EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA PODNIKOVÉHO MANAŽMENTU

Evidenčné číslo: 104006/D/2017/36069194047305988

MANAŽMENT INFORMAČNEJ BEZPEČNOSTI ELEKTRONICKÉHO PODNIKANIA

Dizertačná práca

2017 **Ing. František Korček**

EKONOMICKÁ UNIVERZITA V BRATISLAVE
FAKULTA PODNIKOVÉHO MANAŽMENTU

MANAŽMENT INFORMAČNEJ BEZPEČNOSTI ELEKTRONICKÉHO PODNIKANIA

Dizertačná práca

Študijný program: Ekonomika a manažment podniku

Študijný odbor: Ekonomika a manažment podniku

Školiace pracovisko: Katedra informačného manažmentu

Školiteľ: doc. Ing. Mojmír Kokles, PhD.

Bratislava 2017 **Ing. František Korček**

Ekonomická univerzita v Bratislave
Fakulta podnikového manažmentu

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta:	Ing. František Korček
Študijný program:	Ekonomika a manažment podniku (Jednoodborové štúdium, doktorandské III. st., denná forma)
Študijný odbor:	3.3.16 Ekonomika a manažment podniku
Typ záverečnej práce:	Dizertačná záverečná práca
Jazyk záverečnej práce:	slovenský
Sekundárny jazyk:	anglický

Názov: Manažment informačnej bezpečnosti elektronického podnikania

Cieľ: Cieľom práce je navrhnúť model manažmentu informačnej bezpečnosti v podnikoch obchodujúcich na elektronickom trhu s využitím normy ISO/IEC 27000.

Anotácia: Dizertačná práca sa zameriava na analýzu rizík elektronického podnikania vo vybraných oblastiach na slovenskom trhu s vyústením do návrhu modelu informačnej bezpečnosti v podnikoch. Práca klasifikuje informačné aktíva, identifikuje hrozby a riziká, ktoré môžu tieto podniky ohrozovať.

Školiteľ:	doc. Ing. Mojmír Kokles, PhD.
Katedra:	KIM FPM - Kat. informacneho manazmentu FPM
Vedúci katedry:	doc. Ing. Mojmír Kokles, PhD.
Dátum zadania:	01.09.2014

Dátum schválenia: 25.03.2014

prof. Ing. Štefan Majtán, PhD.
predseda odborovej komisie

Čestné vyhlásenie

Čestne vyhlasujem, že záverečnú prácu som vypracoval samostatne a že som uviedol všetku použitú literatúru.

Dátum: 26. 06. 2017 .....

Ing. František Korček

Poďakovanie

Na tomto mieste chcem poďakovať doc. Ing. Mojmírovi Koklesovi, PhD., môjmu školiteľovi, za cenné rady, poskytnuté znalosti, skúsenosti a podnecovanie môjho profesijného a osobnostného rozvoja počas doktorandského štúdia. Moje ďakujem patrí členom Katedry informačného manažmentu za osobný prístup, rady, pripomienky a usmernenie pri spracovaní dizertačnej práce. Ďakujem mojej manželke Emílii za trpezlivosť a neustálu podporu. Chcem poďakovať aj rodičom, rodine a priateľom za ochotu pomôcť v rôznych situáciách počas štúdia.

Abstrakt

KORČEK, František: *Manažment informačnej bezpečnosti elektronického podnikania*. – Ekonomická univerzita v Bratislave. Fakulta podnikového manažmentu; Katedra informačného manažmentu. – Školiteľ: doc. Ing. Mojmír Kokles, PhD. – Bratislava: FPM EU, 2017, 155 s.

Hlavným cieľom dizertačnej práce je navrhnúť model manažmentu informačnej bezpečnosti so zameraním na podniky, ktoré pri predaji tovaru a služieb využívajú elektronický trh. Implementovaním modelu podniky zvýšia bezpečnosť informačných aktív, čím eliminujú možné následky existujúcich hrozieb informačnej bezpečnosti. Hlavný cieľ vychádza z komparácie poznatkov súčasného stavu problematiky, je dosiahnutý vhodne zvolenými metódami vedeckej práce a prináša riešenie pre skúmanú oblasť. Dizertačná práca sa zameriava na analýzu rizík elektronického podnikania na slovenskom trhu s využitím noriem rady ISO/IEC 27000.

Práca je rozdelená do 5 kapitol. Obsahuje 23 grafov, 13 obrázkov, 44 tabuliek a 3 prílohy. Prvá kapitola sa zaoberá analýzou a syntézou súčasného stavu poznania manažmentu informačnej bezpečnosti, porovnáva modely manažmentu informačnej bezpečnosti a uvádza prehľad elektronického podnikania na Slovensku a v zahraničí.

V ďalšej kapitole je spolu s určením predpokladov stanovený hlavný cieľ a čiastkové ciele dizertačnej práce spolu s formuláciou troch výskumných hypotéz.

Nasleduje kapitola Metodika práce a metódy skúmania, v ktorej charakterizujeme objekt skúmania, určujeme spôsob získavania údajov pre výskum, opisujeme analyzované premenné a vyberáme metódy pre konkrétne činnosti spracovania dizertačnej práce.

V kapitole Výsledky práce sú s využitím štatistických metód spracované dáta z prieskumu a je uskutočnená analýza a priorizovanie rizík informačnej bezpečnosti, ktoré pôsobia na elektronické podnikanie. V rámci kapitoly verifikujeme alebo falzifikujeme stanovené hypotézy. Získané poznatky vyúsťujú do návrhu kvalitatívneho modelu manažmentu informačnej bezpečnosti elektronického podnikania.

Posledná kapitola predkladá odporúčania k zavedeniu navrhovaného modelu v elektronickom podnikaní, vyhodnocuje získané výsledky, dosiahnuté ciele a identifikuje prínosy dizertačnej práce pre teoretickú, pedagogickú a podnikovú oblasť.

Kľúčové slová: manažment informačnej bezpečnosti, informačné aktívum, hrozba, riziko, bezpečnostné opatrenie, elektronické podnikanie, elektronický obchod

Abstract

KORČEK, František: *E-business information security management.* – University of Economics in Bratislava. Faculty of Business Management; Department of Information Management. – Supervisor: doc. Ing. Mojmír Kokles, PhD. – Bratislava: FPM EU, 2017, 155 p.

The main objective of the dissertation is to design a model of information security management focusing on enterprises that use the electronic market while selling goods and services. By implementing the model, the enterprises will increase security of information assets and eliminate possible consequences of existing information security threats. The main objective is based on the comparison of knowledge gained from the current state of the issue. It is achieved by suitably chosen scientific methods and brings a solution for the studied area. The dissertation focuses on a risk analysis of e–business in the Slovak market using the ISO/IEC 27000 family of standards. The dissertation is divided into 5 chapters. It contains 23 graphs, 13 figures, 44 tables and 3 attachments.

The first chapter deals with the analysis and synthesis of knowledge gained from the current state of information security management, compares information security management models and provides an overview of Slovak and foreign e–business.

In the next chapter, along with the assumptions' determination, the main objective and the partial objectives are set together with the formulation of three research hypotheses.

The following chapter of Methodology and Research Methods characterises an object of research, determines a way of data acquisition for research, describes analysed variables and selects methods for specific activities to process the dissertation.

In the Results chapter, the survey data is processed using statistical methods and the analysis and prioritisation of information security risks involved in e–business are conducted. Within the chapter, the established hypotheses are verified or falsified. The acquired knowledge results in the design of the qualitative model of e–business information security management.

The final chapter presents recommendations for introducing the proposed model in the e–business environment, evaluates the obtained results, the achieved objectives, and identifies benefits of the dissertation for the area of theory, education and business practice.

Key words: information security management, information asset, threat, risk, security control, e–business, e–commerce

Obsah

Zoznam grafov

Zoznam obrázkov

Zoznam tabuliek

Zoznam skratiek

ACL	–	Access Control List
ANOVA	–	Analysis of Variance
APT	–	Advanced Persistent Threat
B2B	–	Business–to–Business
B2C	–	Business–to–Consumer
B2G	–	Business–to–Government
BMIS	–	Business Model for Information Security
BSI	–	Bundesamt für Sicherheit in der Informationstechnik
BYOD	–	Bring Your Own Device
C2B	–	Consumer–to–Business
C2C	–	Consumer–to–Consumer
CCTA	–	Central Communication and Telecommunication Agency
CCTV	–	Closed–Circuit Television
CEO	–	Chief Executive Officer
CIO	–	Chief Information Officer
CIS	–	Center for Information Security
CISO	–	Chief Information Security Officer
CMS	–	Content Management System
COBIT	–	Control Objectives for Information and Related Technologies
CompTIA	–	Computing Technology Industry Association
CRAMM	–	CCTA Risk Analysis and Management Method
CRM	–	Customer Relationship Management
CSET	–	Cyber Security Evaluation Tool
CSIRT	–	Computer Security Incident Response Team
ČR	–	Česká republika
DE	–	Nemecko
DoS	–	Denial of Service
DDoS	–	Distributed Denial of Service
DLP	–	Data Loss Prevention
EBIOS	–	Expression des Besoins et Identification des Objectifs de Sécurité
EFQM	–	European Foundation for Quality Management
ENISA	–	European Union Agency for Network and Information Security
EP	–	Európsky parlament
EPS	–	Elektronická požiarna signalizácia
ERP	–	Enterprise Resource Planning
EÚ	–	Európska únia
EY	–	Ernst & Young
EZS	–	Elektronická zabezpečovacia signalizácia
FAIR	–	Factor Analysis of Information Risk
FISMA	–	Federal Information Security Management Act
HDD	–	Hard Disk Drive
IB	–	Informačná bezpečnosť
ICIIP	–	Institute for Critical Information Infrastructure Protection
IDS	–	Intrusion Detection System
IPS	–	Intrusion Prevention System
IEC	–	International Electrotechnical Commission
IKT	–	Informačno–komunikačné

		Technológie
IRAM2	–	Information Risk Assessment Methodology 2
IS	–	Informačné systémy
ISA	–	International Society of Automation
ISACA	–	Information Systems Audit and Control Association
ISF	–	Information Security Forum
ISMS	–	Information Security Management System
ISO	–	International Organization for Standardization
ISSRM	–	Information System Security Risk Management
IT	–	Informačné technológie
K–S	–	Kolmogorovov–Smirnovov
LAN	–	Local Area Network
M	–	Aritmetický priemer
M_o_R	–	Management of Risk
MAGERIT	–	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
MEHARI	–	Méthode harmonisée d'analyse des risques
MIBEP	–	Manažment informačnej bezpečnosti elektronického podnikania
MSP	–	Malé a stredné podniky
N	–	Veľkosť vzorky
NBÚ	–	Národný bezpečnostný úrad
NACE	–	Štatistická klasifikácia ekonomických činností
NIST	–	National Institute of Standards and Technology
OCTAVE	–	Operationally Critical Threat, Asset and Vulnerability Evaluation
PCI DSS	–	Payment Card Industry Data Security Standard
PCI SSC	–	Payment Card Industry Security Standards Council
PDCA	–	Plan–Do–Check–Act
RAMSES	–	Risk Analysis and Management System for Enhanced Security
RO	–	Register organizácií
SANS	–	SysAdmin, Audit, Network, Security
SD	–	Smerodajná odchýlka
SIEM	–	Security Information and Event Management
SLA	–	Service–Level Agreement
SMS	–	Short Message Service
SP	–	Special Publication
SQL	–	Structured Query Language
SR	–	Slovenská republika
SRIB	–	Systém riadenia informačnej bezpečnosti
SSD	–	Solid State Drive
SSO	–	Single Sign–On
STN	–	Slovenská technická norma
TLS	–	Transport Layer Security
TQISM	–	Total Quality Information Security Management
TQM	–	Total Quality Management
UML	–	Unified Modeling Language
UPS	–	Uninterruptible Power Supply
USA	–	Spojené štáty americké
USC	–	University of Southern California
VPN	–	Virtual Private Network
WAF	–	Web Application Firewall
Wi–Fi	–	Wireless Fidelity

Úvod

Informácia je ústredným pojmom súčasnej spoločnosti, ktorú získavame účelným spájaním dát s využitím informačno–komunikačných technológií. Pretože informácii je priveľké množstvo, je potrebné ich spracovávať, triediť, analyzovať, porovnávať, ale predovšetkým vyberať a ukladať tie podstatné. Ak informácii priradíme zmysel a význam, získame znalosť, ktorá má v spoločnosti veľkú závažnosť, pretože prináša jej vlastníkovi určitú výhodu. Keďže je táto výhoda v spoločnosti viditeľná, vždy sa nájdu protivníci, ktorí ju chcú získať pre seba. Úlohou vlastníka je chrániť svoje znalosti a informácie, z ktorých znalosti pochádzajú.

Rovnako aj podniky sú ako súčasť spoločnosti prelínané informáciami vo všetkých fázach ich životného cyklu a transformačného procesu. Chrániť svoje významné znalosti, dôverné informácie a ostatné informačné aktíva je ich povinnosťou. Ak podnik nadobudne z informácií znalosti, získava konkurenčnú výhodu a dokáže predbehnúť svojich protivníkov. Analogicky, protivníci sa snažia získať výhodu podniku využitím rôznych útokov a hrozieb informačnej bezpečnosti. Manažment informačnej bezpečnosti pomáha podnikom úspešne čeliť hrozbám a ochrániť dôvernosť, dostupnosť a integritu ich dôverných informácií a znalostí na primeranej úrovni.

Pokiaľ budú podnikové procesy podporované IKT, budú stále vznikať nové riziká informačnej bezpečnosti a možnosti úniku alebo straty dôverných informácii. Tento únik alebo strata má za následok vyzradenie obchodného tajomstva, prešetrovanie a čas opravy zraniteľného miesta, stratený pracovný čas, dodatočné finančné náklady, stratu konkurenčnej výhody, príležitostí, dobrého mena a reputácie, zníženie efektivity práce, existenčné problémy a mnohé iné. Preto je nevyhnutné podnik rôznymi spôsobmi chrániť, ideálne vhodným systémom riadenia informačnej bezpečnosti. Tento systém zavádza procesný prístup k manažmentu informačnej bezpečnosti a tým dbá na neustále zlepšovanie kvality ochrany informačných aktív podniku pred rizikami informačnej bezpečnosti.

Na území Slovenskej republiky stále sledujeme nárast vstupu podnikov s rôznymi predmetmi podnikania na elektronický trh tovaru a služieb. Dôvody sú jednoznačné, ide o mnohonásobné rozšírenie trhu, zlepšenú konkurencieschopnosť a marketing podniku, zvýšené povedomie potenciálnych zákazníkov o značke, nárast počtu objednávok a s tým súvisiaci nárast tržieb, atď. Avšak mnohé začínajúce, ale aj etablované podniky si dostatočne neuvedomujú, že podnikanie na elektronickom trhu, ktorý je súčasťou kybernetického priestoru, prináša stále nové a zároveň odlišné hrozby ako sú hrozby pri bežnom podnikaní.

V nepripravených podnikoch sa hrozby informačnej bezpečnosti môžu jednoducho realizovať vo forme bezpečnostných incidentov. Takéto podniky nemajú dostatok znalostí o hrozbách a bezpečnostných incidentoch a o pokročilých možnostiach zabezpečenia ich informačných aktív predovšetkým v dôsledku neidentifikovanej potreby riešiť problematiku informačnej bezpečnosti vedením podniku, ale aj v dôsledku nedostatku finančných a materiálnych zdrojov, nekvalifikovanosti a neskúsenosti zamestnancov a i. Spomenuté nedostatky sú bežné aj v podnikoch, na ktoré smerujeme výskumné ciele dizertačnej práce, teda podniky využívajúce elektronický obchod na slovenskom území. Téma je aktuálna pre všetky podniky na slovenskom elektronickom trhu z dôvodu potreby zabezpečenia ich informačných aktív znížením pravdepodobnosti alebo následkov možných a narastajúcich rizík informačnej bezpečnosti.

Ponuka tovaru a služieb zákazníkom na internete, teda zavedenie a aktívne používanie elektronického obchodu je nepochybne moderný spôsob ponúkania tovaru a služieb. Zabezpečenie interných alebo externých hrozieb, prostredia, zariadení, podnikových procesov, obchodného tajomstva a dodávateľsko–odberateľských vzťahov môže byť v súčasných podnikoch rýchlo zastarané pre neustály a rýchly rozvoj IKT. Preto je potrebné preskúmať a vyhodnotiť aktuálny stav manažmentu informačnej bezpečnosti v podnikoch realizujúcich svoje obchodné aktivity na elektronickom trhu a vytvoriť model, ktorého implementácia v podnikoch minimalizuje celkovú úroveň rizika a maximalizuje bezpečnosť informačných aktív za akceptovateľné náklady.

Viaceré organizácie, ktoré sa zaoberajú systémovým prístupom k informačnej bezpečnosti v podnikoch na národnej alebo medzinárodnej úrovni, vytvárajú odporúčania, metodiky, postupy a procedúry, prípadne normy a zákony, ktoré nie sú vždy aplikovateľné na podmienky skúmaných podnikov z dôvodu ich všeobecnosti, zložitosti, zamerania na profesionálov v oblasti informačnej bezpečnosti alebo nákladovej náročnosti. Tento stav nás podnecuje ku vytvoreniu komplexného riešenia manažmentu informačnej bezpečnosti elektronického podnikania pre vybraný objekt skúmania, ktorým sú podniky obchodujúce na slovenskom elektronickom trhu.

Dizertačná práca je rozdelená do piatich nadväzujúcich kapitol. V prvej kapitole analyzujeme, porovnávame a spájame poznatky z dostupných vedeckých a odborných zdrojov za účelom nadobudnúť prehľad o súčasnom stave riešenej problematiky v Slovenskej republike a zahraničí. Zameriavame sa na teoretické východiská manažmentu informačnej bezpečnosti ako systému, existujúce normy a štandardy, proces posúdenia a ošetrenia rizík informačnej bezpečnosti, bezpečnostné incidenty a výber ochranných

opatrení. Ďalej analyzujeme a porovnávame existujúce modely manažmentu informačnej bezpečnosti, definujeme elektronické podnikanie, vytvárame prehľad elektronických obchodov na Slovensku, identifikujeme informačné aktíva podnikov na elektronickom trhu a využívané opatrenia na zabezpečenie aktív pred rizikami informačnej bezpečnosti.

Kapitola o súčasnom stave riešenej problematiky slúži ako podklad pre vytvorenie predpokladov a formuláciu vedeckých cieľov a hypotéz, ktoré sú spracované v druhej kapitole. Predpoklady a stanovené hypotézy sú podporené viacerými prieskumami organizácií, vedeckými prácami a tvrdeniami viacerých autorov publikujúcich v oblasti informačnej bezpečnosti.

Metodika práce a metódy skúmania je kapitola, kde charakterizujeme objekt skúmania, určujeme postup spracovania jednotlivých častí práce a spôsoby získavania údajov s ich zdrojmi. Ďalej stanovujeme výber metodiky pre analýzu rizík informačnej bezpečnosti podnikov na slovenskom elektronickom trhu a uvádzame použité všeobecné a špeciálne metódy skúmania pre konkrétne časti práce.

