvateľov patrí k najľudnatejšie štáty, sídli tu mnoho významných firiem, etc. Toto všetko a mnoho ďalších faktorov spôsobuje, že tu bol a je vysoký dopyt po poistení. USA je tiež krajina, kde je ponuka poistných produktov veľmi široká, poistiť sa tu dá takmer „všetko“, poisťovne investujú dostatočne veľa času a finančných prostriedkov na výskum. Výsledkom týchto a mnohých ďalších faktorov bol vznik poistných produktov kryjúcich riziká IT, najprv ako doplnky, a neskôr aj špecializované produkty.

Dnes v USA ponúka poistenie rizík IT viacero poisťovní, z ktorých sú niektoré medzinárodne známe a uznávané. „Poistenie kybernetických rizík je v súčasnosti

[26] Citované: Majtánová, A. a kol. 2006. *Poisťovníctvo*. Bratislava : Iura Edition, 2009. s. 62. ISBN 978-80-8078-2060-3

najrozšírenejšie v USA. Podľa štatistík najväčšej americkej poisťovne tržby z tohto druhu poistenia vlani stúpli o 30 percent. Kyberpoistenie má zatiaľ približne 31 percent firiem v USA“[27] a dopyt po ňom stúpa.[28] Krytie rizík IT poskytuje v USA poskytuje viacero spoločností, napríklad ACE, Travelers, AIG, ktorá uviedla na trh aj kybernetické krytie pre jednotlivcov.

3.2.1 ACE

Spoločnosť ACE Group bola založená v roku 1985 a pôsobí v 54 krajinách. Je to finančne silná spoločnosť a patrí medzi najväčšie poisťovne na svete.

Nie je špecializovaná, ale poskytuje rôzne druhy poistenia pre individuálnych klientov aj spoločnosti. Ponúka poistenie majetku, poistenie zodpovednosti, úrazové poistenie, doplnkové zdravotné poistenie, životné poistenie.

Na poistenie rizík IT má zamerané štyri produkty:

- ACE Privacy Protection®
- ACE DigiTech®
- ACE Digital DNA®
- Privacy and Network Liability Insurance Program Designed for Health Care and Managed Care

ACE Privacy Protection®

Tento program zahŕňa tradičné krytie zodpovednosti za počítačovú sieť, ale zameriava sa aj na poistenie zodpovednosti za osobné údaje, ktoré vyplývajú zo straty počítačového príslušenstva, bezpečnostných chýb v sieti a ľudských omylov. K výhodám tohto produktu patrí aj to, že je vhodný pre spoločnosti rôznych veľkostí.

Poistné krytie	Zodpovednosť za súkromie • Strata vyplývajúca zo zlyhania organizácie ochraňovať senzitívne informácie o jednotlivcoch alebo spoločnosti • Regulačné konanie vznesené vládnou agentúrou za porušenie vládneho, federálneho alebo zahraničného zákona o krádeži identity alebo ochrane osobných údajov

[27] Citované: Rundesová, T. 2014. Poistite sa proti hackerom. Ide to aj u nás. In *Hnonline.* [online] 2014. [cit. 12.05.2014]. Dostupné na internete: <http://hnporadna.hnonline.sk/clanky-168/poistite-sa-proti-hackerom-ide-to-aj-u-nas-611750>

[28] Podľa: Mello, Jr., J. P. 2013. Rise in Data Braches Drives Interest in Cyber Insurance. In *CIO.* [online] 2013. [18.05.2014]. Dostuné na internete: <http://www.cio.com/article/738144/Rise_in_Data_Breaches_Drives_Interest_in_Cyber_Insurance>

	Data Breach Fund • Náklady na vyšetrovanie zdroja úniku, dodržanie predpisov o ochrane osobných údajov, oznamovanie a sledovanie podozrivých informácií a na získanie obstaranie právnych služieb, služieb public relations alebo krízového manažmentu na opätovné získanie podnikovej reputácie Zodpovednosť za sieťovú bezpečnosť • záväzky organizácie vyplývajúce zo zlyhania sieťovej bezpečnosti, vrátane neoprávneného prístupu alebo neoprávneného používania podnikových systémov, útok na odmietnutie služieb alebo prenos malvéru Zodpovednosť za internetové masmédiá • porušenie autorského práva alebo ochrannej značky, narušenie súkromia, ohováranie, urážku na cti, plagiáty alebo škody z nedbalosti plynúcu z obsahu na internetovej stránke organizácie Network Extortion Threat • peňažné vydieranie a a s tým spojené náklady vyplývajúce z vyhrážania sa zverejnením citlivých informácií alebo zvrhnutím siete
Minimálne poistné alebo spoluúčasť (minimum)	Žiadne obmedzenia
Limit poistného plnenia	Do 20 miliónov USD
Profil klienta	Každý podnik pracujúci s: • citlivými informáciami o svojich zákazníkoch alebo zamestnancoch • informácie o tretej zmluvnej strane • Počítačovou sieťou • Internetovou stránkou Cielené kategórie zahŕňajú maloobchod, finančné inštitúcie a

	zdravotníctvo

Zdroj: vlastné spracovanie podľa: ACE USA: ACE Privacy Protection®. [online] 2014. [cit. 14.05.2014]. Dostupné na internete: <http://www.acegroup.com/us-en/businesses/ace-privacy-protection-privacy-network-liability.aspx>

ACE DigiTech®: Digital Technology and Professional Liability Insurance

Ďalší program je zameraný na poistenie zodpovednosti za škody pri výkone povolania a digitálne technológie. Poskytuje komplexné poistné krytie zodpovednosti za technologické produkty a služby, ochranu bezpečnosti najmodernejších sietí a zodpovednosti za citlivé informácie, ktoré sú uložené v systémoch spoločnosti.