V kapitole Výsledky práce sú za pomoci štatistických metód a vybranej metodiky pre analýzu rizík spracované dáta z dotazníkového prieskumu, ktorých analýza vstupuje do návrhu modelu manažmentu informačnej bezpečnosti elektronického podnikania v závere kapitoly. V tejto kapitole testujeme stanovené hypotézy, analyzujeme informačné aktíva a hrozby informačnej bezpečnosti, vyhodnocujeme miery rizík informačnej bezpečnosti skúmaných podnikov, analyzujeme využívané bezpečnostné opatrenia a následne navrhujeme výber primeraných opatrení na zníženie miery rizika.

Záverečnou kapitolou dizertačnej práce je Diskusia, ktorá predkladá odporúčania k implementácii navrhnutého modelu v podnikoch a vyhodnocuje dosiahnuté výsledky, splnenie predpokladov a stanovených výskumných cieľov. Na konci kapitoly identifikujeme prínosy výsledkov dizertačnej práce pre teoretickú, pedagogickú a podnikovú oblasť.

Dovoľujeme si tvrdiť, že manažment informačnej bezpečnosti je v podmienkach podnikov, ktoré aktívne obchodujú na slovenskom elektronickom trhu, ešte málo známy a rozhodne nevyužívaný. Chýba adekvátne bezpečnostné povedomie oproti hrozbám súvisiacim s rozmachom IKT. Z pohľadu veľkosti podniku sa všeobecne predpokladá, že čím je podnik väčší, tým sa viac zaoberá informačnou bezpečnosťou. Zraniteľné aktíva je však potrebné zabezpečiť v každom podniku, pretože následky zneužitia môžu byť až existenčné. Uvedené výroky v rámci dizertačnej práce dokazujeme a navrhujeme vhodné riešenie danej situácie. Výsledky práce a návrhy obohacujú nielen teoretickú a pedagogickú oblasť, ale aj podnikovú prax.

1 Súčasný stav riešenej problematiky doma a v zahraničí

Informácia je aktívum, ktoré musí byť v narastajúcom a prepojenom podnikateľskom prostredí vhodne chránené.[1] Téma informačnej bezpečnosti je pre podniky vysoko aktuálna, pretože denne spracúvajú a triedia množstvo informácií, z ktorých mnohé sú považované za dôverné. Takéto informácie chcú podniky z rozličných dôvodov utajiť pred nezainteresovanými osobami, pretože ich strata, vyzradenie alebo odcudzenie môže viesť ku kríze podniku. Bezpečnosť informácií je potrebné riadiť, ideálne vytvorením systému riadenia informačnej bezpečnosti. V tejto kapitole priblížime a vyhodnotíme súčasný stav problematiky manažmentu informačnej bezpečnosti so zameraním na podniky, ktorých jeden zo spôsobov ponuky tovaru a služieb je prostredníctvom elektronického obchodu.

1.1 Manažment informačnej bezpečnosti

Informácie sú dôležitou súčasťou každého podniku. Získavanie, spracovanie, uchovávanie a utajovanie informácií patria medzi najdôležitejšie činnosti života podniku.[2] Na ich zabezpečenie je nevyhnutná starostlivosť o technické zariadenia, ktoré slúžia na prístup k informáciám, vhodné nastavenie systému nakladania s informačnými nosičmi a dodržiavanie organizačných princípov na ochranu pred vznikom škôd. Ochrana informácií je potrebná vo vzťahu ku každej zainteresovanej strane, napríklad ku zákazníkom, zamestnancom, obchodným partnerom, dodávateľom, atď. Bezpečnostné nedostatky vyplývajú z nedostatočného docenenia dôležitosti manažmentu informačnej bezpečnosti.[3] S rozvojom IKT a konkurencie je nutné prikladať ochrane dôverných informácií čoraz väčší význam, pretože IKT sa stali nástrojom alebo predmetom počítačovej kriminality.[4] Podľa spoločnosti Ernst & Young existuje 5 hlavných dôvodov, prečo by sa podniky mali zaoberať informačnou bezpečnosťou:[5]

---

[1] SAID, A. R., et al. 2013. Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation. In *Taylor´s 6th Teaching and Learning Conference 2013: Transformative Higher Education Teaching and Learning in Practice (TTLC 2013)*, Selangor: Taylor´s University, 2013. p. 435.

[2] KOKLES, M. – KORČEK, F. 2015. Analýza rizík informačnej bezpečnosti v malých a stredných podnikoch. In *Ekonomika a manažment: Vedecký časopis Fakulty podnikového manažmentu Ekonomickej univerzity v Bratislave.* ISSN 1336-3301, 2015, roč. 12, č. 1, s. 38.

[3] STEHLÍKOVÁ, B. – HOROVČÁK, P. 2012. Manažment informačnej bezpečnosti v malých a stredných podnikoch. In *Security Revue* [online]. 2012 [cit. 2015-12-01]. Dostupné na internete: <http://www.securityrevue.com/article/2012/06/manazment-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch/>.

[4] KOKLES, M. – ROMANOVÁ, A. 2014. *Informatika.* Bratislava: Sprint 2, 2014. s. 225. ISBN 978-80-89710-13-3.

[5] EY. 2014 (a). *Cyber Threat Intelligence – how to get ahead of cybercrime*. [online]. 2014 [cit. 2015-12-01] Dostupné na internete: <http://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf>.

- *Zmena* – zrýchlenie podnikov v období po ekonomickej kríze je zapríčinené vznikom nových produktov, nových fúzií, akvizícií, expanzie trhu a nových technológií. Zmeny majú komplikovaný priebeh a množstvo negatívnych následkov na informačnú bezpečnosť podniku,
- *Ekosystém* – žijeme v ekosystéme digitálne prepojených objektov, ľudí a dát. Pravdepodobnosť vystavenia sa počítačovej kriminalite platí rovnako pre pracovné, ako aj domáce prostredie,
- *Infraštruktúra* – prístup na internet je dnes umožnený aj tradičným uzatvoreným operačným technológiám, preto sa hrozby informačnej bezpečnosti dostávajú do kľúčových infraštruktúr, napríklad do dopravných systémov, automatických systémov, distribúcie elektrickej energie, ale aj do systémov v domácnostiach,
- *Cloud* – služby založené na princípe riadenia a skladovania dát treťou stranou dávajú priestor novým rizikám, ktoré predtým nejestvovali,
- *Mobilita a orientácia na zákazníka* – spoločenské prijatie mobilnej výpočtovej techniky spôsobuje zánik podnikových hraníc a priblíženie IT viac k používateľovi ako k podniku. Výsledkom používania internetu, smartfónov a tabletov v kombinácii s pozitívnym prístupom podnikov ku BYOD, je dostupnosť podnikových dát prakticky neobmedzená.

Informatizácia spoločnosti nabáda podniky bez ohľadu na ich veľkosť alebo zameranie, aby si problematiku kvalitnej bezpečnosti informačných aktív a citlivých dát urýchlene osvojili. Z historického hľadiska sa informačnou bezpečnosťou ako prvé začali zaoberať veľké podniky, pretože denne spracovali veľké množstvo dát. Väčšie a bohatšie podniky mali dostatok zdrojov na investície do zabezpečenia aktív. Malé a stredné podniky si mylne mysleli, že kybernetické hrozby smerujú len na veľké podniky. Stále viac útočníkov sa sústreďuje práve na MSP, pretože nedostatočne chránia svoje citlivé dáta.[6] Podniky sa stretávajú s rizikami narušenia IB čoraz častejšie, ale mnohé z nich ani nestihnú reagovať, keď bezpečnostný incident nastane.[7] V dôsledku expanzie počítačových sietí a internetu sú podniky náchylnejšie na útoky smerované na dôverné informácie, dáta, informačné systémy[8], IKT a zamestnancov.

[6] KRÁL, D. 2011. Information Security in Small and Medium-Sized Companies. In *ACTA VŠFS*. ISSN 1802-792X, 2011, roč. 5, č. 1, s. 62.
[7] HUO, C. – MENG, L. – CHEN, K. 2015. Research on the University Network Information Security Risk Management Model Based on the Fuzzy Sets. In *International Conference on Automation, Mechanical Control and Computational Engineering AMCEE*. Ji´nan: Atlantis Press, 2015. ISBN 978-94-62520-64-6, p. 89.
[8] BOLEK, V. – KORČEK, F. – BEŇOVÁ, M. 2015. Information security risk management in Slovak enterprises. In *CER Comparative European Research 2015: proceedings of the 4th biannual CER conference*. [online]. London: Sciemcee

Chrániť informačné aktíva podnikov pred hrozbami informačnej bezpečnosti je možné aplikovaním systémového prístupu. Problematikou sa podrobne zaoberá manažment informačnej bezpečnosti. Nižšie uvádzame definície z rôznych zdrojov:

- Norma ISO/IEC 27001 definuje manažment informačnej bezpečnosti ako systém (ISMS – Information Security Management System), ktorý „chráni dôvernosť, dostupnosť a integritu informácií zavedením procesu riadenia rizík a poskytnutím dôvery zainteresovaným stranám, že riziká sú dostatočne riadené,“[9]
- Spoločnosť ESET považuje ISMS za základňu pre riadenie bezpečnostných rizík, ktorej cieľom je zriadiť, implementovať, prevádzkovať, monitorovať, revidovať, udržiavať a zlepšovať informačnú bezpečnosť v organizácii,[10]
- Podľa agentúry EÚ pre sieťovú a informačnú bezpečnosť ENISA, manažment informačnej bezpečnosti predstavuje systém, ktorý umožňuje dosiahnuť požadované kvalitatívne charakteristiky služieb ponúkaných v organizáciách (napríklad dostupnosť služieb, zachovanie dôvernosti a integrity dát, atď.),[11]
- Singh a kol. tvrdia, že ISMS je systém vyváženého prelínania technických, manažérskych a ľudských aspektov informačnej bezpečnosti v organizácii,[12]
- Ondrák a kol. vníma ISMS ako efektívny dokumentovaný systém správy informačných aktív s cieľom eliminovať ich možnú stratu alebo poškodenie.[13]

Podľa uvedených definícií tvrdíme, že ISMS je uceleným systémom v rámci celkového systému riadenia organizácie, ktorý chráni informácie pred rizikami. Zároveň, pri správe bezpečnosti nejde len o zavedenie technických opatrení, ale najmä o manažment, čo potvrdzuje agentúra ENISA v nasledujúcich osvedčených pravidlách pre ISMS:[14]

- Správcovia bezpečnosti IS a IKT strávia približne dve tretiny z pracovného času vytváraním politík, procedúr, bezpečnostných kontrol, analýz rizík a zvyšovaním povedomia o bezpečnosti. Iba tretinu z času venujú riešeniu technických záležitostí,

publishing, 2015, p. 13-16 [cit. 2015-12-01]. Dostupné na internete: <http://www.sciemcee.org/library/proceedings/cer/cer2015_proceedings02.pdf>. ISBN 978-0-9928772-8-6.

[9] STN ISO/IEC 27001: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Požiadavky.*

[10] ESET. 2014. *Systém riadenia informačnej bezpečnosti.* [online]. 2014 [cit. 2015-12-01]. Dostupné na internete: <http://static1.esetstatic.com/uploads/media/System_riadenia_informacnej_bezpecnosti.pdf>.

[11] ENISA. 2015 (a). *The ISMS Framework.* [online]. 2015 [cit. 2015-12-01]. Dostupné na internete: <https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/framework>.

[12] SINGH, A. N. et al. 2013. Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. In *Global Journal of Flexible Systems Management*. ISSN 0972-2696, 2013, vol. 14, no. 4, p. 226.

[13] ONDRÁK, V. – SEDLÁK, P. – MAZÁLEK, V. 2013. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. s. 66. ISBN 978-80-7204-872-4.

[14] ENISA. 2015 (b). *The Need for ISMS.* [online]. 2015 [cit. 2015-12-01]. Dostupné na internete: <https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/need>.

- Bezpečnosť závisí viac na ľuďoch ako na technológii,
- Zamestnanci sú oveľa väčšia hrozba ako externé osoby,
- Sila bezpečnosti je definovaná jej najslabším článkom,
- Úroveň bezpečnosti závisí na troch faktoroch – ochote podstúpiť riziko, funkciách systému a vynaložených nákladoch,
- Bezpečnosť nie je stav, ale neustály proces.

Zavedenie, údržba a neustála aktualizácia ISMS indikuje systémový prístup podnikov ku identifikácii, posúdeniu a riadeniu rizík informačnej bezpečnosti.[15] Systém riadenia informačnej bezpečnosti prináša obchodnú kontinuitu, konkurencieschopnosť, ziskovosť, prestíž, elimináciu hrozieb a strát plynúcich z realizovaných rizík.

1.1.1 Východiská, ciele a požiadavky informačnej bezpečnosti

Norma ISO/IEC 27000 definuje informačnú bezpečnosť ako zachovanie dôvernosti, bezúhonnosti (integrity) a dostupnosti informácií. K tejto definícii zahŕňa aj ďalšie vlastnosti ako „pravosť, zodpovednosť, nepopierateľnosť a spoľahlivosť.“[16] Dostupnosť predstavuje zaistenie prístupu k informácii v požadovaný okamih. Účelom dôvernosti je zaistenie prístupu k informácii len oprávnenému používateľovi a bezúhonnosť (resp. integrita) zabezpečuje správnosť a úplnosť informácie.[17] Prikláňame sa k tvrdeniu Čermáka, že je nutné vytvoriť také opatrenia, aby nedošlo k narušeniu uvedených troch charakteristík informácií,[18] ktoré musia existovať v súlade. Ak je iba jedna charakteristika narušená, celá IB podniku je v ohrození. Ak je informácia odhalená neoprávnenému používateľovi alebo oprávnený používateľ nedostane požadovanú informáciu v čase, kedy ju potrebuje, prípadne dostane nesprávnu a neúplnú informáciu, nastáva zlyhanie bezpečnosti.

Systémy s vynikajúcou úrovňou dostupnosti neustále poskytujú relevantnú informáciu pre autorizovaných používateľov. Príkladom opatrenia pre udržanie dostupnosti sú zálohovacie systémy a využitie cloudových služieb proti distribuovaným útokom odmietnutia služby (DDoS). Systémy s vynikajúcou úrovňou dôvernosti sú schopné predvídať a zamedziť neoprávnenému zverejneniu informácii. Bežným opatrením na zachovanie dôvernosti je šifrovanie a dvojfaktorová autentizácia založená na bezpečnom

[15] ENISA. 2015 (b). *The Need for ISMS.* [online]. 2015 [cit. 2015-12-01]. Dostupné na internete: <https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/need>.
[16] STN ISO/IEC 27000: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnéj bezpečnosti – Prehľad a slovník.*
[17] ONDRÁK, V. – SEDLÁK, P. – MAZÁLEK, V. 2013. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. s. 15. ISBN 978-80-7204-872-4.
[18] ČERMÁK, M. 2009. *Řízení informačních rizik v praxi.* Brno: Tribun EU, 2009. s. 12. ISBN 978-80-7399-731-1.

hesle a zasielaní autentizačných SMS správ. Nakoniec, systémy s vynikajúcou úrovňou bezúhonnosti lepšie predvídajú a zabraňujú nesprávnej úprave informácie, chybovosti alebo odstráneniu. Niektoré úpravy informácie sú náhodné, iné sú výsledkom úmyselného napadnutia neautorizovaným používateľom. Bežným opatrením je elektronický podpis alebo antivírové programy, ktoré bránia vírusom dáta pozmeniť alebo odstrániť.[19]

Podľa Hudeca je informačná bezpečnosť „dosiahnutá zavedením vhodnej sady opatrení, vrátane politiky, procesov, procedúr, organizačných štruktúr, softvérových a hardvérových funkcií. Je potrebné tieto opatrenia stanoviť, realizovať, monitorovať, preskúmať a zlepšiť, kde je to nutné, aby sa zabezpečilo, že sú splnené špecifické bezpečnostné ciele a poslanie organizácie.“[20] IB je vo vzťahu s bezpečnosťou celej organizácie a zahŕňa bezpečnosť IS, ktorá je však zameraná iba na aktíva IS podporované IKT. Taktiež chráni aj informácie v nedigitálnej podobe.[21] Pri skúmaní IB sa bežne stretávame s pojmom kybernetická bezpečnosť, ktorý je Výkladovým slovníkom kybernetickej bezpečnosti definovaný ako súhrn právnych, organizačných, technických a vzdelávacích prostriedkov smerujúcich k zabezpečeniu ochrany kybernetického priestoru.[22] Kybernetická bezpečnosť je jednou z domén IB a pôsobí len v kybernetickom priestore, čiže v digitálnom prostredí.[23] Na druhej strane, informačná bezpečnosť má vo svojej pôsobnosti nielen IS a dáta podniku, ale aj IKT, celé interné prostredie a okolie podniku so zainteresovanými stranami.

Zhrnutím vyššie uvedených poznatkov získavame cieľ IB, ktorým je chrániť dôvernosť, dostupnosť a integritu informácií v akejkoľvek podobe. Podniky potrebujú pri plánovaní dosiahnutia cieľov IB určiť rozsah činností, zdroje, zodpovednosť, termíny realizácie a spôsoby vyhodnotenia výsledku. Podľa normy ISO/IEC 27001 ciele musia:[24]

- Byť v súlade s politikou informačnej bezpečnosti,
- Byť merateľné, pokiaľ je možné ciele merať,
- Byť oznámené,

[19] HARTONO, E., et al. 2014. Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. In *Decision Support Systems.* [online]. 2014, vol. 62, s. 13 [cit. 2014-11-16]. Dostupné na internete: <http://www.sciencedirect.com/science/article/pii/S0167923614000396>. ISSN 0167-9236.
[20] HUDEC, L. 2014. *Manažment informačnej bezpečnosti.* [online]. 2014 [cit. 2015-12-01]. Dostupné na internete: <http://www.informatizacia.sk/ext_dok-prezgr_manazment_ib/17907c>.
[21] ONDRÁK, V. – SEDLÁK, P. – MAZÁLEK, V. 2013. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. s. 13. ISBN 978-80-7204-872-4.
[22] JIRÁSEK, P. – NOVÁK, L. – POŽÁR, J. 2015. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2015. s. 69. ISBN 978-80-7251-436-6.
[23] CYBERSECURITY. 2016. *Cyber Security (Kybernetická bezpečnost)*. [online]. 2016 [cit. 2017-02-27]. Dostupné na internete: <http://www.cybersecurity.cz/basic.html>.
[24] STN ISO/IEC 27001: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Požiadavky.*

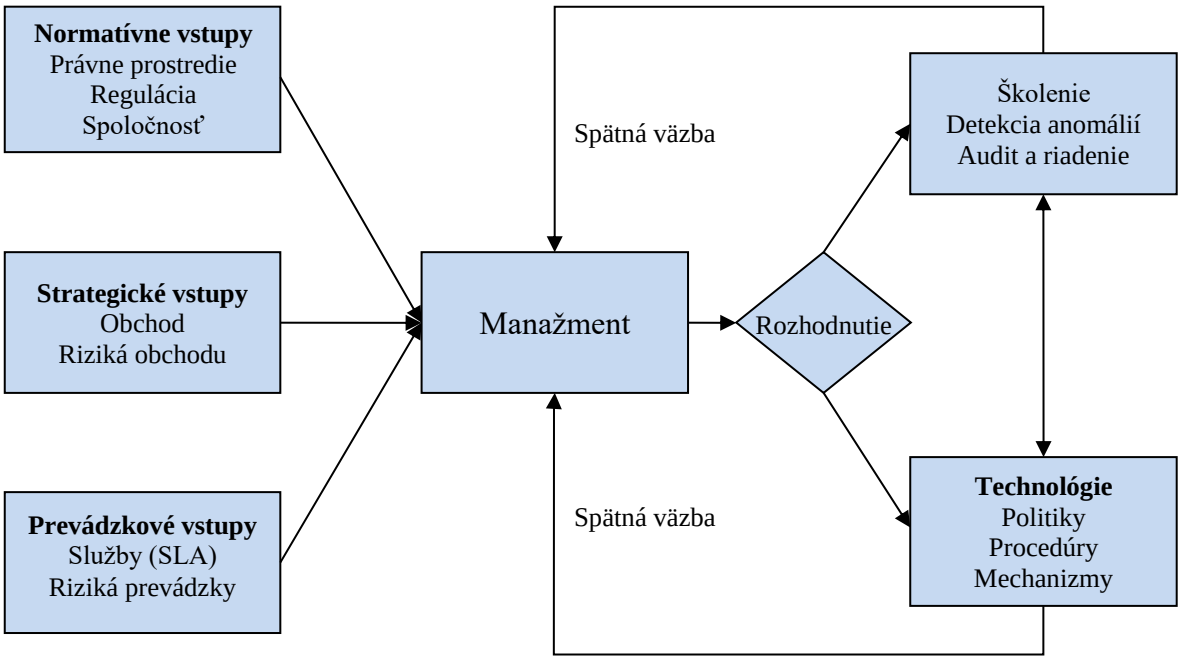
- Byť primerané aktualizované,
- Brať do úvahy výsledky z procesov posúdenia a ošetrenia rizík.

Okrem stanovení cieľov je povinnosťou podnikov zistiť svoje bezpečnostné požiadavky. Požiadavky zjednodušene identifikujú potrebu vykonania určitých činností, ktoré sú zásadné pre zaistenie adekvátnej úrovne informačnej bezpečnosti. Norma ISO/IEC 27002 určuje tri hlavné zdroje požiadaviek bezpečnosti:[25]

- Posúdenie rizík organizácie, ktorým sa identifikujú hrozby na zraniteľnosť aktív, a vyhodnocuje sa ich pravdepodobnosť výskytu s odhadom možných následkov,
- Zákonné, štatutárne, regulačné a zmluvné požiadavky, ktoré musí organizácia a zainteresované strany splniť,
- Súbor cieľov, princípov a obchodných požiadaviek na prácu s informáciami, ich spracovaním a ukladaním, ktoré organizácia vytvorila na podporu jej prevádzky.

1.1.2 Štruktúra a rámec manažmentu informačnej bezpečnosti

Pre hlbšie pochopenie vstupov, výstupov a jednotlivých prvkov v systéme riadenia informačnej bezpečnosti uvádzame jeho štruktúru na obrázku 1.

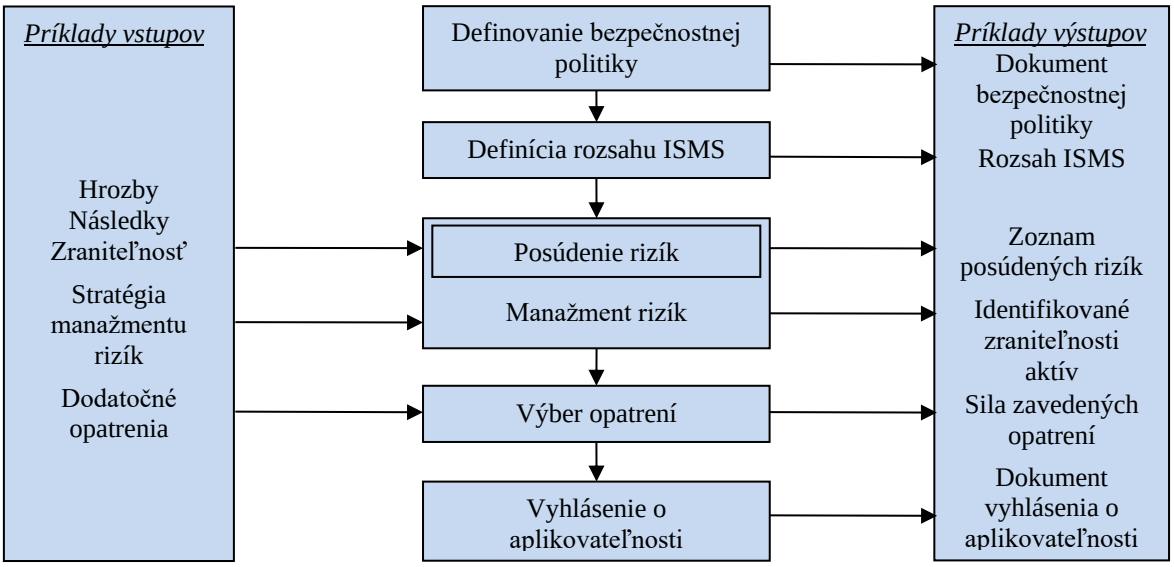


Obr. 1: Štruktúra ISMS
Zdroj: ONDRÁK, V. – SEDLÁK, P. – MAZÁLEK, V. 2013. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. s. 15. ISBN 978-80-7204-872-4.

[25] STN ISO/IEC 27002: 2014: *Informačné technológie – Bezpečnostné metódy – Pravidlá dobrej praxe riadenia informačnej bezpečnosti.*

ISMS má svoje normatívne, strategické a prevádzkové vstupy, ktoré pozostávajú z podnikateľsko–právneho prostredia, rizík informačnej bezpečnosti, požiadaviek organizácie, špecifík trhu, atď. Systém vstupy transformuje na výstupy za pomoci vhodného manažmentu. Manažment rozhoduje o najvhodnejších a najefektívnejších výstupoch, ktoré môže získať a implementovať. Výstupy ISMS obsahujú školenia, audit, politiky, opatrenia, procedúry, bezpečnostné mechanizmy, atď. Po aplikácii výstupov v podniku, manažment získa spätnú väzbu vo forme vyhodnotenia realizovaných výstupov, prípadne splnených metrík, a následne môže vytvoriť nové rozhodnutia s ohľadom na možnú zmenu vstupov. Tento proces zachováva funkčnosť celého systému riadenia informačnej bezpečnosti.

ISMS je súčasťou riadenia podniku a zameriava sa na ustanovenie, zavedenie, prevádzku, monitorovanie, preskúmanie, údržbu a zlepšovanie IB. Postihuje oblasť IT bezpečnosti, komunikačnej bezpečnosti, personálnej bezpečnosti, administratívnej bezpečnosti, fyzickej bezpečnosti, dokumentácie a oblasť bezpečnostných funkcií a mechanizmov.[26] Jeho úlohou je zaviesť pravidlá a postupy pre riadenie IB organizácie.[27]



Obr. 2: Rámec ISMS
Zdroj: ENISA. 2015 (a). *The ISMS Framework.* [online]. 2015 [cit. 2015-12-02]. Dostupné na internete: <https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/framework>.

Rámec ISMS, ktorý je zobrazený na obrázku 2, dokumentuje proces realizácie ISMS po jednotlivých etapách. Rámec nie je daný iba veľkosťou podniku, ale aj špecifickými podnikateľskými aktivitami, ktoré diktujú bezpečnostné požiadavky na legislatívnej,

[26] ONDRÁK, V. – SEDLÁK, P. – MAZÁLEK, V. 2013. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. s. 66.. ISBN 978-80-7204-872-4.
[27] NOVÁK, L. – POŽÁR, J. 2011. *Systém řízení informační bezpečnosti*. [online]. 2011 [cit. 2015-12-02]. Dostupné na internete: <http://www.cybersecurity.cz/data/SRIB.pdf>.

regulačnej a operatívnej úrovni.[28] Prvou etapou procesu manažmentu informačnej bezpečnosti podľa rámca ISMS je vytvorenie bezpečnostnej politiky, ktorá definuje ciele, požiadavky a stratégiu ISMS a ustanovuje kritéria pre hodnotenie rizík. Nasleduje vymedzenie rozsahu a hraníc na základe požiadaviek podniku. Výstupom je rozsah ISMS, ktorý vychádza z cieľov a požiadaviek podniku. Do tretej etapy, ktorá riadi identifikované riziká, vstupujú hrozby, ich následky a zraniteľnosti informačných aktív. Posúdenie rizík predstavuje základ celého systému. Ďalšia etapa sa zameriava na výber vhodných opatrení na elimináciu a zvládanie posúdených rizík. Výstupom je úroveň bezpečnosti, ktorú vytvárajú implementované opatrenia. Posledným výstupom a etapou je dokument vyhlásenia o aplikovateľnosti.[29] Dokument opisuje „ciele riadenia a opatrenia, ktoré sú relevantné a použiteľné pre ISMS organizácie.“[30] Pre optimálne zabezpečenie informácií je potrebné tento proces v podnikoch opakovať, pretože podnikateľské prostredie je nestabilné, neustále sa mení. Rovnako sa menia a vyvíjajú hrozby informačnej bezpečnosti, ktoré aktívne pôsobia na zraniteľnosť informačných aktív podniku.

1.1.3 Legislatíva a normy manažmentu informačnej bezpečnosti

Manažmentom informačnej bezpečnosti sa zaoberajú mnohé medzinárodné organizácie, orgány štátnej správy a inštitúcie. Navrhujú zákony a vydávajú štandardy, normy, rámce, smernice, metodické pokyny a stratégie k problematike zabezpečenia informácii a jej konkrétnym oblastiam. V nasledujúcej tabuľke sa nachádza prehľad tých organizácií a orgánov štátnej správy s ich najvýznamnejšími dielami, ktoré v posledných rokoch ovplyvnili ochranu kybernetického priestoru. Pre porovnanie uvádzame významné dokumenty zo Slovenska a susednej Českej republiky.

Tab. 1: Organizácie aktívne v oblasti ISMS

Organizácia	Legislatíva alebo norma
Medzinárodná organizácia pre normalizáciu (ISO), Medzinárodná elektrotechnická komisia (IEC)	• Normy rady ISO/IEC 27000 – podrobne definujú oblasti ISMS
Medzinárodná spoločnosť pre automatizáciu (ISA)	• Normy rady ISA/IEC-62443 – postupy pre zabezpečenie systémov priemyselnej automatizácie
Organizácia ISACA	• COBIT 5 for Information Security – profesionálny rámec IB
Organizácia CompTIA	• Channel Standard: Cybersecurity – norma kybernetickej bezpečnosti dodávky IT riešení
Organizácia PCI SSC	• PCI DSS – norma dátovej bezpečnosti platobných kariet

[28] ENISA. 2015 (a). *The ISMS Framework.* [online]. 2015 [cit. 2015-12-02]. Dostupné na internete: <https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/framework>.
[29] NOVÁK, L. – POŽÁR, J. 2011. *Systém řízení informační bezpečnosti*. [online]. 2011 [cit. 2015-12-02]. Dostupné na internete: <http://www.cybersecurity.cz/data/SRIB.pdf>.
[30] STN ISO/IEC 27000: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Prehľad a slovník.*

Organizácia	Legislatíva alebo norma
Organizácia ISF	• The Standard of Good Practice for Information Security – norma osvedčených postupov pre informačnú bezpečnosť
Centrum pre informačnú bezpečnosť (CIS), Inštitút SANS	• The CIS Critical Security Controls for Effective Cyber Defense – skupina kritických bezpečnostných opatrení pre efektívnu kybernetickú obranu
Národný inštitút štandardov a technológie (NIST), Ministerstvo obchodu USA	• Federálny zákon o riadení informačnej bezpečnosti (FISMA) • NIST SP 800-53 – opatrenia bezpečnosti a ochrany súkromia pre federálne informácie a informačné systémy • NIST SP 800-37 – návod pre zavedenie rámca pre riadenie rizík pre federálne informačné systémy • Cybersecurity Framework – rámec kybernetickej bezpečnosti zameraný na kritickú infraštruktúru
Európska komisia, Európsky parlament a Rada EÚ, Európska agentúra pre bezpečnosť sietí a informácií (ENISA)	• Stratégia kybernetickej bezpečnosti Európskej únie: Otvorený, bezpečný a chránený kybernetický priestor • Nariadenie EP a Rady (EÚ) č. 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov • Smernica EP a Rady (EÚ) č. 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
Federálny úrad pre informačnú bezpečnosť DE (BSI)	• Normy rady BSI-Standard 100 – detailné pokyny pre ISMS • BIS-Standard 200-3 – norma rizikového manažmentu
Národní bezpečnostní úřad ČR, Národní centrum kybernetické bezpečnosti ČR	• Zákon č. 181/2014 Sb. o kybernetické bezpečnosti • Vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti
Úrad podpredsedu vlády SR pre investície a informatizáciu, Ministerstvo financií SR	• Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy • Výnos č. 55/2014 Z. z. o štandardoch pre informačné systémy verejne správy
Úrad na ochranu osobných údajov SR	• Zákon č. 122/2013 Z. z. o ochrane osobných údajov • Vyhláška č. 164/2013 Z. z. o rozsahu a dokumentácii bezpečnostných opatrení
Národný bezpečnostný úrad SR	• Koncepcia kybernetickej bezpečnosti SR na roky 2015–2020 • Akčný plán realizácie Koncepcie kybernetickej bezpečnosti • Návrh zákona o kybernetickej bezpečnosti

Zdroj: CSIRT.SK. 2017 (a). *Organizácie*. [online]. 2017 [cit. 2017-02-26]. Dostupné na internete: <https://www.csirt.gov.sk/informacna-bezpecnost/zahranicne-zdroje/organizacie-85e.html>.; CSIRT.SK. 2017 (b). *Štandardy informačnej bezpečnosti*. [online]. 2017 [cit. 2017-02-26]. Dostupné na internete: <https://www.csirt.gov.sk/bezpecnostna-studovna/sulad/standardy-informacnej-bezpecnosti-877.html>.; ÚOOÚ SR. 2017. *Národný právny rámec.* [online]. Úrad na ochranu osobných údajov Slovenskej republiky, 2017 [cit. 2017-06-15]. Dostupné na internete: <https://dataprotection.gov.sk/uoou/sk/content/narodny-pravny-ramec>.; NBÚ SR. 2016. *Strategické dokumenty.* [online]. Národný bezpečnostný úrad, 2016 [cit. 2017-02-27]. Dostupné na internete: <http://www.nbusr.sk/kyberneticka-bezpecnost/strategicke-dokumenty/index.html>.

Viacero uvedených organizácií a štátnych orgánov čerpá informácie práve z noriem rady ISO/IEC 27000, ktoré však vo svojich dokumentoch obohacujú, rozširujú a detailizujú, pretože normy ISO/IEC 27000 sú všeobecné a výber metód, opatrení a postupov ponechávajú na samotné organizácie s možnosťou prispôsobenia. Z organizácií by sme chceli vyzdvihnúť združenia ISACA a CompTIA, ktoré ponúkajú celý rad prestížnych a celosvetovo žiadaných školení a certifikácií pre profesionálov IB. Zo štátnych orgánov je v popredí americký inštitút NIST, ktorý je v oblasti ISMS vzorom pre mnohé krajiny. V EÚ považujeme za lídrov kybernetickej ochrany z dlhodobého hľadiska Nemecko

a krátkodobého Českú republiku. ČR dokázala v priebehu posledných pár rokov vybudovať solídny systém pre ochranu kybernetického priestoru štátu a je stále schopná systém zdokonaľovať a rozširovať, čím sa stala príkladom vhodným nasledovania pre všetky členské krajiny EÚ. V roku 2016, EÚ v spolupráci s európskou agentúrou ENISA vydala Smernicu č. 2016/1148, ktorá významne ovplyvňuje bezpečnosť sietí a IS viacerých organizácií. Inak povedané, určité organizácie musia spĺňať nariadením stanovené požiadavky ISMS. Ide predovšetkým o podniky s kritickou infraštruktúrou (poskytovatelia základných služieb), online trhoviská, internetové vyhľadávače a podniky so službami v oblasti cloud computingu (poskytovatelia digitálnych služieb).[31] Túto smernicu členské krajiny EÚ postupne začleňujú do svojej legislatívy.

Slovenský NBÚ, ktorý je gestorom kybernetickej bezpečnosti štátu, v súčasnej dobe pripravuje Zákon o kybernetickej bezpečnosti. Prijatie zákona vychádza z aktuálnej Koncepcie a Akčného plánu kybernetickej bezpečnosti SR na roky 2015 – 2020. Pripravovaný zákon plne zakomponuje spomínanú smernicu EÚ a inšpiruje sa existujúcou českou legislatívou, ktorú sa pokúsi vylepšiť. Po jeho prijatí sa tak oblasť kybernetickej bezpečnosti, ale aj celkovej informačnej bezpečnosti v SR významne posilní a zároveň stúpne bezpečnostné povedomie aj vďaka aktivitám NBÚ cez pripravované Národné centrum pre kybernetickú bezpečnosť.[32]

Pre účely dizertačnej práce sa zameriame na normy rady ISO/IEC 27000, ktoré sú východiskovými dokumentmi pre štandardizáciu procesu zavedenia a udržiavania ISMS. „Súbor noriem ISMS je určený na pomoc organizáciám vyvíjať a implementovať rámec pre riadenie bezpečnosti ich informačných aktív vrátane finančných informácií, duševného vlastníctva, detailov o zamestnancoch alebo informácií im zverených od zákazníkov alebo tretích strán.“[33] Medzinárodné organizácie ISO a IEC vytvorili všeobecný a úplný prehľad o ISMS pre všetky druhy organizácií.

Úrad pre normalizáciu, metrológiu a skúšobníctvo SR doteraz preložil len štyri základné normy z celkového súboru okolo 45 medzinárodných noriem a prebral ďalších šesť noriem bez prekladu. Zoznam ponúkaných noriem rady ISO/IEC 27000 v SR je uvedený v nasledujúcej tabuľke.

---

[31] EUR-LEX. 2016. *Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.* [online]. 2016. [cit. 2017-02-27]. Dostupné na internete: <http://eur-lex.europa.eu/legal-content/SK/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SLK>.

[32] ROKOVANIE VLÁDY SR. 2015. *Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.* [online]. 2017. [cit. 2017-02-27]. Dostupné na internete: <http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-197723?prefixFile=m_>.

[33] STN ISO/IEC 27000: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Prehľad a slovník.*

Tab. 2: Normy rady ISO/IEC 27000 vydané v SR

STN ISO/IEC	Názov	Rok vydania	Vydanie v SR	Jazyk normy v SR
27000	Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Prehľad a slovník.	2012	2014	Slovenský
27001	Informačné technológie. Bezpečnostné metódy. Systémy riadenia informačnej bezpečnosti. Požiadavky	2013	2014	Slovenský
27002	Informačné technológie. Bezpečnostné metódy. Pravidlá dobrej praxe riadenia informačnej bezpečnosti	2013	2014	Slovenský
27005	Informačné technológie. Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti	2011	2012	Slovenský
27037	Informačné technológie. Bezpečnostné metódy. Návod na identifikáciu, zber, získavanie a zachovanie digitálnych dôkazov	2012	2017	Anglický
27038	Informačné technológie. Bezpečnostné metódy. Špecifiká digitálnej redakcie	2014	2017	Anglický
27040	Informačné technológie. Bezpečnostné metódy. Bezpečnosť ukladania dát	2015	2017	Anglický
27041	Informačné technológie. Bezpečnostné metódy. Návod na zaistenie vhodnosti a adekvátnosti metód vyšetrovania incidentov	2015	2017	Anglický
27042	Informačné technológie. Bezpečnostné metódy. Návod na analýzu a interpretáciu digitálnych dôkazov	2015	2017	Anglický
27043	Informačné technológie. Bezpečnostné metódy. Princípy a procesy vyšetrovania incidentov	2015	2017	Anglický

Zdroj: SUTN.SK. 2017. *Zoznam vybraných noriem*. [online]. Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2017 [cit. 2017-02-25]. Dostupné na internete: <https://www.sutn.sk/eshop/public/search.aspx>.