Poistné krytie	Zodpovednosť za opomenutie a technologické a internetové chyby • Konanie, chyby a opomenutia pri poskytovaní technologických služieb alebo pri predaji technologických produktov Zodpovednosť za elektronické médiá • Porušenie autorského práva alebo ochrannej známky, narušenie súkromia, ohováranie, urážka na cti, plagiáty alebo škody z nedbalosti vyplývajúce z elektronického publikovania, rozširovania, uvoľňovania, zberu, prenosu, vytvárania, internetového vysielania alebo inej distribúcie elektronického obsahu na internete Zodpovednosť za sieťovú bezpečnosť • Záväzok organizácie vyplývajúci zo zlyhania sieťovej bezpečnosti, vrátane neautorizovaného prístupu alebo neautorizovaného používania podnikových systémov, útok na odoprenie služby alebo prenos malvéru. • regulačné opatrenia vznesené vládnou agentúrou pre obvinenie z porušenia štátneho, federálneho alebo zahraničného zákona o krádeži identity a ochrane osobných údajov Zodpovednosť za súkromie • Strata plynúca zo zlyhania organizácie chrániť citlivé informácie o podniku alebo spoločnosti Data Breach Fund

	• Náklady na počítačové vybavenie na určenie zdroja úniku, dodržanie predpisov o ochrane osobných údajov, oznamovanie a sledovanie podozrivých operácií a na získanie obstaranie právnych služieb, služieb public relations alebo krízového manažmentu na opätovné získanie podnikovej reputácie Network Extortion Threat • Peňažné vydieranie a s tým spojené náklady vyplývajúce z vyhrážania sa zverejnení citlivých informácií alebo zvrhnutím siete Zodpovednosť za rôzne odborné služby • Konania, chyby a opomenutia pri poskytovaní služieb iných ako technologických
Minimálne poistné	5 000 USD
Profil klienta	• Všeobecný poskytovateľ technologických služieb • Konzultant alebo integrátor hardvéru, softvéru alebo systémovej koncepcie • Poskytovatelia aplikačných služieb • Spracovávatelia údajov • Vývojári softvéru

Zdroj: vlastné spracovanie podľa: ACE USA: ACE DigiTech®: Digital Technology and Professional Liability Insurance. [online] 2014. [cit. 15.05.2014]. Dostupné na internete: <http://www.acegroup.com/us-en/businesses/ace-digitech-digital-technology.aspx>

ACE Digital DNA® Network Risk Insurance Program

Program ACE Digital DNA je zameraný na poistenie rizík počítačových sietí, predovšetkým na ochranu bezpečnosti počítačových sietí a citlivých údajov, ktoré by mohli spôsobiť spoločnostiam vážne finančné problémy. Na rozdiel od predchádzajúceho produktu, tento program je určený pre tú kategóriu spoločností, ktoré sú odkázané na používanie počítačových sietí a internetu.

Poistné krytie	Strata digitálnych aktív • Výdavky na náhradu alebo obnovu údajov, ktoré boli poškodené alebo zničené pre zlyhanie bezpečnosti siete Kybernetické vydieranie

	• Peňažné vydieranie a s stým spojené výdavky vyplývajúce z vyhrážania sa zverejnením senzitívnych informácií alebo zvrhnutím siete Výdavky na oznámenie zlyhania bezpečnosti • Ponúka náhradu za spôsobené výdavky na dodržanie predpisov o osobnom súkromí a krádeži identity, vrátane štátnej krádeže identity a zákonov o hlásení Prerušenie prevádzky • Strata príjmu a ďalšie výdavky vyplývajúce z prerušenia sieťovej služby kvôli útoku na sieť poisteného, vrátane útokov hackerov, interných pracovníkov a distribuovaných útokov na odopretie služby Podmienené prerušenie prevádzky • Strata príjmu a ďalšie výdavky vyplývajúce z prerušenia siete spôsobeného poskytovateľom základných služieb, čo môže tiež zahŕňať prostriedky spoločností poskytujúcich internetové služby a externých poskytovateľov služieb elektronického obchodu
Minimálne poistné alebo spoluúčasť	žiadne
Poistné plnenie	Do 15 miliónov dolárov
Profil klientov	• Prevádzkovatelia internetových stránok • Používatelia počítačovej siete pri každodenných činnostiach • Tých, ktorý sú zodpovední za elektronické úložiská s informáciami o klientoch a/alebo hodnotným nehmotným majetkom • Tých, ktorí sa spoliehajú na externého poskytovateľa sieťových služieb • Tých, ktorí sa spoliehajú na príjem z internetových stránok

Zdroj: vlastné spracovanie podľa: ACE USA: ACE Digital DNA® Network Risk Insurance Program. [online] 2014. [cit. 15.05.2014]. Dostupné na internete: <http://www.acegroup.com/us-en/businesses/ace-digital-dna-network-risk-insurance-program.aspx>

ACE Privacy Protection®: Privacy and Network Liability Insurance Program Designed for Health Care and Managed Care

Posledný program je špeciálne navrhnutý pre spoločnosti, ktoré poskytujú zdravotnú starostlivosť a starostlivosť o ľudí. Poskytuje komplexné krytie na ochranu ich počítačových sietí a internetových stránok, ale aj ochranu informácií o ich zákazníkoch, zamestnancoch a obchodných partneroch.

Poistné krytie	Zodpovednosť za súkromie (zahŕňa všetky osobné informácie; nevyhradené iba cez únik cez sieť; informácie o zákazníkoch a zamestnancoch) Zodpovednosť za bezpečnosť počítačovej siete Data Breach Fund zahŕňa: • Náklady prvej a tretej strany • Súdne výdavky • Náklady na konanie v zhode s obstaraním oznámenia spotrebiteľa o príslušnej právomoci najviac vyhovujúcej krytiu týchto nákladov • Náklady na dobrovoľné oznámenie (požaduje sa predchádzajúci písomný súhlas) • Náklady na public relations, krízový manažment a advokátske kancelárie • Právne náklady vzniknuté poisteným na vymedzenie nároku na odškodnenie podľa zmluvy • Náklady na sledovanie podozrivých operácii (ktoré sa už nevzťahuje na predpisy o ochrane osobných údajov)
Limit poistného plnenia	Nad 20 miliónov USD
Profil klienta	Spoločnosti zaoberajúce sa zdravotnou starostlivosťou alebo starostlivosťou o ľudí so citlivými informáciami o zákazníkoch alebo zamestnancoch, informáciami o tretej obchodnej strane, počítačovú sieť alebo internetovú stránku

Zdroj: vlastné spracovanie podľa: ACE USA: ACE Privacy Protection® Privacy and Network Liability Insurance Program Designed for Health Care and Managed Care. [online] 2014. [cit. 15.05.2014]. Dostupné na internete:

<http://www.acegroup.com/us-en/businesses/ace-privacy-protection-privacy-network-liability-insurance-program-designed-for-health-care-managed-care.aspx>

Ako možno vidieť, poistné programy poisťovne ACE sú špecializované podľa potrieb jednotlivých skupín klientov, aby pokrývali potreby podľa ich zamerania, keďže v každom sektore prevažujú riziká iného typu. Tiež možno pozorovať, že tieto produkty sú predovšetkým zamerané na ochranu informácií, ktorých únik či strata sa pre podniky v USA stali hlavnou hrozbou.[29]

3.2.2 TRAVELERS

The Travelers Companies Inc. patrí k najväčším poisťovniam majetku v USA. Bola založená v roku 1853 a poskytuje poistenie spoločnostiam aj individuálnym klientom. Poskytuje rôzne druhy poistenia, medzi ktoré patrí aj produkt CyberFirst®.[30]

CyberFirst® je poistný produkt vyvinutý na krytie kybernetických rizík určený predovšetkým pre spoločnosti podnikajúce v oblasti technológií. CyberFirst® zahŕňa:

- Celopodnikové krytie na poistníkov podnik aj prácu, zahŕňa hardvér aj softvér
- Celosvetové poistné krytie, ak to nie je proti zákonom USA
- Automaticky kryje aj nové dcérske spoločnosti s o ziskom do 10% celej spoločnosti
- Právo a povinnosť chrániť kryté nároky a požiadavky
- Právo a povinnosť chrániť svoje požiadavky na náhradu škody[31]

V rámci neho sa ponúkajú štyri moduly:

- Poistenie zodpovednosti za technologické chyby a omyly
- Poistenie zodpovednosti za bezpečnosť sietí a informácií
- Poistenie zodpovednosti za komunikácie a masmédiá
- Poistenie úhrady nákladov

Poistenie zodpovednosti za technologické chyby a omyly je špeciálne navrhnuté pre dnešné high-tech spoločnosti. Chráni poistené subjekty pred škodami, za ktoré musia

[29] Podľa: Wells, A. 2014. What´s Next for Cyber Insurance? In *Carrier Managenet.*[online] 2014. [18.05.2014]. dostupné na internete: <http://www.carriermanagement.com/features/2014/05/08/122728.htm>
[30]Spracované podľa: The Travelers Indemnity Company: About Travelers. [online] 2014. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/about-us/index.aspx>
[31] Spracované podľa: The Travelers Indemnity Company. 2012. Coverage Advantages. *In Insuring Innovation. CyberFirst®.Coverage for Technology Companies*. [online] 2012. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/business-insurance/specialized-industries/technology/docs/CyberFirst-Suite-locked.pdf>

platiť, ak došlo pri výrobe alebo práci k chybe či omylu a zákazník podá proti danej spoločnosti obvinenie za ušlý zisk či prerušenie prevádzky. Obvinená spoločnosť je povinná tieto náklady zaplatiť, a keďže sú vysoké, môže čo môže mať na ňu katastrofálne dopady ak to musí zaplatiť sama, ale pri takomto krytí to za ňu zaplatí poisťovňa.

Napríklad sa môže stať, že podnik vyvíja nový produkt a dôjde pri tom k náhodnému omylu, spôsobí to chyby vo výrobných schémach. A tak nastanú vo výrobe poruchy, ale problém bude objavený až neskôr, keď už bude mnoho vyrobených mnoho produktov. Ak budú zákazníci pýtať odškodné, podnik to musí zaplatiť, a to buď z vlastných peňazí alebo cez poisťovňu.[32]

Poistenie zodpovednosti za bezpečnosť sietí a informácií je zameraný predovšetkým na ochranu citlivých informácií a ochranu pred škodami spôsobenými vírusom. Poskytuje poistné krytie:

- Ak spoločnosť nepredíde neoprávnenému prístupu k citlivým informáciám alebo ich použitiu
- Ak spoločnosť nepredíde prenosu počítačového vírusu
- Ak spoločnosť neoznámi chyby v bezpečnosti v súlade so zákonom
- Nezabezpečenie prístupu oprávneným používateľom na internetové stránky alebo komunikačné siete
- Zlyhanie bezpečnostného hardvéru alebo softvéru alebo ak ich poistený včas neaktualizuje
- Elektrické alebo mechanické poruchy, napríklad výpadok energie, elektriny

Príkladom je, že zamestnanec pre svoju nedbalosť stiahne do počítača vírus, ktorý sa rozšíri po celej podnikovej počítačovej sieti a súboroch. Ak si potom klient stiahne nejaké informácie z internetovej stránky, dostane sa mu do počítača vírus. Výsledkom toho bude strata mnohých údajov. Klient zažaluje podnik za to, že tomu mal zabrániť, a bude žiadať odškodné.[33]

[32] Spracované podľa: The Travelers Indemnity Company. 2012. Technology Errors & Omissions Liability. *In Insuring Innovation. CyberFirst®.Coverage for Technology Companies*. [online] 2012. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/business-insurance/specialized-industries/technology/docs/CyberFirst-Suite-locked.pdf>

[33] Spracované podľa: The Travelers Indemnity Company. 2012. Network & Information Security Liability. *In Insuring Innovation. CyberFirst®.Coverage for Technology Companies*. [online] 2012. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/business-insurance/specialized-industries/technology/docs/CyberFirst-Suite-locked.pdf>

V rámci poistenia zodpovednosti za komunikácie a masmédiá sa poskytuje poistné krytie na:

- Porušenie autorských práv, ochrannej známky, obchodnej úpravy, obchodnej značky alebo obchodného mena
- Neoprávnené používanie reklamného materiálu, sloganu alebo názvu použitého v reklamách iných subjektov
- Plagiáty alebo neoprávnené používanie literárneho alebo umeleckého formátu, charakteru alebo výkonu

Môže sa stať, že podnik umiestni na svoju internetovú stránku reklamu na novú službu od svojho obchodného partnera a táto reklama obsahuje materiál, na ktorý si jeden z konkurentov uplatňuje nárok ako jeho vlastný. Tento konkurenčný podnik podá žalobu za škody spôsobené neoprávneným používaním reklamného materiálu.[34]

Poistenie úhrady nákladov poskytuje poistné krytie na:

- Náklady na oznámenie o poruchách bezpečnosti a na opravu
- Náklady prerušenia prevádzky a dodatočné náklady
- Náklady z vydierania
- Náklady na obnovu počítačových programov a elektronických údajov
- Počítačový podvod
- Podvod prevodu finančných prostriedkov
- Telekomunikačná krádež

Napríklad, ak podnikateľský subjekt dostane niekoľko oznámení, v ktorých sú vyhrážky o infiltrácií sa do databázy s informáciami o zákazníkoch tohto podniku a uverejniť ich kontaktné informácie širokej verejnosti. Toto poistné krytie zahŕňa aj peniaze alebo cenné papiere zaplatené vydieračom.