Keď porovnáme preklady noriem v SR napríklad so susednou Českou republikou, v dostupnosti preložených noriem výrazne zaostávame. Zodpovedný úrad v Českej republike preložil už 18 noriem ISMS a prebral ďalších 6.[34] Aj keď normy ISMS je možné zakúpiť v pôvodnom anglickom znení priamo cez ISO, význam vidíme práve v preložení normy do jazyka konkrétnej krajiny. Po zaobstaraní preloženej normy môžu podniky implementovať ISMS zrozumiteľným spôsobom a zároveň jednoduchšie zvyšovať vlastné bezpečnostné povedomie. Štúdium a implementácia normy v pôvodnom jazyku je náročnejšie z dôvodu vysokej odbornosti.

Organizácia ISO umožňuje certifikovať akúkoľvek organizáciu podľa normy ISO/IEC 27001 v prípade splnenia požiadaviek. Avšak, celý certifikačný proces môžu organizácie vnímať nielen ako organizačnú a časovú záťaž, ale hlavne finančnú. V konečnom dôsledku, aj keď certifikácia organizácie svedčí o vynikajúcej úrovni ISMS, v mnohých prípadoch je len zdrojom prestíže a marketingových výhod. Na druhej strane, výsledky prieskumu ISO o distribuovaní certifikátov podľa ISO/IEC 27001 v roku 2015

[34] ÚNMZ CZ. 2017. *Podrobné vyhledávání v normách*. [online]. Úřad pro technickou normalizáci, metrologii a státní zkušebnictví, 2017 [cit. 2017-02-25]. Dostupné na internete: <http://seznamcsn.unmz.cz/vyhledavani.aspx>.

ukazujú nárast až o 20 % oproti roku 2014. Celkovo bolo v roku 2015 certifikovaných 27536 organizácií. Krajiny, kde je najviac certifikovaných organizácií sú Japonsko (8240), Veľká Británia (2790) a India (2490). Z krajín V4 vlastní najviac certifikátov Poľsko (448), nasleduje Česká republika (381), Maďarsko (323) a nakoniec Slovensko (232). Slovensko si oproti roku 2014 polepšilo o 70 certifikovaných organizácií, zatiaľ čo v Českej republike prešlo certifikačným procesom viac organizácií, celkovo 105.[35] Zvýšený nárast v celkovom záujme môže znamenať, že organizácie prestávajú vnímať certifikáty len ako prestíž, ale začínajú prikladať IB určitú váhu, čo je pravdepodobne spôsobené medializáciou mnohých prípadov kybernetickej kriminality a propagačnými aktivitami organizácií činných v oblasti IB. Certifikačný proces však nie je nutné absolvovať, pretože primeranú úroveň ISMS za rozumné náklady možno implementovať aj bez certifikácie. Navyše, celkový nárast povedomia o IB vďaka aktivitám zainteresovaných organizácií už sám spôsobuje zvyšovanie zabezpečenia informácií.

1.1.4 Bezpečnostné incidenty v organizáciách

Inštitút NIST definuje incident ako porušenie alebo bezprostrednú hrozbu narušenia politiky počítačovej bezpečnosti, zásad prijateľného použitia alebo štandardných bezpečnostných praktík.[36] Podľa združenia ISACA, incidentom je pokus alebo úspešne neautorizovaný prístup, použitie, prezradenie, modifikácia, strata informácií alebo zasahovanie do systému a sieťových operácií.[37] Je potrebné rozlíšiť medzi incidentom a udalosťou informačnej bezpečnosti, pretože tieto dva pojmy sú často vnímané ako synonymá, ale v skutočnosti majú rozdielny význam. Incidenty teda považujeme za neželané alebo neočakávané udalosti IB, ktoré majú vysokú pravdepodobnosť ohrozenia dôvernosti, dostupnosti a integrity informácií. Hrozba je príčinou incidentu, ktorá môže viesť k poškodeniu systému alebo organizácie.[38] Udalosť je každý výskyt zmeny, chyby v systéme alebo sieti. Udalosťami sú pripojenie používateľa ku zdieľanému súboru, server, ktorý prijíma žiadosť o web stránku, firewall, ktorý blokuje pokus o pripojenie, atď.[39] Incidenty môžeme klasifikovať na neúmyselné (zodpovedná osoba zabudne aktivovať ACL, teda

[35] ISO. 2017. *The ISO Survey of Management System Standard Certifications (2006-2015).* [online]. 2017 [cit. 2017-02-25]. Dostupné na internete: < http://www.iso.org/iso/iso_27001_iso_survey2015.xls>.
[36] CICHONSKI, P. et al. 2012. *Computer Security Incident Handling Guide.* [online]. Gaithersburg: NIST, 2012, p. 6 [cit. 2015-12-03]. Dostupné na internete: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.
[37] ISACA. 2015. *CSX Cybersecurity Nexus: Cybersecurity Fundamentals – study guide.* Rolling Meadows: ISACA, 2015. s. 115. ISBN 978-1-60420-593-0.
[38] STN ISO/IEC 27000: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Prehľad a slovník.*
[39] CICHONSKI, P. et al. 2012. *Computer Security Incident Handling Guide.* [online]. Gaithersburg: NIST, 2012, p. 6 [cit. 2015-12-03]. Dostupné na internete: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.

zoznam pre riadenie prístupu na smerovači) a úmyselné (cielený útok hackera) alebo technické (malvér, útok DoS, zlyhanie systému) a fyzické (útoky sociálneho inžinierstva, stratené alebo odcudzené notebooky a mobilné zariadenia).[40] Kategórie bezpečnostných incidentov nájdeme v tabuľke 3.

Tab. 3: Kategórie bezpečnostných incidentov

Kategória	Názov	Popis
KAT 1	Neoprávnený prístup	Osoba získa logický a fyzický prístup do siete, systémov, aplikácií, ku dátam a iným zdrojom bez povolenia.
KAT 2	Odmietnutie služby (DoS)	Útok, ktorý úspešne narušuje a zabraňuje bežnú autorizovanú funkčnosť sietí, systémov alebo aplikácií.
KAT 3	Škodlivý kód	Úspešná inštalácia škodlivého softvéru (napr. vírus, červ, Trójsky kôň, a i.), ktorý infikuje operačný systém alebo aplikáciu.
KAT 4	Nesprávne použitie	Osoba poruší politiku prijateľného zaobchádzania s počítačmi.
KAT 5	Sondy, Skeny, Pokus o prístup	Aktivita, ktorá hľadá prístup alebo identifikuje počítač, otvára porty, protokoly, služby, atď.
KAT 6	Vyšetrovanie	Nepotvrdené incidenty, ktoré sú potenciálne škodlivé alebo anomálna aktivita.

Zdroj: ISACA. 2015. *CSX Cybersecurity Nexus: Cybersecurity Fundamentals – study guide.* Rolling Meadows: ISACA, 2015. s. 115. ISBN 978-1-60420-593-0.

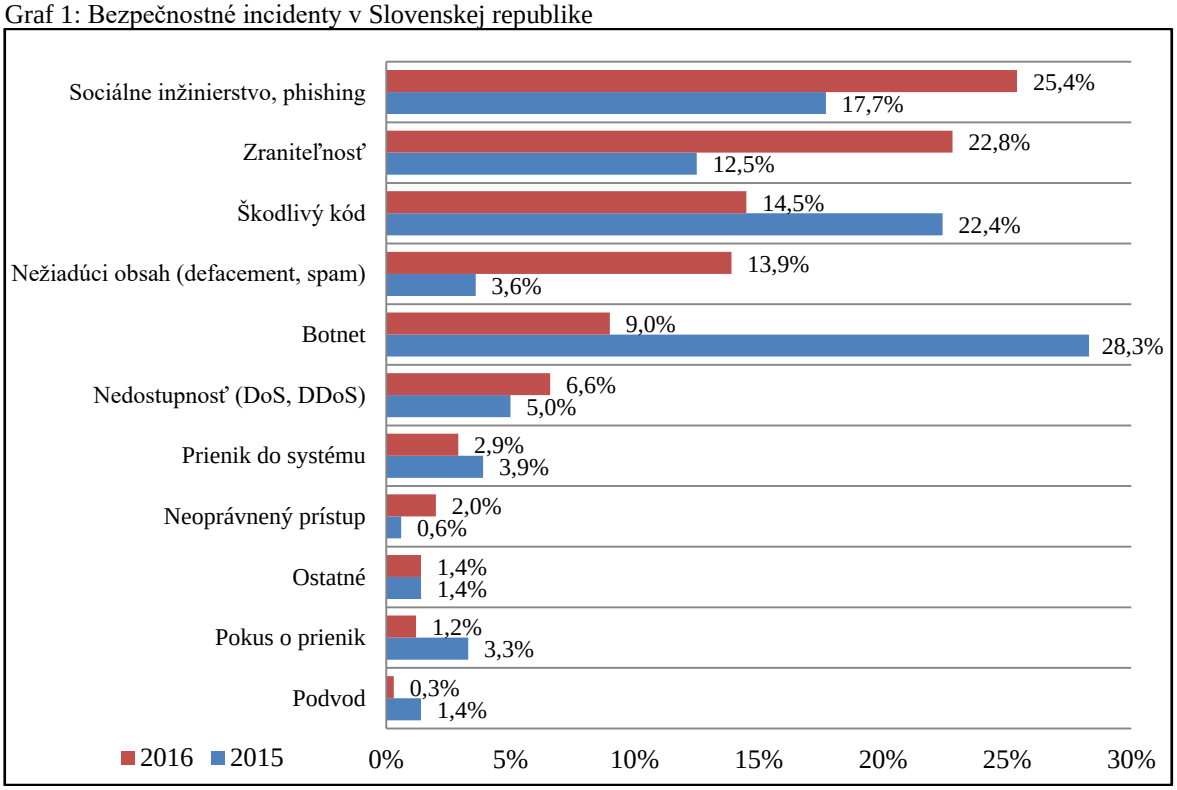
Podľa prieskumu spoločnosti Kaspersky Lab, 90 % oslovených podnikov priznalo bezpečnostný incident a 46 % stratilo dôverné dáta kvôli internej alebo externej hrozbe, čo vyústilo k vysokým nákladom na zotavenie z narušenia bezpečnosti.[41] Na Slovensku sa dokumentácii a hľadaniu riešení počítačových bezpečnostných incidentov venuje špecializovaný útvar CSIRT.SK zriadený vládou SR. CSIRT.SK odhaduje, že najmenej 6 % slovenských pracovných staníc je infikovaných škodlivým kódom a desiatky tisíc zariadení vypomáha pri DDoS útokoch bez vedomia ich vlastníkov. Väčšina nahlásených incidentov má príčinu práve v nedodržiavaní základných bezpečnostných zásad.[42] Výsledkami prieskumov chceme poukázať na reálnosť bezpečnostných incidentov v podmienkach slovenských podnikov. Realizácia bezpečnostného incidentu v podniku, ktorého jednou z príčin je nedostatočné bezpečnostné povedomie a disciplína personálu, skutočne môže viesť k dodatočným nákladom a v konečnom dôsledku aj k finančným stratám podniku.

Podiely z celkového počtu nahlásených incidentov sú zobrazené v grafe 1. Najväčšie zastúpenie z bezpečnostných incidentov v roku 2016 majú metódy sociálneho inžinierstva spolu s phishingom, 25,4 %. V tejto kategórii bol zaznamenaný medziročný nárast až 7,7 %. Spomínané metódy mieria priamo na používateľa IKT, sú najjednoduchším spôsobom

[40] ISACA. 2015. *CSX Cybersecurity Nexus: Cybersecurity Fundamentals – study guide.* Rolling Meadows: ISACA, 2015. s. 115. ISBN 978-1-60420-593-0.
[41] KASPERSKY. 2015. *Damage control: The cost of security breaches, IT security risks special report series.* [online]. 2015. [cit. 2014-10-17]. Dostupné na internete: <http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf>.
[42] CSIRT.SK. 2014. *Analýza aktuálneho stavu a vývoja incidentov v prvom polroku 2014.* [online]. 2014 [cit. 2015-12-03]. Dostupné na internete: <https://www.csirt.gov.sk/doc/Analyza_CSIRT.SK.pdf>.

kybernetickej kriminality na dosiahnutie cieľa útočníkom. Významný nárast vysvetľujeme dvomi spôsobmi. Buď si útočníci v prostredí SR uvedomili, že ľudský faktor je najzraniteľnejším miestom IB alebo v skúmaných obdobiach nastal nárast vzdelanostnej úrovne osôb oprávnených na nahlasovanie incidentov. To znamená, že dokázali takéto útoky identifikovať. Prípadne mohli nastať obe situácie naraz.

Graf 1: Bezpečnostné incidenty v Slovenskej republike



Zdroj: CSIRT.SK. 2017 (c). *Incidenty za obdobie od 1.1.2016 do 31.12.2016.* [online]. 2017 [cit. 2017-02-26]. Dostupné na internete: <https://www.csirt.gov.sk/graf-2016-8a0.html>.; CSIRT.SK. 2017 (d). *Incidenty za obdobie od 1.1.2015 do 31.12.2015.* [online]. 2017 [cit. 2017-02-26]. Dostupné na internete: <https://www.csirt.gov.sk/graf-2015-893.html>.

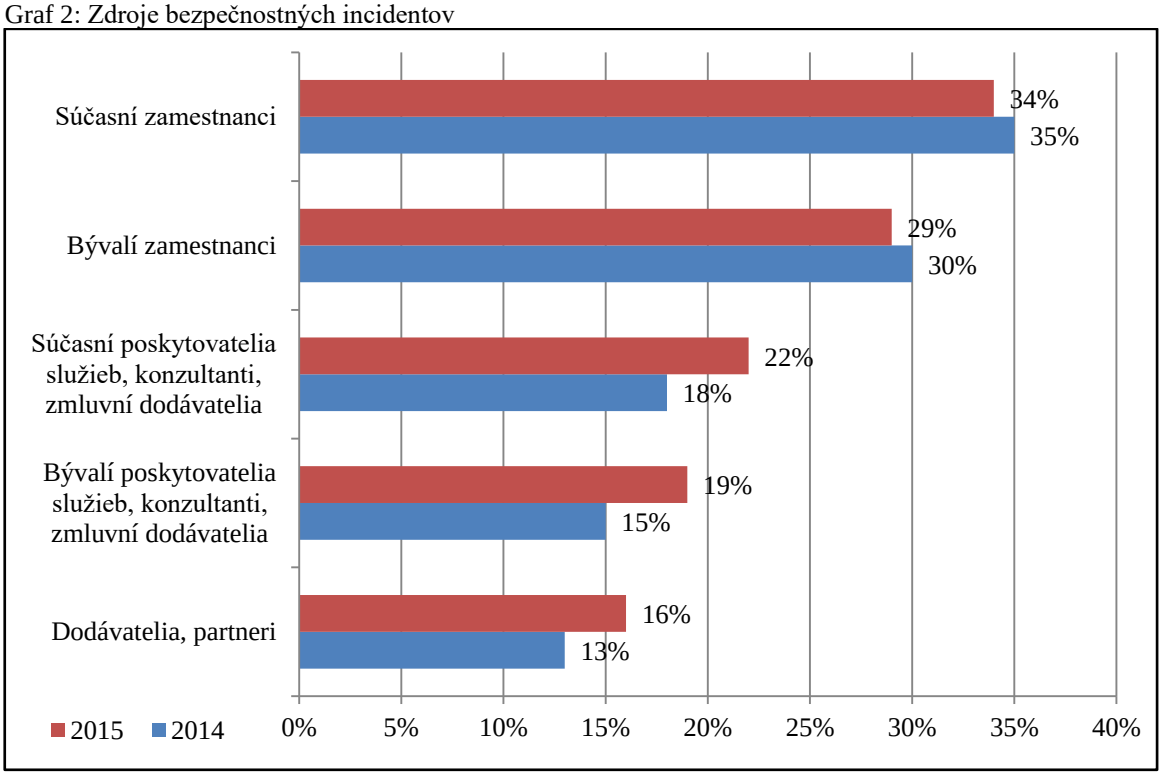
V roku 2015 boli najpočetnejším incidentom botnety, 28,3 %. V tomto prípade nastal výrazný pokles, medziročne až 19,3 %. Botnety sú počítače, ktoré vykonávajú bez vedomia používateľa naprogramovanú úlohu od útočníka na základe podvrhnutého kódu.[43] Takto významný pokles môžeme opäť pripísať nárastu incidentov sociálneho inžinierstva, ktoré sú oveľa jednoduchšie a účinnejšie. Zároveň, organizácie v priebehu roka pravdepodobne našli vhodný spôsob na identifikáciu nezvyčajného správania počítačov a elimináciu týchto rizík (napr. antivírusový softvér, IDS/IPS a i.). V roku 2016 je druhým najpočetnejším incidentom s 22,8 % zraniteľnosť, teda slabé miesto softvéru, hardvéru alebo iného informačného aktíva, s medziročným nárastom 10,3 %. Nasleduje škodlivý kód, 14,5 %, pri ktorom však

[43] KOKLES, M. – KORČEK, F. 2015. Analýza rizík informačnej bezpečnosti v malých a stredných podnikoch. In *Ekonomika a manažment: Vedecký časopis Fakulty podnikového manažmentu Ekonomickej univerzity v Bratislave.* ISSN 1336-3301, 2015, roč. 12, č. 1, s. 40.

sledujeme pokles o 7,9 %. Predpokladáme, že to bolo spôsobené investíciami do kvalitných antivírusových softvérov. Výskyt ostatných incidentov nie je taký výrazný, avšak podniky rôznej veľkosti sa nimi musia v rámci ISMS zaoberať, pretože ich realizácia spôsobuje významné škody a straty.

V nasledujúcich odstavcoch chceme poukázať na zraniteľnosť používateľov IKT ako jednu z najväčších hrozieb IB, čo potvrdzujú viacerí autori. Podľa Schiffovej, 6 najväčších zdrojov podnikových bezpečnostných incidentov sú nespokojní zamestnanci, neinformovaní a nedôslední zamestnanci, mobilné zariadenia (napr. BYOD), cloudové služby, poskytovatelia služieb tretích strán a neaktualizované zariadenia.[44] Bojanc a Jerman–Blažičová tvrdia, že incidenty sú naviazané na technické zlyhania, externé udalosti, zraniteľnosti ľudského faktoru a systému.[45] Nebezpečenstvo ľudského faktoru potvrdzuje aj spoločnosť PwC vo svojom globálnom prieskume zameranom na IB v organizáciách. Graf 2 zobrazuje aktuálne zdroje incidentov a ich porovnanie s rokom 2014 podľa manažérov zodpovedných za ISMS.