Tiež sa môže stať, že organizovaná skupina zločincov získa neautorizovaný prístup k platobným účtom v počítačovom systéme spoločnosti, kde potom zmení informácie o odchádzajúcich platbách. Obrovské množstvá peňazí sa tak nedostanú na účet v banke,

[34] Spracované podľa: The Travelers Indemnity Company. 2012. Communications & Media Liability. *In Insuring Innovation. CyberFirst®.Coverage for Technology Companies*. [online] 2012. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/business-insurance/specialized-industries/technology/docs/CyberFirst-Suite-locked.pdf>

ale na účet danej skupiny. Toto poistné krytie zahŕňa náklady na priamu stratu peňazí, cenných papierov alebo iného majetku.[35]

3.3 Poistenie rizík informačných technológií na Slovensku

Trh s poistením rizík IT je v súčasnosti na Slovensku oveľa užší a menej rozvinutý ako vo väčšine vyspelých krajín. Rizík IT však pribúda a dopyt po nich narastá, a tak aj poisťovne na Slovensku naňho začínajú reagovať.

Napriek tomu, že poistiteľnosť IT rizík niektorí vnímajú ako diskutabilnú, existuje na svete viacero poisťovní, ktoré už poskytujú poistné produkty na ich krytie. Na Slovensku sa dali poistiť iba niektoré z nich v rámci poistných krytí, ktoré však neboli zamerané na ich krytie. Napríklad, poistením prerušenia prevádzky, poistením elektroniky, poistením zodpovednosti za škodu spôsobenú vadným výrobkom, etc. Dopyt po poistení rizík v rámci IT sektora však rástol, a tak poisťovne začali ponúkať aj také poistenia ako napríklad poistenie zodpovednosti za škodu spôsobenú pri poskytovaní služieb informačných technológií.[36]

3.3.1 Allianz

Allianz - Slovenská poisťovňa a. s. vznikla v roku 2003 zlúčením Allianz AG a Slovenskej poisťovne. Poskytuje životné aj neživotné poistenie.[37] Allianz – Slovenská poisťovňa získala v Zlatej minci 2013 deviate víťazstvo za sebou v tejto súťaži.[38] V roku 2010 „Allianz – Slovenská poisťovňa rozšírila svoje portfólio poistení profesijnej zodpovednosti o služby v oblasti IT a stala sa tak jedinou poisťovňou na slovenskom trhu, ktorá toto poistenie poskytuje prostredníctvom samostatných poistných podmienok.“[39]

Allianz – Slovenská poisťovňa ponúka komplexný produkt pre IT spoločnosti zahŕňajúci viacero druhov poistenia, ktoré sú pre také spoločnosti vhodné. Patria sem:

---

[35] Spracované podľa: The Travelers Indemnity Company. 2012. Expense Reimbursement Coverage. In *Insuring Innovation. CyberFirst®.Coverage for Technology Companies*. [online] 2012. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/business-insurance/specialized-industries/technology/docs/CyberFirst-Suite-locked.pdf>

[36] Slovenská asociácia poisťovní. 2013. *Poistné produkty na slovenskom poistnom trhu.* [online]. 2013. [cit. 16.05.2014]. Dostupné na internete: <http://www.slaspo.sk/tmp/asset_cache/link/0000045324/Poistne%20produkty%20na%20SK%20poistnom%20trhu%20k%203103%202013%20na%20web%20stranku%20SLASPO.pdf>

[37] Spracované podľa: Allianz – Slovenská poisťovňa. *Základné informácie o spoločnosti.* [online] [16.05.2014]. Dostupné na internete: <http://www.allianzsp.sk/spolocnost>

[38] Spracované podľa: 2013. Zlatá minca 2013: Výsledky. In *Zlatá minca*. [online] 2013. [cit. 16.05.2014]. Dostupné na internete: <http://zlataminca.sk/zlata-minca-2013-vysledky/cmsarticle/#.U3XdT7_xp0K>

[39] Allianz – Slovenská poisťovňa. 2010. *Poistenie zodpovednosti za škodu pri poskytovaní IT služieb*. [online] 2010. [cit. 2010]. Dostupné na internete: <http://www.allianzsp.sk/96497>

- „Poistenie zodpovednosti za škodu spôsobenú pri poskytovaní služieb informačných technológií
- Poistenie majetku
- Poistenie prerušenia prevádzky
- Poistenie strojov a elektroniky
- Poistenie nákladu
- Poistenie prevádzkovej zodpovednosti za škodu
- Stavebné poistenie
- Poistenie zodpovednosti za environmentálnu škodu.“[40]

Špecifickým je práve Poistenie za škodu spôsobenú pri poskytovaní služieb informačných technológií. Toto poistenie je určené pre medzinárodné spoločnosti, stredné a malé podniky, aj živnostníkov, ktorí sa pri vykonávaní činnosti dostávajú do styku s IT. Poistenie sa vzťahuje na tieto profesijné služby:

a) „vývoj software;
b) poskytovanie softwaru – predaj hotových programov na základe zmluvy s autorom, dodávka softwaru, služby pri údržbe a podpore softwaru, update a upgrade software;
c) distribúcia, dodávka, inštalácia/montáž, oprava a údržba hardware a počítačového príslušenstva;
d) automatizované spracovanie dát; služby súvisiace s počítačovým spracovaním údajov;
e) systémová analýza a integrácia;
f) správa počítačových sietí;
g) zabezpečovanie internetových služieb;
h) poradenstvo a podpora v oblasti IT;
i) školenia v oblasti IT.“[41]

V rámci hlavného poistenia sa poskytuje poistné krytie na:

- finančnú ujmu
- škodu na zdraví a/alebo na majetku

[40] Citované: Allianz – Slovenská poisťovňa. 2014. *IT spoločnosti.* [online] 2014. [cit. 16.05.2014]. Dostupné na internete: <http://www.allianzsp.sk/poistenie-pre-it-spolocnosti#flap_108840_2>
[41] Citované: Allianz – Slovenská poisťovňa. *Všeobecné poistné podmienky.* [online] [cit. 16.05.2014]. Dostupné na internete: <http://www.allianzsp.sk/tmp/image_cache/link/0000395451/VPP_IT_spolocnosti.pdf>

- náklady konania v súdnom, správnom alebo administratívnom konaní o náhrade škody

Poisťovňa ponúka i dobrovoľné pripoistenia:

- neúmyselné poručenie práv duševného vlastníctva
- náklady na obnovu alebo nahradenie dokumentov a/alebo počítačových záznamov[42]

Allianz SP je jedna z mála poisťovní, ktoré podobné produkty pre IT sektor ponúkajú, no tiež má ešte mnoho nedostatkov. Napríklad ochranu dát kryje iba veľmi okrajovo. Táto poisťovňa však vyvíja nový produkt poistenie zodpovednosti za škodu v súvislosti s ochranou dát. Bude určené pre právnické a podnikajúce fyzické osoby a poisťovňa by ho čoskoro mala uviesť na trh.[43]

3.3.2 AIG

AIG Europe Limited je dcérskou spoločnosťou medzinárodnej poisťovacej organizácie American Insurance Group, Inc. Na Slovensku pôsobí ako pobočka zahraničnej poisťovne a od roku 1998 ponúka neživotné poistenie pre organizácie, podnikateľov aj osoby.[44]

K jej produktom patrí aj CyberEdge alebo Cyber zodpovednosť, zodpovednosť za kybernetické riziká. Je dostupný pre všetky typy organizácií, ale špecializuje sa na organizácie, ktoré pracujú s dátami, zodpovedajú za ich ochranu, spracovávajú ich, uchovávajú ich alebo získavajú pri svojej podnikateľskej činnosti, najmä zdravotnícke spoločnosti, finančné inštitúcie, obchodné či výrobné podniky.[45] Tento poistný produkt poskytuje poistné krytie rizík spojených s únikom a krádežou dát, ale aj služby konzultantov.

Zodpovednosť za ochranu údajov	Zodpovednosť za dáta	Škody a náklady právneho zastúpenia spojené s porušením ochrany osobných alebo firemných údajov
	Bezpečnosť systémov	Škody a náklady právneho zastúpenia

[42] Spracované podľa: Allianz – Slovenská poisťovňa. *IT spoločnosti.* [online] 2014. [16.05.2014]. Dostupné na internete: <http://www.allianzsp.sk/poistenie-pre-it-spolocnosti#flap_108840_2>
[43] Spracované podľa: Mittaš, M. 2014. Proti hekerom sa dá aj poistiť!. In *Next Future.* [online] 2014. [16.05.2014]. Dostupné na internete: <http://www.nextfuture.sk/poistovne/clanky/proti-hekerom-sa-da-chranit-aj-poistit/>
[44] Spracované podľa: AIG: AIG Europe Limited. *O AIG*. [online] [16.05.2014]. Dostupné na internete: <http://www.aigpoistenie.sk/_887_216442.html>
[45] Spracované podľa: Mittaš, M. 2014. Proti hekerom sa dá aj poistiť!. In *Next Future.* [online] 2014. [16.05.2014]. Dostupné na internete: <http://www.nextfuture.sk/poistovne/clanky/proti-hekerom-sa-da-chranit-aj-poistit/>

		pokiaľ nastane: • kontaminácia dát tretej strany vírusom • chyba alebo omyl, ktorého výsledkom je neautorizovaný vstup tretej strany do systémov • krádež prístupového hesla neelektronicky • krádež hardwaru, ktorý obsahuje osobné dáta • zverejnenie údajov a dát ako výsledok konania zamestnancov
	Povinnosti pred správnymi a štátnymi orgánmi	• primerané náklady právneho zastúpenia a poradenstva v súvislosti s vyšetrovaním alebo porušením legislatívy o ochrane osobných údajov • pokuty a penále uložené dozornými orgánmi pre oblasť ochrany osobných údajov
	Elektronické dáta	Konzultačné služby v oblasti obnovy elektronických dát alebo ich znovu vytvorenie a náklady na znovu zabezpečenie dát proti ďalšiemu úniku
	Krízový manažment	Konzultačné služby a aktivity smerujúce k minimalizácii škôd na dobrom mene a povesti organizácie, dotknutých jednotlivcov ako aj náklady súvisiace s notifikáciou subjektov, ktorých sa únik týka.
Pripoistenia (voliteľné)	Porušenie prevádzky siete	Stratu čistého zisku následkom fyzického prerušenia prevádzky informačnej siete

		poisteného, ktoré je výsledkom narušenia bezpečnosti systému
	Multimediálna zodpovednosť	Škody a náklady právneho zastúpenia v prípade porušenia práv intelektuálneho vlastníctva tretej osoby, alebo nedbanlivosti pri správe elektronického obsahu médií
	Cyber/súkromie vydieranie	Vynútené platby (výkupné, vydieranie) tretím osobám, ktoré sú vynaložené na eliminovanie bezpečnostného rizika

Zdroj: vlastné spracovanie podľa: Loula, I. *CyberEdge od AIG*. [online] [16.05.2014]. Dostupné na internete: <http://www.aigpoistenie.sk/chartisint/internet/SK/sk/files/AIG_cyber_ebrochure-SK-v2a_tcm887-445264.pdf>

Takéto poistenie ponúkajúce ochranu pri strate, poškodení či úniku údajov alebo informácií a rizík s tým súvisiacich zatiaľ neponúka žiadna iná poisťovňa na Slovensku. Ochrana informácií je však dôležitá aj pre organizácie a subjekty podnikajúce na tomto území, a preto dopyt po takomto poistení rastie. Následkom toho sa vytvára tlak na poisťovne spojený s možnosťou rozšíriť s svoje portfólio o poistenie takýchto rizík. Mnohé poisťovne už začínajú pripravovať produkty na krytie takýchto rizík.

Poisťovňa AIG tiež poskytuje napríklad poistný produkt na poistenie profesnej zodpovednosti. V rámci neho ponúka aj poistenie vyvinuté špeciálne pre organizácie a podnikateľské subjekty pôsobiace v sektore informačných technológií.

Ďalej tiež poskytuje poistenie majetku, poistenie zodpovednosti za škodu a iné univerzálne poistenia, ktoré sú vhodné aj pre IT sektor, i keď ich neponúka ako jednotný poistný program, ako je to u Allianz poisťovne, ktorá však neponúka poistné krytie kybernetických rizík.

Možno teda povedať, že AIG poisťovňa patrí k málu poisťovní, ktoré na slovenskom trhu ponúkajú krytie niektorých špecifických rizík, ktoré so sebou prinášajú informačné technológie.

Záver

Vo svojej bakalárskej práci som vytýčila a rozdelila najvýznamnejšie riziká, ktoré súvisia s informačnými technológiami. Dajú sa rozdeliť na tri kategórie podľa dôvodu ich vzniku. Tiež som zistila, že najväčším rizikom, ktoré so sebou prinášajú informačné technológie, je práve strata, poškodenie či únik informácií, pretože prinášajú vážne ohrozenie pre všetky subjekty.

V ďalšej časti som poskytla pohľad na niekoľko opatrení pre podnikateľské subjekty, ktoré by mali zavádzať kvôli predchádzaniu vzniku najčastejších nepriaznivých udalostí spôsobených informačnými technológiami pre podnik a minimalizácii vzniknutých škôd. Podľa mňa je zatiaľ najzákladnejšie riešenie kvalitný antivírusový program, pretože by mal uchrániť informačné technológie pred vniknutím malvérov, ktoré majú na rizikách informačných technológií obrovský podiel. Potrené opatrenia pre podniky sa nevzťahujú len na ne, avšak mnohé sú jednoduché a efektívne, i keď nie vždy využívané, a tak nastávajú v podnikoch udalosti, ktoré vedú k problémom podnikov, a väčšine z nich sa dá zabrániť

Neskôr sa zaoberám dôvodmi, ktoré vedú k problematickosti poistenia informačných technológii. Je to spôsobené najmä problémami s ohodnocovaním veľkosti rizík informačných technológií, ktoré sú rozvinuté veľmi komplexne. Na vznik nových poistných produktov však majú vplyv najmä dopyt a ponuka, a tak sa takéto poistenia poskytujú, pričom hlavným kritériom je poistné, ktoré musí byť prijateľné tak pre poisťovňu, ako aj pre poistníka.

Posledná časť je venovaná analýze trhu na Slovensku a spojených štátoch amerických. Najprv rozoberám stav trhu poistenia informačných technológií v USA, kde ponúkam bližšiu charakteristiku produktov kryjúcich riziká informačných technológií od ACE poisťovne a Travelers poisťovne. Na tomto trhu ponúka poistenie takmer všetkých rizík informačných technológií a tieto produkty sú tiež poskytované vo formách, ktoré sa špecializujú na jednotlivé kategórie klientov, ktoré prichádzajú do styku s týmito rizikami.

Na slovenskom poistnom trhu je situácia oveľa horšia. Niektoré riziká sa dajú poistiť, avšak tieto nekryjú najväčšie riziká informačných technológií. Aj poisťovne na Slovensku už ale začali ponúkať poistné produkty na takéto druhy rizík. Jednou z nich je poisťovňa Allianz, ktorá ponúka program určený pre informačný sektor, v rámci ktorého je

tiež poistenie zodpovednosti za škodu spôsobenú pri poskytovaní služieb informačných technológií. Ďalšou významnou poisťovňou v tejto oblasti je AIG, ktorá ponúka produkt CyberEdge, ktorý je významným najmä pre ochranu informácií a niektorých iných kybernetických rizík. Na poistnom trhu by sa však za krátky čas mali objaviť i ďalšie nové produkty, ktoré zatiaľ poisťovne vyvíjajú Problém oboch s týchto produktov však spočíva v tom, že sú dostupné len pre organizácie a podnikateľské subjekty, pretože individuálni klienti zatiaľ neprejavujú dostatočný záujem o takéto poistenie. Podľa mňa má poistenie rizík informačných technológií obrovský potenciál na rozvoj, viacero poisťovní ho využije na svoj rast či udržanie sa na trhu a začnú sa i u nás poskytovať produkty špecializované pre jednotlivé sektory využívajúce informačné technológie.

Zoznam použitej literatúry

Kokles, M., Romanová, A. 2010. *Informatika*. 6. vyd. Bratislava : Sprint dva, 2010. 304 s. ISBN 978-80-89393-14-5

Littvová, Z. – Marko, P. – Vachálková, I. 2012. *Riziko v poisťovníctve*. Bratislava : Ekonóm, 2012. 114 s. ISBN 978-80-225-3385-0

Majtánová, A. 2009. *Poisťovníctvo.* Bratislava : Iura Edition, 2009. 327 s. ISBN 978-80-8078-260-3

Majtánová, A. a kol. 2010 *Vývojové trendy v poistnom krytí životných a neživotných rizík : s podtitulom Poisťovníctvo v európskych dimenziách*. Bratislava : Vydavateľstvo EKONÓM, 2010. 192 s. ISBN 978-80-225-2900-6.

Pastoráková, E. - Drugdová, B. - Brokešová, Z. 2010. *Dopad globalizačných a integračných procesov na poistný trh v SR : (vybrané problémy).* Bratislava : Vydavateľstvo EKONÓM, 2010. 77 s. ISBN 978-80-225-3106-1

ACE USA: ACE Digital DNA® Network Risk Insurance Program. [online] 2014. [cit. 15.05.2014]. Dostupné na internete: <http://www.acegroup.com/us-en/businesses/ace-digital-dna-network-risk-insurance-program.aspx>

ACE USA: ACE DigiTech®: Digital Technology and Professional Liability Insurance. [online] 2014. [cit. 15.05.2014]. Dostupné na internete: <http://www.acegroup.com/us-en/businesses/ace-digitech-digital-technology.aspx>

ACE USA: ACE Privacy Protection® Privacy and Network Liability Insurance Program Designed for Health Care and Managed Care. [online] 2014. [cit. 15.05.2014]. Dostupné na internete: < http://www.acegroup.com/us-en/businesses/ace-privacy-protection-privacy-network-liability-insurance-program-designed-for-health-care-managed-care.aspx>