Graf 2: Zdroje bezpečnostných incidentov



Zdroj: PWC. 2015. *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016.* [online]. 2015 [cit. 2015-12-03]. Dostupné na internete: <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html>.

[44] SCHIFF, J. L. 2015. *6 Biggest Business Security Risks and How You Can Fight Back* [online]. 2015 [cit. 2015-11-13]. Dostupné na internete: <http://www.cio.com/article/2872517/data-breach/6-biggest-business-security-risks-and-how-you-can-fight-back.html?page=2>.

[45] BOJANC, R. – JERMAN-BLAŽIČ, B. 2008. An economic modelling approach to information security risk management. In *International Journal of Information Management*, ISSN 0268-4012, 2008, vol. 28, no. 5, p. 413.

Zatiaľ čo súčasní a bývalí zamestnanci sú uvádzaní manažérmi ako najčastejšie zdroje incidentov, súčasní zmluvní poskytovatelia služieb vzrástli na 22 % oproti 18 % z roku 2014 a bývalí poskytovatelia na 19 % oproti 15 %. Väčším zdrojom incidentov sa stávajú aj nezmluvní dodávatelia a ostatní partneri, ktorých uviedlo 16 % respondentov v roku 2015. Manažéri začínajú súčasným aj bývalým zamestnancom o trochu viac dôverovať, čo indikuje medziročný pokles. Avšak byť zamestnancom ako najväčším zdrojom bezpečnostných incidentov je opodstatnené, pretože pracuje s citlivými alebo inak dôvernými údajmi a je zároveň človekom, ktorého emócie, dôvera a nízke bezpečnostné povedomie sa dajú jednoducho a efektívne zneužiť.

Na problém ľudského faktoru poukazuje aj spoločnosť Ernst & Young, ktorá tvrdí, že zo všetkých incidentov je v 56 % zdrojom zamestnanec.[46] Podľa prieskumu stavu IB vykonanom spoločnosťou ESET v slovenských organizáciách, až 63 % organizácií označilo za primárnu príčinu bezpečnostného incidentu práve správanie zamestnancov. Väčšina rizík sa spája s ľudskou nepozornosťou, chybou, nevedomosťou a nezáujmom. Ďalším dôvodom je podľa 33 % organizácií škodlivý kód.[47] Čo sa týka škodlivého kódu, najfrekventovanejším spôsobom nakazenia malvérom a úniku citlivých informácii je podľa štúdie spoločnosti GFI Software z roku 2013 prezeranie internetového obsahu a infikované alebo falošné e–maily,[48] ktorých adresát je opäť len používateľ IKT. Závery mnohých odborníkov sa zhodujú na zamestnancoch ako slabine IB podniku. S týmito závermi sa plne stotožňujeme. Zvyšovanie bezpečnostného povedomia zamestnancov pomôže eliminovať alebo vyhnúť sa množstvu rizík informačnej bezpečnosti.

Spoločnosť PwC celkovo identifikovala 38 % nárast v odhaľovaní bezpečnostných incidentov organizáciami oproti roku 2014. Dokonca, 61 % respondentov má lepšie znalosti v oblasti externých hrozieb a 49 % v oblasti interných hrozieb. Síce stále mnoho organizácií nemá znalosti riadenia informačnej bezpečnosti alebo nedisponujú dostatočnými zdrojmi na boj proti hrozbám počítačovej kriminality, ale situácia sa zlepšuje. Organizácie sa začínajú zameriavať na ISMS, vytvárajú bezpečnostné rozpočty (46 % respondentov), bezpečnostné stratégie (45 %), bezpečnostné politiky (41 %), zavádzajú bezpečnostné technológie (37 %)

[46] EY. 2015. *Creating trust in the digital world: EY´s Global Information Security Survey 2015.* [online]. 2015 [cit. 2015-12-03]. Dostupné na internete: <http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf>.
[47] NETOLICKÁ, B. 2012 (a). *Sociálne inžinierstvo v kontexte informačnej bezpečnosti v organizácii.* [online]. 2012 [cit. 2015-12-03]. Dostupné na internete: <http://www.eset.com/sk/firmy/services/clanky/socialne-inzinierstvo-ib/>.
[48] EFOCUS. 2014. Až 90 % slovenských podnikov registruje zneužívanie pracovného webu zamestnancami. In *eFocus*. [online]. 2014 [cit. 2015-12-03]. Dostupné na internete: <http://www.efocus.sk/kategoria/bezpecnost/clanok/az-90-slovenskych-podnikov-registruje-zneuzivanie-pracovneho-webu-zamestnan/>. ISSN 1337-9801.

a posudzujú riziká (32 %).[49] Množstvo vysokopostavených manažérov si uvedomuje možné následky bezpečnostných incidentov na ich podniky, preto vyčleňujú zdroje na zabezpečenie dôverných informácií. Aktivity na zvyšovanie úrovne IB možno najlepšie pozorovať v medzinárodných spoločnostiach. To dokazuje aj veľké množstvo voľných pracovných ponúk zameraných na IB v medzinárodných spoločnostiach a veľkých podnikoch, ktoré sa priamo IB nezaoberajú (napríklad banky, automobilový priemysel, poisťovníctvo, atď.).

1.1.5 Posúdenie rizík informačnej bezpečnosti

Proces posúdenia rizík považujeme za najdôležitejšiu časť ISMS, pretože identifikuje, analyzuje a vyhodnocuje riziká informačnej bezpečnosti. Takto uskutočňuje komplexné riadenie rizík. „Cieľom riadenia rizík je identifikácia a kvantifikácia rizík, ktorým je potrebné vzdorovať a potom vhodným spôsobom rozhodnúť o ošetrení týchto rizík.“[50] Riziku môžeme prideliť množstvo definícií. Tie najvýstižnejšie sú:[51]

- Pravdepodobnosť vzniku straty,
- Odchýlenie skutočných od očakávaných výsledkov,
- Nebezpečenstvo chybného rozhodnutia,
- Variabilita možných výsledkov alebo neistota ich dosiahnutia,
- V oblasti ISMS považujeme riziko za „kombináciu následkov udalosti informačnej bezpečnosti a priradenej pravdepodobnosti jej výskytu.“[52]

„Posúdenie rizika určuje hodnotu informačných aktív, označuje použiteľné hrozby a slabé miesta, ktoré existujú, identifikuje existujúce kontroly a ich vplyv na zistené riziko, určuje prípadné následky a nakoniec uprednostňuje odvodené riziká a radí ich oproti kritériám vyhodnotenia rizík nastavených v určenom kontexte.“[53] Úlohou organizácie je definovať a zaviesť vlastný prístup k riadeniu rizík informačnej bezpečnosti, ktorého proces sa nachádza v tabuľke 4. V závislosti od výberu metódy je možné činnosti v jednotlivých fázach vykonávať v inom poradí.

[49] PWC. 2015. *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016.* [online]. 2015 [cit. 2015-12-03]. Dostupné na internete: <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html>.
[50] ONDRÁK, V. – SEDLÁK, P. – MAZÁLEK, V. 2013. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. s. 95. ISBN 978-80-7204-872-4.
[51] SMEJKAL, V. – RAIS, K. 2013. *Řízení rizik ve firmách a jiných organizacích.* 4. vyd. Praha: Grada Publishing, 2013. s. 90. ISBN 978-80-247-4644-9.
[52] STN ISO/IEC 27000: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Prehľad a slovník.*
[53] STN ISO/IEC 27005: 2012: *Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti.*

Tab. 4: Proces posúdenia rizík informačnej bezpečnosti

Fáza	Činnosť	Popis činnosti
A. Identifikácia rizík	1. Identifikácia aktív	• Aktívum je čokoľvek, čo má pre organizáciu hodnotu (informácie, procesy, systémy, dáta, atď.), • Popisuje aktíva, ktoré organizácia vlastní, • Určuje hodnoty aktív a ich význam pre organizáciu, • Určuje vlastníka aktíva pre každé aktívum, za ktoré poskytuje zodpovednosť, • Určuje hranice preskúmania ako perimeter aktív, • Vytvára zoznam aktív organizácie.
	2. Identifikácia hrozieb	• Určuje druhy udalostí a akcií, ktoré môžu negatívne ovplyvniť hodnotu aktív, • Hrozba môže poškodiť aj viac ako jedno aktívum, • Vytvára odhad pravdepodobnosti výskytu hrozieb, • Vytvára zoznam hrozieb s uvedením typu a pôvodu.
	3. Identifikácia existujúcich opatrení	• Určuje plánované a existujúce opatrenia pre zamedzenie duplicity, • Preskúmava dokumenty o detailoch realizovaných opatrení, • Preveruje správnu a efektívnu funkčnosť opatrení zodpovednými osobami a používateľmi.
	4. Identifikácia zraniteľností	• Určuje slabé miesta subjektov, ktoré umožňujú pôsobenie hrozieb na aktíva, • Zameriava sa na organizáciu, procesy, personál, fyzické prostredie, konfiguráciu IS, IKT, závislosť od tretích strán, • Určuje nesprávne realizované opatrenia, ktoré sa môžu stať potenciálnou zraniteľnosťou, • Vytvára zoznam druhov zraniteľnosti.
	5. Identifikácia následkov	• Určuje následky scenárov incidentu, ktoré ovplyvňujú obchodné procesy a aktíva stratou integrity a dostupnosti, • Vytvára zoznam scenárov incidentu s ich následkami.
B. Analýza rizík	1. Výber metódy analýzy rizík	• Kvalitatívna – je prispôsobiteľná, vhodná pre rozhodnutia, používa stupnicu kvalifikačných atribútov na rozsah následkov a pravdepodobnosti ich výskytu, • Kvantitatívna – používa stupnicu s číselnými hodnotami na rozsah následkov a pravdepodobnosti ich výskytu, kvalita analýz je spojená s presnosťou a úplnosťou číselných hodnôt, • Kombinovaná – kombinuje vyššie uvedené metódy v závislosti od okolností.
	2. Posúdenie následkov	• Posudzuje následky naplnenia incidentov na konkrétne aktíva a na činnosť organizácie, • Posudzuje obchodný vplyv na organizáciu, ktorý vyplýva z incidentov, • Vytvára zoznam posudzovaných následkov scenáru incidentu.
	3. Posúdenie pravdepodob. incidentu	• Určuje pravdepodobnosť každého scenára incidentu využitím kvalitatívnych alebo kvantitatívnych techník odhadu, • Berie v úvahu množstvo výskytu hrozieb a jednoduchosť zneužitia zraniteľnosti.
	4. Úroveň určovania rizík	• Určuje úroveň (mieru) rizík pre všetky scenáre incidentu, • Odhadnuté riziká sú kombinácia pravdepodobnosti scenára incidentu a ich následkov, • Vytvára zoznam rizík s priradenou mierou rizík.
C. Vyhodnotenie rizík	1. Rozhodovanie o budúcich činnostiach	• Porovnáva mieru rizík oproti kritériu vyhodnotenia rizík a kritériu prijatia rizík, • Rozhoduje o tom, či sa majú činnosti vykonávať, • Rozhodnutia sú založené na prijateľnej miere rizík, • Berie v úvahu priority rizík, • Berie v úvahu právne, zmluvné a regulačné požiadavky.
	2. Vytvorenie zoznamu rizík	• Vytvára zoznam rizík zoradených podľa kritérií. • Zoznam predkladá na ošetrenie rizík informačnej bezpečnosti

Zdroj: STN ISO/IEC 27005: 2012: *Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti;* SMEJKAL, V. – RAIS, K. 2013. *Řízení rizik ve firmách a jiných organizacích.* 4. vyd. Praha: Grada Publishing, 2013. s. 90-136. ISBN 978-80-247-4644-9; ČERMÁK, M. 2009. *Řízení informačních rizik v praxi.* Brno: Tribun EU, 2009. s. 21-111. ISBN 978-80-7399-731-1.

Existuje množstvo metód na vyhodnotenie rizika a výpočet miery rizika IB. Ako príklady uvádzame M_o_R, COBIT 5 for Risk, EBIOS, FAIR, MEHARI, OCTAVE Allegro, CSET, IRAM2, MAGERIT, CRAMM, RAMSES, metódy podľa ISO/IEC 27005, metóda podľa Zákona o kybernetickej bezpečnosti ČR, atď. Avšak, všetky metódy sú postavené na rovnakom základe, pretože výpočet miery rizika závisí od premenných ako sú hodnota informačného aktíva, zraniteľnosť aktíva, pravdepodobnosť hrozby, resp. incidentu, a veľkosť následku hrozby. Rôzne metódy používajú rôzne kombinácie týchto premenných podľa toho, ako chápu a definujú pojem riziko. Viaceré organizácie, ktoré sú aktívne v oblasti ISMS, ponúkajú podnikom možnosť čiastočnej úpravy metódy podľa vlastných potrieb. Toto odporúčanie nájdeme aj v norme ISO/IEC 27005, ktorá sama určuje niekoľko metód, avšak všetky s možnosťou prispôsobenia podmienkam konkrétneho podniku. Variabilita umožňuje podnikom nasadiť správnu metódu, ktorá pokrýva všetky potreby podniku s najvhodnejšími spôsobmi identifikácie, analýzy a vyhodnotenia rizík informačnej bezpečnosti.

1.1.6 Ošetrenie rizík informačnej bezpečnosti

Norma ISO/IEC 27005 predkladá štyri možnosti ošetrenia rizík. Čermák tieto možnosti vysvetľuje nasledovne:[54] [55]

- *Retencia* – prijatie rizika, ak je jeho úroveň zhodná zo stanovenými kritériami; nie je nutné aplikovať dodatočné opatrenia,
- *Redukcia* – úprava rizika implementovaním vhodných a oprávnených opatrení, ktoré odstraňujú príčinu rizika,
- *Vyhnutie sa riziku* – vyhnutie sa činnosti, ktorá zvyšuje konkrétne riziko,
- *Transfer* – prenos rizika, prípadne spoločné znášanie rizika s inou organizáciou; môže ísť o outsourcing, poistenie, dohody a i.

Pri prevádzkovaní ISMS musia podniky definovať a realizovať proces ošetrenia rizík informačnej bezpečnosti, ktorý:[56]

- Vyberá vhodný spôsob ošetrenia rizík, pričom zohľadňuje výsledok z procesu posúdenia rizík,
- Určuje všetky potrebné opatrenia,

[54] STN ISO/IEC 27005: 2012: *Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti.*
[55] ČERMÁK, M. 2009. *Řízení informačních rizik v praxi.* Brno: Tribun EU, 2009. s. 123-125. ISBN 978-80-7399-731-1.
[56] STN ISO/IEC 27001: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Požiadavky.*

- Overuje, či sa nejaké opatrenie neprehliadlo,
- Vytvára dokument vyhlásenia o aplikovateľnosti, ktorý opisuje ciele riadenia a opatrenia,
- Formuluje plán ošetrenia rizík,
- Získava súhlas zodpovedných osôb s plánom ošetrenia rizík a o akceptovaní zostatkových rizík,
- Implementuje plán ošetrenia rizík a samotné opatrenia.

Podľa Strnáda, žiadaným výsledkom procesu ošetrenia rizík informačnej bezpečnosti je, aby podniky v praxi dosahovali požadovanú úroveň zostatkových rizík.[57] Zostatkové riziká ostávajú po vykonaní procesu posúdenia a ošetrenia. Úlohou manažérov podniku je, aby rozhodli, či dané riziko príjmu na požadovanej úrovni.

1.1.7 Výber bezpečnostných opatrení

Princíp výberu ochranných opatrení má základ v potrebe minimalizácie rizík informačnej bezpečnosti. Medzi najdôležitejšie opatrenia radíme tie, ktoré spĺňajú podmienku všeobecnej aplikovateľnosti. Mnohé štandardy členia opatrenia do kategórií, ktoré sú logickými zoznamami príbuzných bezpečnostných opatrení. Podľa Ondráka a kol. sú základnými kategóriami riadenie bezpečnostnej politiky, kontrola bezpečnostnej zhody s právnymi a zmluvnými požiadavkami, riešenie incidentov, personálne opatrenia, bezpečnosť prevádzky, plánovanie kontinuity činností organizácie, fyzická bezpečnosť a bezpečnosť prostredia.[58] Norma ISO/IEC 27002 kategórie rozširuje o organizáciu IB, riadenie aktív, riadenie prístupov, kryptografické opatrenia, bezpečnosť prevádzky, komunikačnú bezpečnosť, opatrenia akvizície, vývoja a údržby informačných systémov a riadenie vzťahov s dodávateľmi.[59] Väčšina podnikov sa orientuje na výber opatrení, ktoré pokrývajú externé hrozby a interné zostávajú nepovšimnuté.[60] Podľa nášho názoru je nevyhnutné, aby podnik pokryl všetky kategórie opatrení a vyberal tie opatrenia, ktoré sú primerané, aplikovateľné a mieria na riziká identifikované v rizikovej analýze bez ohľadu na to, či hrozby pochádzajú z externého alebo interného prostredia.

---

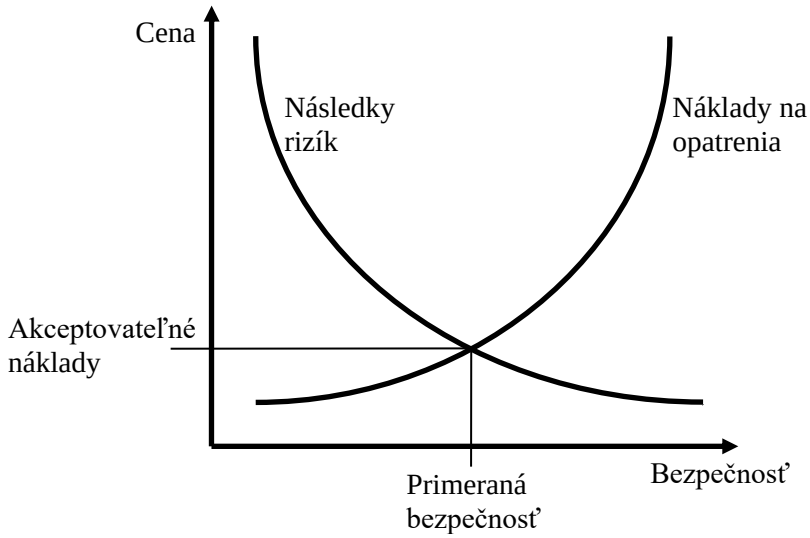
[57] STRNÁD, O. 2011. *Systém riadenia informačnej bezpečnosti.* Ostrava: Amos, 2011. s. 180. ISBN 978-80-904766-6-0.
[58] ONDRÁK, V. – SEDLÁK, P. – MAZÁLEK, V. 2013. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. s. 101. ISBN 978-80-7204-872-4.
[59] STN ISO/IEC 27002: 2014: *Informačné technológie – Bezpečnostné metódy – Pravidlá dobrej praxe riadenia informačnej bezpečnosti.*
[60] ČERNÝ, M. – ROMANOVÁ, A. 2012. Interní zamestnanci ako hrozba bezpečnosti dát. In *Ekonomika a manažment podniku: vedecký časopis pre ekonomiku, riadenie a manažment slovenských podnikov.* ISSN 1336-4130, 2012, roč.10, č. 1-2, s. 7.