ACE USA: ACE Privacy Protection®. [online] 2014. [cit. 14.05.2014]. Dostupné na internete: <http://www.acegroup.com/us-en/businesses/ace-privacy-protection-privacy-network-liability.aspx>

AIG: AIG Europe Limited. *O AIG.* [online] [16.05.2014]. Dostupné na internete: <http://www.aigpoistenie.sk/_887_216442.html>

Allianz – Slovenská poisťovňa. 2010. *Poistenie zodpovednosti za škodu pri poskytovaní IT služieb*. [online] 2010. [cit. 2010]. Dostupné na internete: <http://www.allianzsp.sk/96497>
Allianz – Slovenská poisťovňa. 2014. *IT spoločnosti.* [online] 2014. [cit. 16.05.2014]. Dostupné na internete: <http://www.allianzsp.sk/poistenie-pre-it-spolocnosti#flap_108840_2>
Allianz – Slovenská poisťovňa. *IT spoločnosti.* [online] 2014. [16.05.2014]. Dostupné na internete: <http://www.allianzsp.sk/poistenie-pre-it-spolocnosti#flap_108840_2>
Allianz – Slovenská poisťovňa. *Všeobecné poistné podmienky.* [online] [cit. 16.05.2014]. Dostupné na internete: <http://www.allianzsp.sk/tmp/image_cache/link/0000395451/VPP_IT_spolocnosti.pdf>
Allianz – Slovenská poisťovňa. *Základné informácie o spoločnosti.* [online] [16.05.2014]. Dostupné na internete: <http://www.allianzsp.sk/spolocnost>
Bálint, T. 2011. Poistenie rizík v oblasti informačných a komunikačných technológií. In: *Mezinárodní vědecká konference : Hradecké ekonomické dny 2011 : Ekonomický rozvoj a management regionů : Sborník recenzovaných příspěvků; Díl I* [online]. Hradec Králové : Univerzita Hradec Králové, 2011 [cit. 12.05.2014]. s. 22. Dostupné na: <https://cisco.uhk.cz/hed/data/sbornik/SBORNIK2011_I.pdf#page=19>
EMC Corporation. 2014. *RSA Monthly Online Fraud Report.* [online] 2014. [12.05.2014] <http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf>
Európska rada. 2013. *Európska rada: zaostrené na digitálne hospodárstvo.* [online] 2013. [cit. 13.05.2014]. Dostupné na internete: <http://www.european-council.europa.eu/home-page/highlights/european-council-focus-on-the-the-digital-economy?lang=sk>
EUROSTAT: Level of Internet access – households. [online] [13.05.2014] Dostupné na internete: <http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00134>
GFI Software. 2011. *The corporate threat posed by email trojans.* [online] [08.05.2014]. Dostupné na: <http://www.gfi.com/whitepapers/network-protection-against-trojans.pdf>
IT NEWS: 2014. Ďalší krok k realistickejšej virtuálnej realite. Technológia Ultragraphics umožní „dotknúť" sa virtuálnych predmetov. In *IT NEWS.I.* [online] 2014. [cit. 14.05.2014]. Dostupné na internete: <http://www.itnews.sk/spravy/startupy/2014-05-02/c162970-dalsi-krok-k-realistickejsej-virtualnej-realite.-technologia-ultrahaptics-umozni-dotknut-sa-virtualnych-predmetov>

Jašková, Ľ. 2014. *Informačná spoločnosť*. [online]. Univerzita Komenského v Bratislave. 2014. [cit. 08.05.2014]. Dostupné na internete: <http://edi.fmph.uniba.sk/~jaskova/InformacneSystemy/tema01/tema01.html>
Kokles, M., Romanová, A. 2010. *Informatika*. 6. vydanie. Bratislava : Sprint dva, 2010. s. 120-121. ISBN 978-80-89393-14-5
Krátka, Z. 2007. Poistiteľnosť rizika informačných a komunikačných systémov. [online] 2007. [cit. 08.05.2014]. Dostupné na internete: <http://maag.euba.sk/documents/PoistitelnostrizikaICS_konferenciaKPOI2007.pdf>
Krátka, Z. 2007. *Poistiteľnosť rizika informačných a komunikačných technológií.* [online] 2007. [cit. 11.05.2014]. Dostupné na: <http://maag.euba.sk/documents/PoistitelnostrizikaICS_konferenciaKPOI2007.pdf>
Loula, I. *CyberEdge od AIG*. [online] [16.05.2014]. Dostupné na internete: http://www.aigpoistenie.sk/chartisint/internet/SK/sk/files/AIG_cyber_ebrochure-SK-v2a_tcm887-445264.pdf
Mello, Jr., J. P. 2013. Rise in Data Braches Drives Interest in Cyber Insurance. In *CIO.* [online] 2013. [18.05.2014]. Dostuné na internete: <http://www.cio.com/article/738144/Rise_in_Data_Breaches_Drives_Interest_in_Cyber_Insurance>
Microsoft. 2013. Prevencia a odstraňovanie vírusov a ďalšieho malvéru. [online] 2013. [cit. 09.05.2014]. Dostupné na internete: <http://support.microsoft.com/kb/129972/sk>
Mittaš, M. 2014. Proti hekerom sa dá aj poistiť!. In *Next Future.* [online] 2014. [16.05.2014]. Dostupné na internete: <http://www.nextfuture.sk/poistovne/clanky/proti-hekerom-sa-da-chranit-aj-poistit/>
Mittaš, M. 2014. Proti hekerom sa dá aj poistiť!. In *Next Future.* [online] 2014. [16.05.2014]. Dostupné na internete: <http://www.nextfuture.sk/poistovne/clanky/proti-hekerom-sa-da-chranit-aj-poistit/>
Ördögh, P. 2014. Čo je to: Počítačová kriminalita a počítačové pirátstvo na Slovensku. In *PENonline.* [online] 2014. [14.05.2014]. Dostupné na internete: <http://www.penonline.sk/analyzy/co-je-co-pocitacova-kriminalita-a-pocitacove-piratstvo-na-slovensku#edn6>
Prolexic. *What is denial of service*. In PLXportal [online] [13.05.2014]. Dostuné na internete: <http://www.prolexic.com/knowledge-center-what-is-ddos-denial-of-service.html>