Nasledujúce opatrenia sú nevyhnutné na udržiavanie bezpečnosti IT infraštruktúry akejkoľvek organizácie z hľadiska externých, ale aj interných hrozieb. Neschopnosť riešenia týchto procesov je jednou z hlavných príčin zraniteľností:[61]

- Správa identít,
- Prideľovanie a odoberanie práv používateľovi,
- Autorizácia,
- Prístupové zoznamy (ACL),
- Monitorovanie privilegovaných používateľov,
- Riadenie bezpečnostnej konfigurácie sieťových zariadení, aplikácií a systémov,
- Aktualizácia softvéru.

V podnikateľskej praxi sa kombinuje viacero opatrení na ošetrenie analyzovaných rizík. Najčastejšie ide o opatrenia vedúce ku odstraseniu od útoku, zdržaniu útoku, detekcii útoku, reakcii na útok a obnove po útoku. U každého opatrenia by sme mali posudzovať jeho efektivitu, náklady a prínos.[62] Cieľom riadenia ISMS je znížiť následky rizík na minimum a dosiahnuť čo najnižšie náklady na ošetrenie rizík IB, to znamená vyberať opatrenia za akceptovateľné náklady (pozri graf 3).

Graf 3: Primeraná bezpečnosť za akceptovateľné náklady



Zdroj: GOGELA, R. 2011. *Standardy a definice pojmů ISMS.* [online]. 2011 [cit. 2015-12-04]. Dostupné na internete: <http://www.cybersecurity.cz/data/Gogela.pdf>.

Hodnotením jednotlivých aktív je získaná ich ekonomická hodnota pre vrcholový manažment podniku. V podstate ide o vyčíslenie veľkosti strát, keď hrozba naruší úžitkovú

[61] ISACA. 2015. *CSX Cybersecurity Nexus: Cybersecurity Fundamentals – study guide.* Rolling Meadows: ISACA, 2015. s. 37-39. ISBN 978-1-60420-593-0.
[62] ČERMÁK, M. 2009. *Řízení informačních rizik v praxi.* Brno: Tribun EU, 2009. s. 111-112. ISBN 978-80-7399-731-1.

hodnotu aktíva. Každý podnik potrebuje priradiť hodnotu svojim informáciám a prispôsobiť ich ochranu. Hodnotenie informačných aktív býva v praxi východiskom pre stanovenie maximálnych nákladov na realizáciu opatrení na ich ochranu.[63] Funkcie následkov rizík a nákladov na opatrenia sú nepriamo úmerné, pretože ak klesajú náklady na opatrenia, klesá aj úroveň bezpečnosti. Naopak, ak následky rizík klesajú, úroveň bezpečnosti stúpa. Stret funkcií sa nazýva bod primeranej bezpečnosti.

Primeraná bezpečnosť je taká úroveň bezpečnosti, pri ktorej sú dosiahnuté čo najmenšie následky rizík pri akceptovateľných nákladoch na ich opatrenia. Dosiahnuť primeranú bezpečnosť je misiou každého podniku, ktorý zavádza alebo zdokonaľuje proces riadenia informačnej bezpečnosti.

1.1.8 Zhrnutie východísk manažmentu informačnej bezpečnosti

Manažment informačnej bezpečnosti sme definovali ako ucelený systém v rámci organizácie, ktorý chráni informácie pred hrozbami tak, že zavádza a zdokonaľuje proces riadenia rizík informačnej bezpečnosti. Udržiavaním tohto systému sa organizácia stáva dôveryhodnou z pohľadu všetkých zainteresovaných strán, napríklad zamestnancov, dodávateľov alebo zákazníkov. Vytvorenie, zavedenie, monitorovanie a zlepšovanie ISMS pozostáva z mnohých činností, ktoré je nutné vykonávať v pravidelných časových intervaloch. Niektoré častejšie (vyhodnocovanie bezpečnostných incidentov, posudzovanie a ošetrenie rizík, atď.), iné postačí vykonať alebo aktualizovať raz ročne (napr. bezpečnostné politiky, kontrola súladu s vybranou normou, interné alebo externé audity). Posúdenie rizík pokladáme za najvýznamnejšiu časť ISMS z dôvodu vytvorenia kompletnej rizikovej analýzy organizácie. Na základe analýzy možno navrhnúť vhodné spôsoby ošetrenia rizík a vybrať adekvátne bezpečnostné opatrenia za akceptovateľné náklady, čím docielime primeranú bezpečnosť informačných aktív organizácie.

Procesy, odporúčania a ciele ISMS sú všeobecne aplikovateľné na ktorýkoľvek podnik či organizáciu. V mnohých prípadoch je potrebné ISMS vhodne prispôsobiť podmienkam organizácie. Aj z pohľadu podnikov s elektronickým obchodom je nutné bezpečnostné požiadavky ISMS prehodnotiť, upraviť, prípadne niektoré požiadavky úplne vyradiť z dôvodu nejestvovania konkrétneho procesu v podniku.

Manažmentom informačnej bezpečnosti sa profesionálne zaoberá viacero organizácií, spoločností a inštitúcií, ktoré navrhujú, skúmajú a posudzujú stratégie, rámce,

[63] DOUCEK, P. a kol. 2011. *Řízení bezpečnosti informací.* 2. vyd. Praha: Professional Publishing, 2011. 286 s. ISBN 978-80-7431-050-8.

normy, odporúčania a opatrenia ISMS. Takýmto spôsobom apelujú na zvyšovanie bezpečnostného povedomia a zvyšujú celkovú úroveň IB. Na Slovensku sa oblasť rozvíja, v posledných troch rokoch možno pozorovať zvýšený počet pracovných ponúk zameraných na IB. Aktívne sú najmä súkromné (ISACA, PwC, Ernst & Young, ESET, SECTEC, Slovenská asociácia pre informačnú bezpečnosť, atď.), ale aj štátne organizácie (napríklad CSIRT.SK). V blízkej budúcnosti predpokladáme významný nárast aktivít aj zo strany Národného bezpečnostného úradu, čo vyplýva z Koncepcie kybernetickej bezpečnosti SR na roky 2015 – 2020 a pripravovaného Zákona o kybernetickej bezpečnosti.

1.2 Modely manažmentu informačnej bezpečnosti

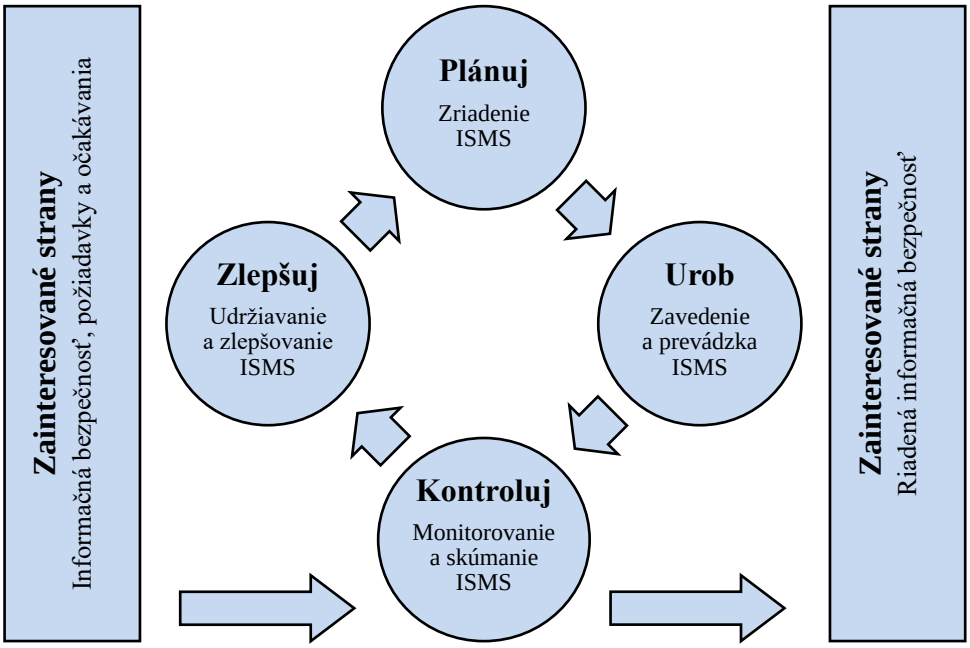
Podniky riadia množstvo činností, aby ich prevádzka bola efektívna. Existujúce modely im umožňujú identifikovať tie činnosti systému, ktoré sú významné a na ktoré potrebujú koncentrovať dostupné zdroje na dosiahnutie neustáleho chodu systému. Implementovaním vybraných modelov manažmentu informačnej bezpečnosti dokážu organizácie kontinuálne riadiť bezpečnosť svojich informačných aktív a navyše sú schopné procesné činnosti neustále zlepšovať. Porovnaním vybraných modelov ISMS získame ucelený prehľad o možnostiach ich uplatnenia v oblasti elektronického podnikania.

1.2.1 Model PDCA

Model PDCA, tiež známy ako Demingov cyklus, je modelom kontinuálneho zlepšovania kvality, napríklad výrobkov, služieb, procedúr, procesov, aplikácií, dát a i. Jeho cieľom je vytváranie, budovanie, monitorovanie a neustále zlepšovanie ISMS v rámci organizácie.[64] Prebieha formou opakovaného praktizovania štyroch základných činností, Plan (Plánuj) – Do (Urob) – Check (Kontroluj) – Act (Zlepšuj):[65]

- *Plánuj* – plánovanie zamýšľaného zlepšenia a stanovenie cieľov,
- *Urob* – realizácia plánu,
- *Kontroluj* – kontrola výsledkov realizácie oproti pôvodnému plánu,
- *Zlepšuj* – úprava zámeru i vlastnej realizácie na základe kontroly spolu so zdokonaľovaním činností.

[64] KOKLES, M. – BOLEK, V. 2013. Hrozby počítačovej kriminality. In *Manažment v teórii a v praxi.* [online]. 2013, roč. 9, č. 3, s. 14 [cit. 2015-12-04.] Dostupné na internete: <http://mtp.euke.sk/wp-content/uploads/2014/03/MTP-3-2013.pdf>. ISSN 1336-7137.
[65] ONDRÁK, V. – SEDLÁK, P. – MAZÁLEK, V. 2013. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. s. 24-25. ISBN 978-80-7204-872-4.



Obr. 3: Model PDCA aplikovaný na ISMS
Zdroj: STEHLÍKOVÁ, B. – HOROVČÁK, P. 2012. Manažment informačnej bezpečnosti v malých a stredných podnikoch. In *Security Revue* [online]. 2012 [cit. 2015-12-04]. Dostupné na internete: <http://www.securityrevue.com/article/2012/06/manazment-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch/>.

Na obrázku 3 sa nachádza model PDCA aplikovaný na činnosti ISMS. Je známy pod názvom životný cyklus ISMS a má tieto fázy:[66]

1. *Zriadenie ISMS* – Zriadenie politiky, cieľov, procesov, organizačnej štruktúry, postupov súvisiacich so zdokonaľovaním manažmentu rizík IB tak, aby poskytovali výsledky v súlade s celkovou politikou a cieľmi organizácie,
2. *Zavedenie a prevádzka ISMS* – Zavedenie a implementácia politiky ISMS, opatrení, procesov a postupov,
3. *Monitorovanie a skúmanie ISMS* – Meranie výkonu procesov voči politike a cieľom ISMS a nahlasovanie výsledkov vedeniu organizácie k preskúmaniu,
4. *Udržiavanie a zlepšovanie ISMS* – Prijatie opatrení k náprave a preventívne opatrenia založené na výsledkoch interného auditu ISMS; preskúmanie ISMS zo strany vedenia organizácie, aby bolo dosiahnuté neustále zlepšovanie systému.

Neustálym praktizovaním jednotlivých fáz, ich činností a opatrení vyplývajúcich z ISMS, podniky zvyšujú zabezpečenie svojich informačných aktív. Zároveň sa tento jednoduchý systém stáva bežnou súčasťou podnikovej prevádzky. Na tomto modeli sú založené normy ISO/IEC rady 27000.

[66] ČSN ISO/IEC 27001: 2006: *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky.*

1.2.2 Model Activate – Adapt – Anticipate

Spoločnosť Ernst & Young vyvinula model Activate – Adapt – Anticipate (vo voľnom preklade Aktivovať – Prispôsobiť – Predvídať) určený na budovanie systému kybernetickej bezpečnosti a riadenie informačnej bezpečnosti v organizáciách. Model identifikuje tri úrovne zrelosti zabezpečenia kybernetického priestoru, ktoré musia byť vykonané v tesnej následnosti s cieľom dosahovať stále pokročilejšie a komplexnejšie bezpečnostné opatrenia na každej úrovni.[67] Charakteristika modelu sa nachádza v tabuľke 5.

Tab. 5: Model Activate – Adapt – Anticipate

Popis úrovne	Úrovne budovania systému kybernetickej bezpečnosti	Aktuálny stav
Aktivácia je počiatočná úroveň. Ide o komplexnú množinu bezpečnostných opatrení zameraných na ochranu súčasného stavu podniku.	Activate (Aktivovať)	Aktivácia je súčasťou bezpečnostného systému každej organizácie. Všetky potrebné opatrenia ešte nie sú implementované. Stále je možné úroveň zlepšovať.
Prispôsobenie je zmena. Systém kybernetickej bezpečnosti sa mení počas zmeny prostredia. Zameriava sa na ochranu zajtrajšieho podniku.	Adapt (Prispôsobiť)	Prispôsobenie ešte nie je široko implementované. Zároveň ani nie je bežnou praktikou posudzovať bezpečnostné hrozby vždy, keď organizácia vykonáva zmeny v podnikaní.
Predvídanie sa upriamuje do neznáma. Pretože je založené na koncepte spravodajstva kybernetických hrozieb, potenciálne útoky sú identifikované a opatrenia implementované pred tým, ako nastane poškodenie.	Anticipate (Predvídať)	Predvídanie postupne vzniká. Stále viac a viac organizácií využíva spravodajstvo kybernetických hrozieb, aby predbehli kybernetické zločiny. Predvídanie je inovačným doplnkom ku Prispôsobeniu.

Zdroj: EY. 2014 (b). *Get Ahaed of Cybercrime: EY´s Global Information Security Survey – 2014.* [online]. 2014 [cit. 2015-12-04]. Dostupné na internete: <http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf>.

Pretože riziká informačnej bezpečnosti sa neustále menia, narastajú, sú sofistikovanejšie a ich prekazenie je ťažšie, cieľom modelu je, aby boli organizácie v predstihu pred útočníkmi a hrozbami. Bezpečnosť podniku je nevyhnutné zamerať na niečo neznáme, teda na budúcnosť a širší ekosystém podniku. Podniky môžu identifikovať zraniteľné miesta a budovať opatrenia ešte pred tým, ako budú využité a pripraviť sa na hrozby ešte skôr ako nastanú.[68] Tomu predchádza úspešne absolvovanie prvých dvoch úrovní modelu. V úrovni aktivácie, kde sa nachádza väčšina podnikov, implementujú celú

[67] EY. 2015. *Creating trust in the digital world: EY´s Global Information Security Survey 2015.* [online]. 2015 [cit. 2015-12-03]. Dostupné na internete: <http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf>.

[68] EY. 2014 (b). *Get Ahaed of Cybercrime: EY´s Global Information Security Survey – 2014.* [online]. 2014 [cit. 2015-12-04]. Dostupné na internete: <http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf>

množinu opatrení proti hrozbám informačnej bezpečnosti. V pokročilejšej úrovni prispôsobenia podniky prehodnocujú opatrenia pri každej podnikateľskej zmene.

1.2.3 Model Confidentiality – Integrity – Availability

Model, ktorý na dosiahnutie zodpovedajúcej úrovne ISMS využíva tri základné vlastnosti IB, je špecifikovaný v tabuľke 6. Aplikovaním odporúčaných metód riadenia konkrétnej vlastnosti IB v podniku je zachovaná nepopierateľnosť informácií. Dôvernosť, bezúhonnosť (resp. integrita) a dostupnosť sú rovnako dôležité faktory v procese zaistenia nepopierateľnosti, ktorá v digitálnom kontexte zabezpečí nefalšovanosť a originálnosť informácie. Nepopierateľnosť je obzvlášť potrebná vo finančných transakciách a právnych záležitostiach. Možno ju zachovať využívaním digitálnych podpisov a spravovaním logov.[69]

Tab. 6: Model Confidentiality – Integrity – Availability

Požiadavka	Vplyv a potenciálne následky	Metódy riadenia
Confidentiality (dôvernosť): Ochrana informácií pred neoprávneným zverejnením	*Strata dôvernosti má za následok:* • Prezradenie informácie chránenej zákonmi o ochrane súkromia • Stratu verejnej dôvery • Stratu konkurenčnej výhody • Žalobu proti podniku • Zasahovanie do národnej bezpečnosti	*Dôvernosť môže byť zachovávaná nasledujúcimi metódami:* • Riadenie prístupu • Povolenia k súborom • Šifrovanie
Integrity (bezúhonnosť): Presnosť a úplnosť informácií v súlade s podnikovými hodnotami a očakávaniami	*Strata bezúhonnosti má za následok:* • Nepresnosť • Chybné rozhodnutia • Podvod	*Bezúhonnosť môže byť zachovávaná nasledujúcimi metódami:* • Riadenie prístupu • Logging • Digitálne podpisy • Hašovacie funkcie • Šifrovanie
Availability (dostupnosť): Schopnosť pristupovať k informáciám a zdrojom požadovanými podnikovými procesmi	*Strata dostupnosti má za následok:* • Stratu funkčnosti a operatívnej efektívnosti • Stratu produktívneho času • Zasahovanie do podnikových cieľov	*Dostupnosť môže byť zachovávaná nasledujúcimi metódami:* • Redundancia • Zálohy • Riadením prístupu

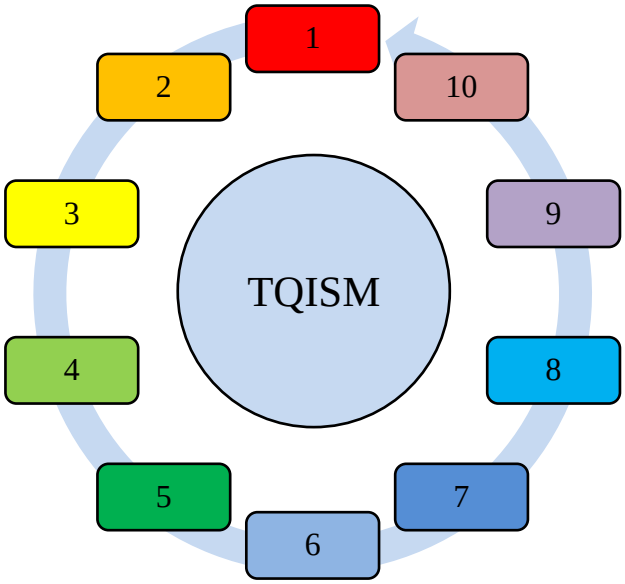
Zdroj: ISACA. 2015. *CSX Cybersecurity Nexus: Cybersecurity Fundamentals – study guide.* Rolling Meadows: ISACA, 2015. s. 12. ISBN 978-1-60420-593-0.

Podniky sú vo svojich procesoch odkázané na pravosť informácií, ktoré získavajú z mnohých zdrojov a ktoré následne spracúvajú a opäť odosielajú ďalej. Strata základných vlastností informačnej bezpečnosti vedie k mnohým ekonomickým, podnikateľským a právnym následkom uvedeným v modeli.

[69] ISACA. 2015. *CSX Cybersecurity Nexus: Cybersecurity Fundamentals – study guide.* Rolling Meadows: ISACA, 2015. s. 12. ISBN 978-1-60420-593-0.

1.2.4 Model TQISM

Model Total Quality Information Security Management (pozri obrázok 4) sa sústreďuje na maximalizáciu kvality manažmentu informačnej bezpečnosti. Je to procesný model v podobe cyklu, ktorý zdôrazňuje neustále zdokonaľovanie ISMS v organizácii.



Obr. 4: Model TQISM
Zdroj: SHARBAF, M. S. 2014. A New Perspective to Information Security: Total Quality Information Security Management. In *Proceedings of the 7th International Conference on Security of Information and Networks (SIN '14)*, New York: ACM, 2014. ISBN 978-1-4503-3033-6, p. 57.

Autor modelu vyzdvihuje jeho komplexnosť a schopnosť nepretržitého zlepšovania kvality procesov a procedúr IB. Jadrom modelu je manažérsky prístup ku dlhodobému úspechu implementácie kvalitnej IB v organizácii. V modeli TQISM všetci členovia organizácie (CEO, CIO, CISO, zamestnanci IT oddelenia, koncoví používatelia a i.) participujú na zlepšovaní procesov, procedúr a kultúry spojenej s kvalitou IB. Na dosiahnutie tejto úrovne musí organizácia integrovať 10 dimenzií v stanovenom poradí:[70]

1. Vytvoriť a prijať novú kultúru kvality IB v organizácii,
2. Neustále rozvíjať zmysel pre zlepšovanie kvality IB,
3. Zriadiť školenia, program vzdelávania a zvyšovania informovanosti v súvislosti s kvalitou IB na pracovných miestach,
4. Zaistiť, aby kvalita IB bola zodpovednosťou každého a búrať bariéry medzi IT oddelením a ostatnými oddeleniami,
5. Rozvíjať politiku IB a presadzovať ju v organizácii,

[70] SHARBAF, M. S. 2014. A New Perspective to Information Security: Total Quality Information Security Management. In *Proceedings of the 7th International Conference on Security of Information and Networks (SIN '14)*, New York: ACM, 2014. ISBN 978-1-4503-3033-6, p. 58 – 60.

6. Vytvoriť a implementovať kvalitne vrstvené bezpečnostné stratégie v organizácii,
7. Rozvíjať a sledovať mechanizmus na vyhodnotenie kvality IB,
8. Zaviesť účinný program kvalitnej IB prostredníctvom životného cyklu, ktorý podporuje proces riadenia rizík, proces merania, zlepšovania a riadenia,
9. Mať holistický prístup k zabezpečeniu technológií, procesov a ľudí,
10. Navrhnúť a realizovať kvalitnú IB, ktorá podporuje potreby a ciele organizácie.

Model TQISM je na rozdiel od predchádzajúcich troch modelov viac špecifikovaný a zdôrazňuje dôslednosť a efektivitu riadenia IB v organizácii. Autor sa dotýka viacerých konkrétnych oblastí, ktoré včlenením do modelu považuje za kľúčové pri riadení kvality IB (napr. program vzdelávania, politika IB, bezpečnostné stratégie, podpora potrieb a cieľov organizácie, atď.). TQISM považujeme za vhodný model pre implementáciu v podnikoch, ktoré využívajú komplexnú a systémovú metódu riadenia kvality, napríklad TQM alebo Model excelentnosti EFQM.

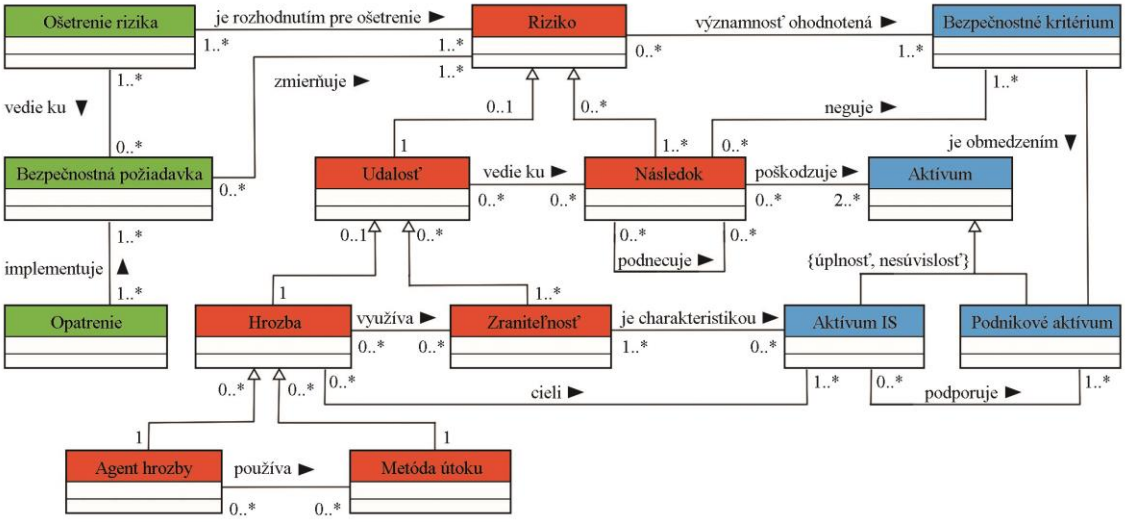
1.2.5 Doménový model ISSRM

Doménový model Information System Security Risk Management predstavuje rizikový manažment bezpečnosti informačného systému v organizácii s dôrazom na ochranu dôvernosti, dostupnosti a integrity informácií. Je koncepčným, entitno–relačný modelom, ktorý vychádza z analýzy štandardov, metód rizikového manažmentu a bezpečnostných štandardov. Bol skonštruovaný ako diagram tried v jazyku UML.[71] Model ISSRM, ktorý sa nachádza na obrázku 5, pozostáva z troch základných konceptov prepojených vzájomnými vzťahmi:[72] [73]

1. *Koncept aktív* – poskytuje životne dôležité služby pre organizáciu a ich bezpečnostné potreby. Existujú dva druhy aktív:
   a. *Podnikové aktíva* – zahŕňajú informácie, procesy a hodnotu podniku,
   b. *Aktíva informačného systému* – podporujú podnikové aktíva,
2. *Koncept rizík* – identifikuje jednotlivé zložky rizika (hrozba, zraniteľnosť, agent hrozby, metóda útoku, udalosť, následok),

[71] MAYER, N. et al. 2008. Towards a Measurement Framework for Security Risk Management. In *Proceedings of the Workshop on Modeling Security (MODSEC08) held as part of the 2008 International Conference on Model Driven Engineering Languages and Systems (MODELS)*. Toulouse: CEUR–WS, 2008. ISSN 1613-0073.
[72] ABBASS, W. – BAINA, A. – BELLAFKIH, M. 2016. Improvement of Information System Security Risk Management. In *4th IEEE International Colloquium on Information Science and Technology (CiSt)*. Tangier–Assilah: IEEE, 2016. ISBN 978-1-5090-0751-6, p. 183.
[73] ALCADE, B. et al. 2009. Towards a Decision Model Based on Trust and Security Risk Management. In *AISC '09 Proceedings of the Seventh Australasian Conference on Information Security. Vol. 98.* Wellington: Australian Computer Society, 2009. ISBN 978-1-920682-79-8, p. 62 – 63.

3. *Koncept ošetrenia rizík* – definuje bezpečnostné požiadavky a rozhodovanie o výbere opatrení a ošetrení rizík.



Obr. 5: Doménový model ISSRM
Zdroj: ABBASS, W. – BAINA, A. – BELLAFKIH, M. 2016. Improvement of Information System Security Risk Management. In *4th IEEE International Colloquium on Information Science and Technology (CiSt)*. Tangier–Assilah: IEEE, 2016. ISBN 978-1-5090-0751-6, p. 183.

Aplikácia ISSRM v organizácii postupuje podľa štandardného procesu rizikového manažmentu. Tento iteratívny proces sa skladá zo šiestich krokov. Ako prvé vývojár definuje kontext a aktíva, ktoré je potrebné zabezpečiť. Potom stanoví ciele týkajúce sa IB (dôvernosť, dostupnosť, integrita) na základe požadovanej úrovne ochrany identifikovaných aktív. Následne analýza a hodnotenie rizík pomôžu identifikovať potenciálne riziká a ich následky. Ďalším krokom je rozhodovanie o ošetrení rizík, ktorého výsledkom je vymedzenie bezpečnostných požiadaviek. Tie sú implementované do bezpečnostných opatrení. Proces riadenia rizík je iteratívny, pretože nové bezpečnostné opatrenia môžu otvoriť ďalšie, doteraz nezistené bezpečnostné riziká.[74] Doménový model zovšeobecňuje rizikový manažment z pohľadu IB v organizácii. Identifikuje podstatné domény v rámci troch konceptov a prehľadne určuje vzťahy medzi doménami. Možnosť priamej aplikácie v organizácii a pripravenosť k vytvoreniu informačného systému sú výhodou modelu.

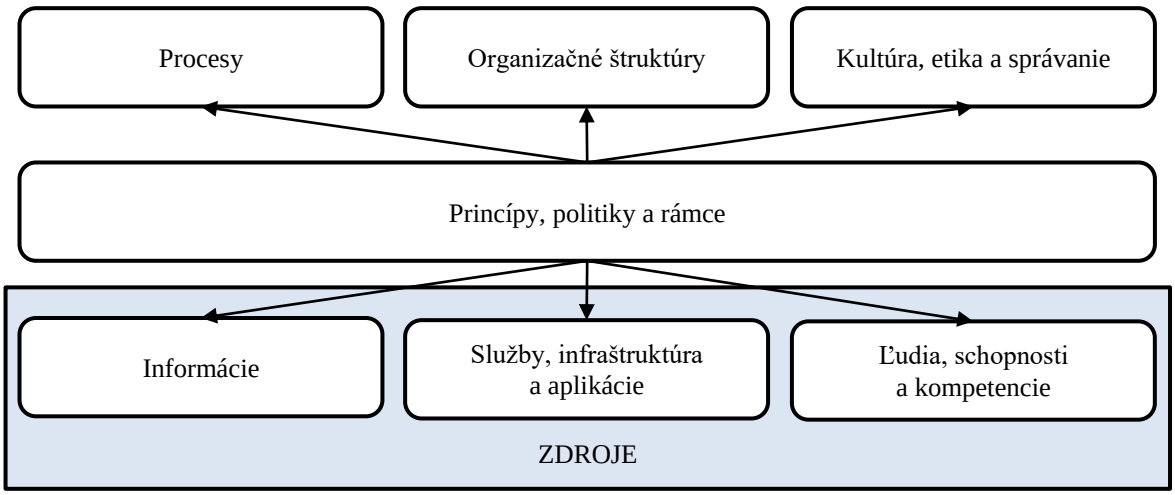
1.2.6 Všeobecný model faktorov vplyvu

Organizácia ISACA vo svojej odbornej publikácii COBIT 5 pre informačnú bezpečnosť, v originálnom znení COBIT 5 for Information Security, definuje Všeobecný

[74] ALTUHHOVA, O. – MATULEVIČIUS, R. – AHMED, N. 2012. Towards Definition of Secure Business Processes. In *Advanced Information Systems Engineering Workshops (CaiSE 2012), Lecture notes in Business Information Processing. Vol. 112*. Berlin: Springer, 2012. ISBN 978-3-642-31069-0, p. 4.

model faktorov vplyvu (v origináli The Generic Enabler Model) určený pre profesionálov v oblasti informačnej bezpečnosti a iné zainteresované strany. Publikácia patrí do komplexného rámca COBIT 5, ktorý napomáha podnikom úspešne spravovať, riadiť a získavať optimálnu hodnotu podnikovej informatiky.[75] Avšak, orientuje sa výhradne na manažment podnikovej informačnej bezpečnosti s využitím princípov, cieľov, metodík a odporúčaní rámca.

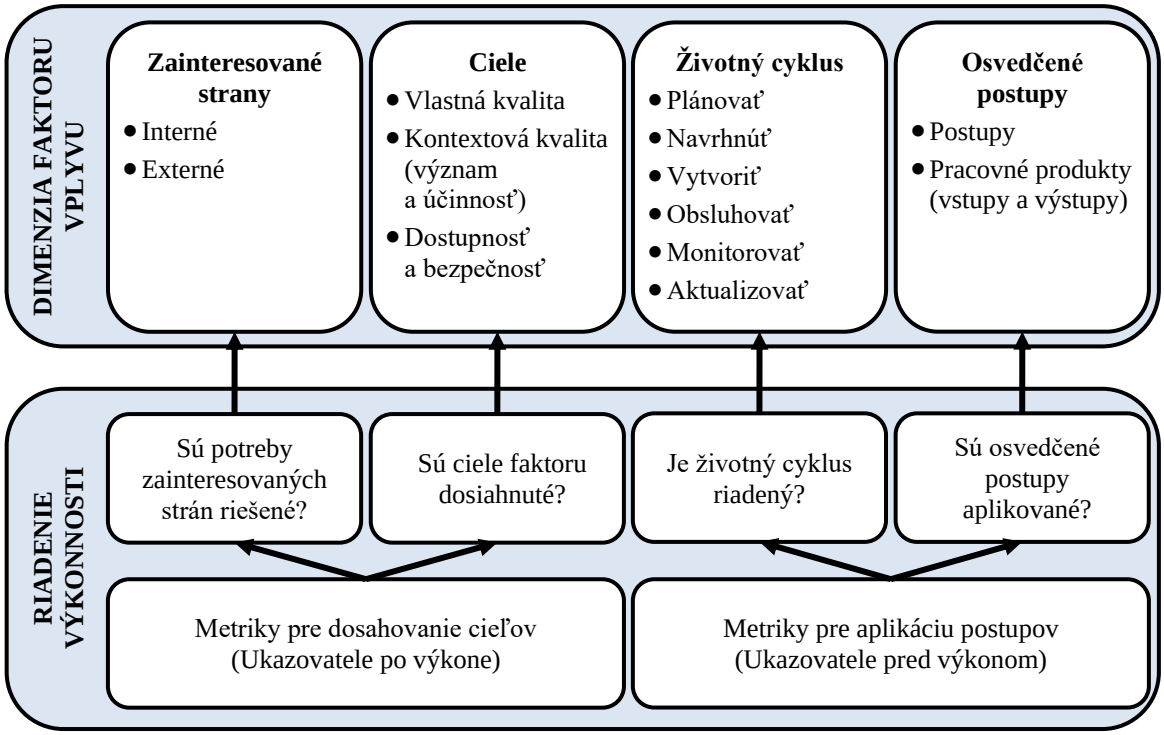
COBIT 5 definuje sedem kategórií faktorov vplyvu na podnik, ktoré mu umožňujú napredovať, a ktoré podporujú implementáciu pokročilej správy systémov podnikovej informatiky a spracovania informácií. Na obrázku 6 vidíme faktory vplyvu, ktoré medzi sebou komunikujú, sú interaktívne a jednotlivo alebo spoločne ovplyvňujú chod podnikových IT so zameraním na správu IB. Všetky prepojené faktory vplyvu je potrebné prediskutovať a upravovať. Týmto spôsobom možno získať skutočný holistický a systémový prístup k IB.[76]



Obr. 6: Interaktívne faktory vplyvu podľa COBIT 5
Zdroj: ISACA. 2012 (b). *COBIT 5 for Information Security.* Rolling Meadows: ISACA, 2012. s. 23. ISBN 978-1-60420-255-7.

Všeobecný model faktorov vplyvu (pozri obrázok 7) aplikuje princípy riadenia informačnej bezpečnosti cez riadenie výkonnosti štyroch dimenzií faktoru vplyvu. Dimenziami sú zainteresované strany, ciele, životný cyklus a osvedčené postupy podniku. Model sa prispôsobuje pre každý faktor vplyvu zvlášť, pričom sa zdôrazňujú tie dimenzie, ktoré sa konkrétneho faktoru priamo dotýkajú.

[75] ISACA. 2012 (a). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.* Rolling Meadows: ISACA, 2012. s. 13. ISBN 978-1-60420-237-3.
[76] ISACA. 2012 (b). *COBIT 5 for Information Security.* Rolling Meadows: ISACA, 2012. s. 23. ISBN 978-1-60420-255-7.



Obr. 7: Všeobecný model faktorov vplyvu
Zdroj: ISACA. 2012 (b). *COBIT 5 for Information Security.* Rolling Meadows: ISACA, 2012. s. 25. ISBN 978-1-60420-255-7.

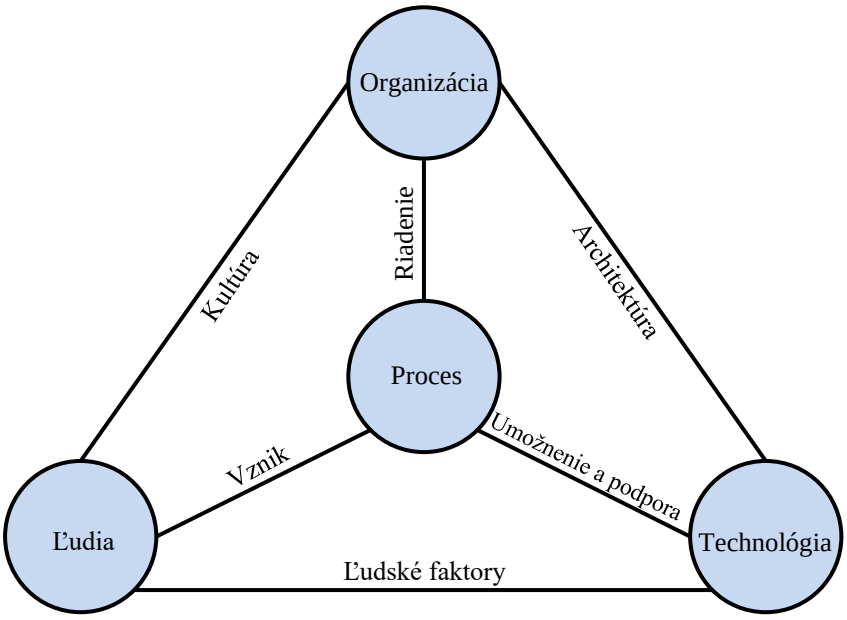
Podniky očakávajú pozitívne výstupy z aplikácie a využitia faktorov vplyvu. Riadenie výkonnosti konkrétneho faktoru určuje pravidelné monitorovanie a zodpovedanie uvedených otázok na základe stanovených metrík pre dosahovanie cieľov alebo aplikáciu postupov. [77] Model začleňuje požiadavky na riadenie IB do podniku ako celku, so všetkými jeho procesmi, štruktúrami, kultúrou, politikami, technológiami, atď. Je prehľadný, jasne definovaný a cez riadenie výkonnosti odovzdáva spätnú väzbu zodpovednému personálu.