Revue Priemyslu. 2014. Ochrana osobných údajov: Ďalší strašiak pre firmy. In *Revue Priemyslu.* [online] 2014. [16.05.2014]. Dostupné na internete: <http://www.revuepriemyslu.sk/stories/clanok/aid/22956/Ochrana_osobn%C3%BDch_%C3%BAdajov/%C4%8Eal%C5%A1%C3%AD_stra%C5%A1iak_pre_firmy>
Rundesová, T. 2014. Poistite sa proti hackerom. Ide to aj u nás. In *Hnonline.* [online] 2014. [cit. 12.05.2014]. Dostupné na internete: <http://hnporadna.hnonline.sk/clanky-168/poistite-sa-proti-hackerom-ide-to-aj-u-nas-611750>
Ryba, A. 2014. *Klasické antivírusy sú už odísané a neplnia svoj účel.* [online] 2014. [cit. 14.05.2014]. Dostupné na internete: <http://www.itnews.sk/spravy/bezpecnost/2014-05-07/c163053-symantec-klasicke-antivirusy-su-uz-odpisane-a-neplnia-svoj-ucel>
Ryba, A. 2014. *Únik firemných dát môže spôsobiť prepad cien akcií.*[online] 2014. [cit. 13.05.2014]. Dostupné na internete: <http://www.itnews.sk/spravy/bezpecnost/2014-03-31/c162377-unik-firemnych-dat-moze-sposobit-prepad-cien-akcii>
Sedlák, J. 2014. Firmy budou muset hlásit kybernetické útoky. Hrozi jim pokuta. In *E15* [online] 2014. [cit. 12.05.2014]. Dostupné na internete: <http://e-svet.e15.cz/it-byznys/firmy-budou-muset-hlasit-kyberneticke-utoky-hrozi-jim-pokuta-1050153>
Slovenská asociácia poisťovní. 2013. *Poistné produkty na slovenskom poistnom trhu.* [online]. 2013. [cit. 16.05.2014]. Dostupné na internete: <http://www.slaspo.sk/tmp/asset_cache/link/0000045324/Poistne%20produkty%20na%20SK%20poistnom%20trhu%20k%203103%202013%20na%20web%20stranku%20SLASPO.pdf>
Slovenská sporiteľňa. *Chráňte svoje peniaze bezpečným používaním služieb elektronického bankovníctva.* [online] [cit. 12.05.2014]. Dostupné na internete: <http://www.slsp.sk/vseobecne-bezpecnostne-pravidla-pri-praci-s-internetom-a-sluzbou-internetbanking.html>
Šenkýřová, L. 2013. *Čo je PHISHING alebo ako sa nestať obeťou podvodníkov*. In *Financesk* [online] 2013. [cit. 12.05.2014]. Dostupné na internete: <http://www.finance.sk/spravy/finance/109628-co-je-phishing-alebo-ako-sa-nestat-obetou-podvodnikov/>
TASR. 2014. V IT činnostiach stúpla v januári zamestnanosť medziročne o 4,3%. [online] 2014. [cit. 13.05.2014]. Dostupné na internete: < http://www.zive.sk/clanok/72951/v-it-cinnostiach-stupla-v-januari-zamestnanost-medzirocne-o-4-3>
The Independent IT-Security Institute. 2014. Malware. [online] 2014. [cit 09.05.2014]. <http://www.av-test.org/en/statistics/malware/>

The Statistics Portal. 2014. Global market share held by the leading Windows antivirus application vendors in August 2013. [online] [cit. 16.05.2014]. Dostupné na internete: <http://www.statista.com/statistics/271048/market-share-held-by-antivirus-vendors-for-windows-systems/>

The Travelers Indemnity Company. 2012. Communications & Media Liability. *In Insuring Innovation. CyberFirst®.Coverage for Technology Companies*. [online] 2012. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/business-insurance/specialized-industries/technology/docs/CyberFirst-Suite-locked.pdf>

The Travelers Indemnity Company. 2012. Coverage Advantages. *In Insuring Innovation. CyberFirst®.Coverage for Technology Companies*. [online] 2012. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/business-insurance/specialized-industries/technology/docs/CyberFirst-Suite-locked.pdf>

The Travelers Indemnity Company. 2012. Expense Reimbursement Coverage. In *Insuring Innovation. CyberFirst®.Coverage for Technology Companies*. [online] 2012. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/business-insurance/specialized-industries/technology/docs/CyberFirst-Suite-locked.pdf>

The Travelers Indemnity Company. 2012. Network & Information Security Liability. *In Insuring Innovation. CyberFirst®.Coverage for Technology Companies*. [online] 2012. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/business-insurance/specialized-industries/technology/docs/CyberFirst-Suite-locked.pdf>

The Travelers Indemnity Company. 2012. Technology Errors & Omissions Liability. *In Insuring Innovation. CyberFirst®.Coverage for Technology Companies*. [online] 2012. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/business-insurance/specialized-industries/technology/docs/CyberFirst-Suite-locked.pdf>

The Travelers Indemnity Company: About Travelers. [online] 2014. [cit. 15.05.2014]. Dostupné na internete: <https://www.travelers.com/about-us/index.aspx>

Valášek, M. 2011. Blízka a vzdialená budúcnosť IT. In *TRENDsk.* [online] 2011. [cit. 13.05.2014]. Dostupné na internete: <http://technologie.etrend.sk/it-biznis/blizka-a-vzdialena-buducnost-it-2.html>

Wells, A. 2014. What´s Next for Cyber Insurance? In *Carrier Managenet.*[online] 2014. [18.05.2014]. dostupné na internete: <http://www.carriermanagement.com/features/2014/05/08/122728.htm>

Zlatá minca 2013: Výsledky. In *Zlatá minca.* [online] 2013. [cit. 16.05.2014]. Dostupné na internete: <http://zlataminca.sk/zlata-minca-2013-vysledky/cmsarticle/#.U3XdT7_xp0K>

Zuzčák, M. 2011. Kybernetický útočníci, ich motívy a filozofia. In *SecIT.sk* [online]. 2011. Dostupné na internete: <http://www.secit.sk/sk/content/kyberneticki-utocnici-ich-motivy-filozofia>

www.allianz.sk
www.etrend.sk
www.hnonline.sk
www.itnews.sk
www.munichre.com
www.opoisteni.sk
www.swissre.com