1.2.7 Model BMIS

V roku 2008 organizácia ISACA uzavrela dohodu s inštitútom ICIIP, USC Marshall School of Business, na spoluprácu vo vývoji manažérskeho modelu systémovej ochrany BMIS, vo voľnom preklade Biznis model informačnej bezpečnosti.[78] BMIS je vyváženým modelom s tromi dimenziami (pozri obrázok 8). Pozostáva zo štyroch prvkov a šiestich dynamických spojení. Ak sú časti modelu pozmenené, prípadne pretrvávajú bezpečnostné nedostatky, model sa stane nevyváženým, čo významne ovplyvní úroveň IB podniku.

[77] ISACA. 2012 (b). *COBIT 5 for Information Security.* Rolling Meadows: ISACA, 2012. s. 26. ISBN 978-1-60420-255-7.
[78] MARSHALL. 2008. *USC Marshall Institute Licenses New Information Security Model*. [online]. 2008 [cit. 2017-03-20]. Dostupné na internete: <https://www.marshall.usc.edu/news/releases/2008/usc-marshall-institute-licenses-new-information-security-model>.

Model BMIS pristupuje k ISMS z pohľadu podnikateľskej činnosti a vychádza zo základných konceptov vyvinutých inštitútom ICIIP. Model využíva systémy, ktoré objasňujú zložité vzťahy v rámci podniku, a tým efektívnejšie riadi bezpečnosť. Prvky a dynamické prepojenia, ktoré sú výsledkom systémového prístupu,[79] stanovujú hranice programu IB, modelujú funkčnosť programu a reagujú na interné a externé zmeny. BMIS poskytuje kontext, v ktorom sú rámce (napr. COBIT) a štandardy (napr. ISO/IEC 27001) zosúladené. Podniky využívajú rámce a štandardy na vytvorenie štruktúry aktivít programu IB. V procese zosúladenia sa formuje holistický a dynamický prístup k IB, ktorý je zároveň prediktívny a proaktívny, pretože sa prispôsobuje zmenám, posudzuje organizačnú kultúru a prináša hodnotu pre podnikanie.[80]



Obr. 8: Model BMIS
Zdroj: ISACA. 2010. *The Business Model for Information Security.* Rolling Meadows: ISACA, 2010. s. 13. ISBN 978-1-60420-154-3.

BMIS primárne určuje tri tradičné prvky IT (ľudia, procesy a technológie) a zároveň pridáva kritický štvrtý prvok, organizáciu. Pokiaľ ide o program IB, pružnosť a vplyv prvkov a dynamických spojení sa líšia. Niektoré prvky sú pomerne neaktívne, ale vždy prítomné, ako napríklad celkový tvar a dizajn organizácie. Rovnako ľudia sú dôležitým prvkom, ktorý sa v priebehu času nemení. Ľudská povaha pretrváva a len prostredníctvom kultúrnych zmien sa správanie prispôsobí tomu, čo chce bezpečnostný program dosiahnuť.

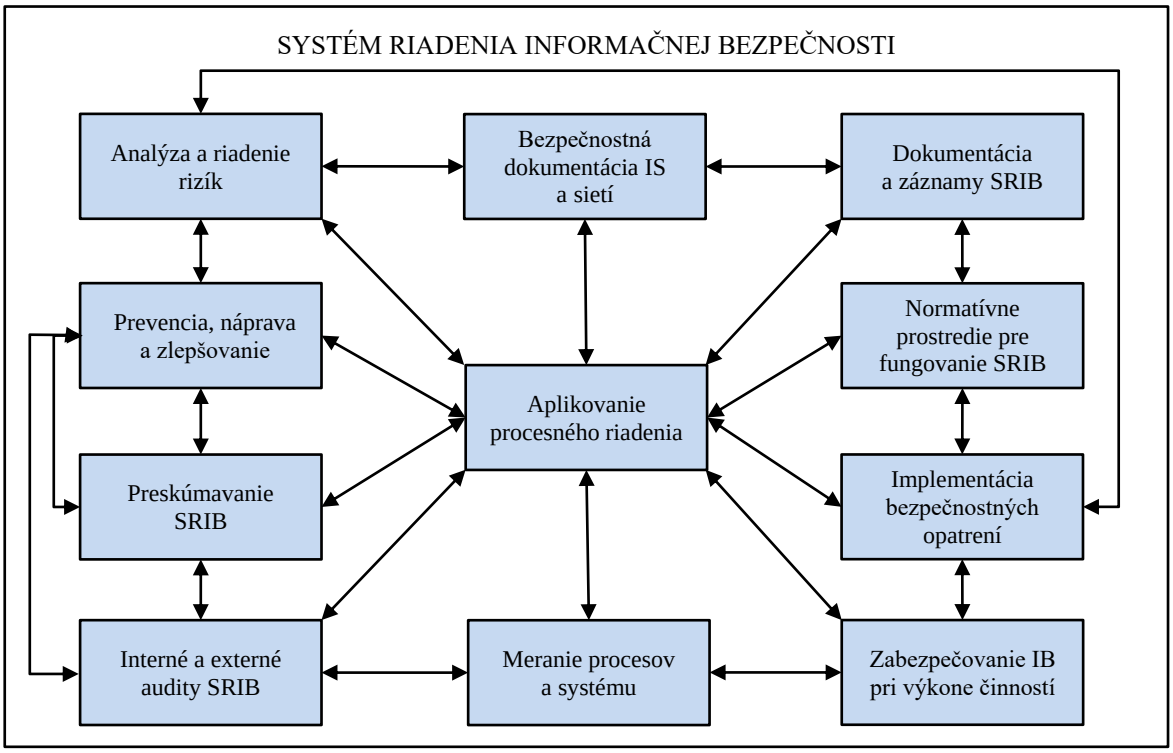
[79] ISACA. 2010. *The Business Model for Information Security.* Rolling Meadows: ISACA, 2010. s. 13. ISBN 978-1-60420-154-3.
[80] ISACA. 2009. *An Introduction to the Business Model for Information Security.* [online]. 2009 [cit. 2017-03-20]. Dostupné na internete: <http://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf>.

Pre získanie maximálnej hodnoty z tohto modelu je dôležité si uvedomiť, že dynamické spojenia môžu byť priamo alebo nepriamo ovplyvnené zmenami generovanými vo všetkých komponentoch modelu, nielen dvomi prvkami na oboch koncoch.[81]

Prvky a spojenia modelu sú logicky prepojené a harmonicky usporiadané. Podniky na udržanie adekvátnej úrovne IB a vytvorenie manažmentu IB ako systému potrebujú sústrediť svoje zdroje na všetky prvky a dynamické spojenia, avšak v každom podniku rozdielne v závislosti na špecifických podmienkach podnikateľského prostredia.

1.2.8 Mapa procesov systému riadenia informačnej bezpečnosti

Ďalší spomedzi grafických modelov, ktorý slúži ako vzor pre organizácie, uvádzame na obrázku 9 s názvom Mapa procesov systému riadenia informačnej bezpečnosti (SRIB).



Obr. 9: Mapa procesov SRIB
Zdroj: STRNÁD, O. 2011. *Systém riadenia informačnej bezpečnosti.* Ostrava: Amos, 2011. s. 174. ISBN 978-80-904766-6-0.

Mapa procesov znázorňuje konkrétne podsystémy s ich vzťahmi vyjadrenými orientovanými šípkami. Tie naznačujú výmenu informácií medzi jednotlivými podsystémami. Podsystémy sú procesy, ktorých kombináciu je potrebné vyberať tak, aby bolo dosiahnuté maximálne pokrytie riadenia IB v organizácii.[82] Autor pri tvorbe modelu

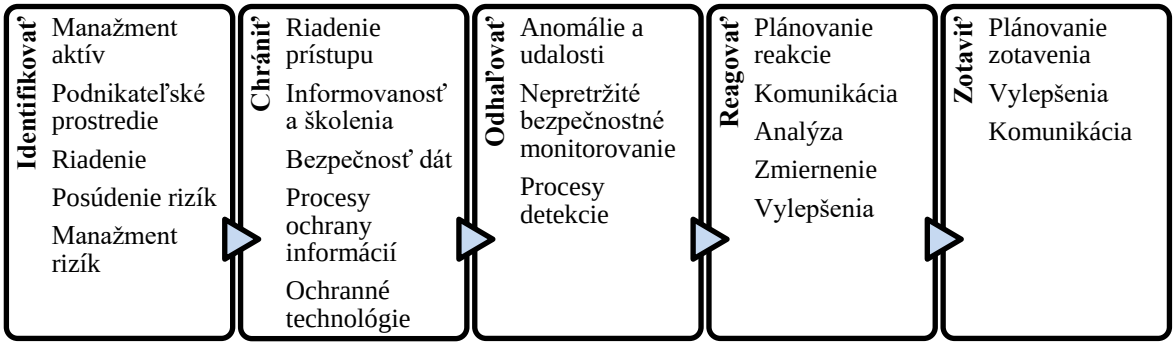
[81] ISACA. 2010. *The Business Model for Information Security.* Rolling Meadows: ISACA, 2010. s. 13. ISBN 978-1-60420-154-3.
[82] STRNÁD, O. 2011. *Systém riadenia informačnej bezpečnosti.* Ostrava: Amos, 2011. s. 167–168. ISBN 978-80-904766-6-0.

vychádzal z noriem ISO/IEC 27001 a ISO/IEC 27002, v ktorých identifikoval kľúčové procesy manažmentu informačnej bezpečnosti a ich väzby.

Ústredným procesom je aplikovanie procesného riadenia, ktoré v každom z procesov apeluje na ich kontinuálne vykonávanie a zdokonaľovanie. Model kladie dôraz na procesy riadenia rizík, vytvárania systému riadenia IB, vykonávania auditov, merania procesov a celého systému, tvorby a aktualizácie dokumentácie, zavedenia bezpečnostných opatrení a súladu s dodržiavaním politík, prípadne noriem alebo osvedčených postupov. V organizácii je zároveň nutné využívať vhodný spôsob výmeny informácií medzi procesmi, pretože bez komunikácie medzi procesmi nie je možné riadiť IB ako systém.

1.2.9 Rámec kybernetickej bezpečnosti

Model, ktorý je uvedený na obrázku 10, vychádza z Rámca kybernetickej bezpečnosti podľa amerického inštitútu NIST.



Obr. 10: Funkcie a kategórie rámca kybernetickej bezpečnosti
Zdroj: NIST. 2014. *Framework for Improving Critical Infrastructure Cybersecurity.* [online]. National Institute of Standards and Technology, 2014. s. 19 [cit. 2017-03-14]. Dostupné na internete: <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

Model určuje funkcie a definuje kategórie, ktoré organizácia vykonáva na dosiahnutie adekvátnej kybernetickej bezpečnosti procesným spôsobom. Rámec kybernetickej bezpečnosti bol pôvodne navrhnutý pre kritickú infraštruktúru. Avšak, stal sa celosvetovo uznávaným a množstvo organizácii činných v oblasti IB prevzalo základné funkcie a odporúčania rámca do svojich metodík a osvedčených postupov ochrany informácií. NIST ale zdôrazňuje, že rámec nedokáže pokryť kybernetické riziká všetkých organizácií, ktoré vždy budú unikátne v dôsledku rôznych hrozieb, zraniteľností, tolerancie rizika a rôznych implementačných praktík rámca v organizáciách.[83]

[83] NIST. 2014. *Framework for Improving Critical Infrastructure Cybersecurity.* [online]. National Institute of Standards and Technology, 2014. s. 2 [cit. 2017-03-14]. Dostupné na internete: <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

Jadro modelu podľa rámca kybernetickej bezpečnosti pozostáva z piatich súbežných a kontinuálnych funkcií, ktoré poskytujú vysokú úroveň a strategický pohľad na životný cyklus riadenia kybernetického rizika v organizácii. Funkcie definujeme nasledovne:[84]

- *Identifikovať* – rozvíjať organizačné porozumenie pre riadenie kybernetických rizík v systémoch, aktívach, dátach a schopnostiach,
- *Chrániť* – rozvíjať a realizovať vhodné bezpečnostné opatrenia, aby zabezpečili dodávku kritických služieb,
- *Odhaľovať* – rozvíjať a vykonávať vhodné činnosti na identifikáciu výskytu kybernetických udalostí,
- *Reagovať* – rozvíjať a implementovať vhodné činnosti na prijatie opatrení v súvislosti s detegovanými kybernetickými udalosťami,
- *Zotaviť* – rozvíjať a implementovať vhodné činnosti na udržanie plánov odolnosti a obnovy všetkých funkcií a služieb, ktoré boli znehodnotené v dôsledku udalosti kybernetickej bezpečnosti.

Model je univerzálny a obsahom ho možno prirovnať k PDCA, oproti ktorému identifikuje konkrétne činnosti (kategórie) ISMS pre jednotlivé funkcie. Na druhej strane nezdôrazňuje potrebu opakovania funkcií po ukončení záverečnej funkcie tak ako model PDCA. Procesný prístup zabezpečuje samostatnou činnosťou Vylepšenia vo funkcii Zotaviť.

1.2.10 Porovnanie vybraných modelov

Z dôvodu získania uceleného prehľadu identifikujeme podobnosti a odlišnosti modelov manažmentu informačnej bezpečnosti z rôznych aspektov. Syntéza nadobudnutých poznatkov je jedným zo vstupov do návrhu modelu manažmentu informačnej bezpečnosti zameraného na prostredie elektronického podnikania. V tabuľke 7 porovnávame predstavené modely, ich podstatu, cieľ, zameranie a východiská. Ako dimenzie komparácie sme vybrali konkrétne požiadavky na implementáciu a zdokonaľovanie ISMS podľa normy ISO/IEC 27001 (kontext v organizácii, postavenie vedenia, plánovanie, podpora, prevádzka, vyhodnotenie výkonnosti a zlepšovanie), ktoré odhalia odlišnosti, prednosti a prípadné nedostatky modelov. Na základe predností a nedostatkov vyhodnocujeme možnosti uplatnenia modelov v oblasti elektronického podnikania, čím určíme, ktoré modely možno aplikovať na všetky procesy, prípadne len na špecifické procesy elektronického podnikania.

[84] ISACA. 2014. *Implementing the NIST Cybersecurity Framework.* Rolling Meadows: ISACA, 2014. s. 29 – 31. ISBN 978-1-60420-358-5.

Tab. 7: Porovnanie vybraných modelov manažmentu informačnej bezpečnosti

Model	PDCA	Activate Adapt Anticipate	Confidentiality Integrity Availability	TQISM	Doménový model ISSRM	Všeobecný model faktorov vplyvu	BMIS	Mapa procesov SRIB	Model podľa Rámca kybernetickej bezpečnosti
Podstata	Proces	Proces	Deskripcia	Proces	Entity a relácie	Analýza	Koncepcia	Súbor procesov	Proces
Cieľ	Kontinuálne zlepšovanie	Budovanie systému	Zosúladenie vlastností IB	Vysoká úroveň kvality IB	Iteratívny proces riadenia rizík	Holistický, systémový prístup k IB	Zosúladenie, holistický prístup k IB	Procesné riadenie IB	Vysoká úroveň kybernetickej bezpečnosti
Zameranie	Univerzálne	Organizácie	Organizácie	Organizácie	Organizácie	Podniky	Podniky	Organizácie	Univerzálne
Východisko	Výskum Shewharta a Deminga	Vlastný prieskum EY	Vlastnosti IB	Total Quality Management	Rizikový manažment	COBIT 5	Podnikateľská činnosť	ISO/IEC 27001, 27002	NIST – Rámec kybernetickej bezpečnosti
Kontext v organizácií	Úplné včlenenie	Nezaoberá sa	Nezaoberá sa	Potreba doplnenia	Nezaoberá sa	Úplné včlenenie	Potreba doplnenia	Chýba určenie rozsahu	Chýba určenie rozsahu
Postavenie vedenia	Úplné včlenenie	Nezaoberá sa	Nezaoberá sa	Čiastočné včlenenie	Nezaoberá sa	Úplné včlenenie	Čiastočné včlenenie	Čiastočné včlenenie	Čiastočné včlenenie
Plánovanie	Úplné včlenenie	Potreba doplniť ciele	Čiastočné včlenenie	Úplné včlenenie	Čiastočné včlenenie	Chýba posúdenie rizík	Chýbajú ciele, posúdenie rizík	Úplné včlenenie	Potreba doplniť ciele
Podpora	Úplné včlenenie	Nezaoberá sa	Nezaoberá sa	Čiastočné včlenenie	Nezaoberá sa	Čiastočné včlenenie	Úplné včlenenie	Úplné včlenenie	Čiastočné včlenenie
Prevádzka	Úplné včlenenie	Úplné včlenenie	Úplné včlenenie	Úplné včlenenie	Úplné včlenenie	Chýba posúdenie rizík	Chýba posúdenie rizík	Úplné včlenenie	Úplné včlenenie
Vyhodnotenie výkonnosti	Úplné včlenenie	Nezaoberá sa	Nezaoberá sa	Úplné včlenenie	Nezaoberá sa	Úplné včlenenie	Nezaoberá sa	Úplné včlenenie	Čiastočné včlenenie
Zlepšovanie	Úplné včlenenie	Čiastočné včlenenie	Nezaoberá sa	Úplné včlenenie	Nezaoberá sa	Úplné včlenenie	Potreba doplnenia	Úplné včlenenie	Úplné včlenenie
Uplatnenie v elektronickom podnikaní	Všetky procesy bez obmedzení	Len ochrana kybernetického priestoru	Riadenie rizík IB, niektoré procesy ISMS	ISMS ako celok	Riadenie rizík IB, niektoré procesy ISMS	Všetky procesy bez obmedzení	Strategický manažment, ISMS ako celok	ISMS ako celok	ISMS ako celok

Zdroj: vlastné spracovanie

Podľa komparácie v tabuľke 7 pozorujeme zhody a viaceré odlišnosti skúmaných modelov. Väčšina modelov je procesne orientovaná so všeobecnou aplikovateľnosťou v organizáciách. Modely PDCA a podľa Rámca kybernetickej bezpečnosti možno použiť univerzálne, čiže aj na špecifické činnosti alebo procesy vo vnútri a mimo organizácie, prípadne v úplne inom prostredí a podmienkach. Pretože každý model vychádza z iného výskumu, prostredia, štandardu či rámca, má odlišný cieľ dosiahnutia informačnej bezpečnosti v organizácii. Avšak, spoločne sa zhodujú na potrebe dosiahnutia primeranej úrovne ISMS v organizácii.

Model, ktorý zahŕňa všetky požiadavky normy na manažment informačnej bezpečnosti, je PDCA. Na druhej strane sú modely, ktoré sa zameriavajú na včlenenie len špecifickej sady požiadaviek (ISSRM, Activate – Adapt – Anticipate, Confidentiality – Integrity – Availability). Ostatné modely vyzdvihujú jednu alebo viac oblastí požiadaviek ISMS a zároveň sa niektorými požiadavkami zaoberajú viac, inými menej. Nedostatky, ktoré sme identifikovali, považujeme za potrebné v modeloch doplniť, napríklad v oblasti kontext v organizácii, modely TQISM a BMIS nevčleňujú požiadavky porozumenia zainteresovaných strán a Mapa procesov s Modelom podľa Rámca kybernetickej bezpečnosti sa nezaoberajú určením rozsahu ISMS. Pri čiastočnom včlenení a pri nezaoberaní sa danými požiadavkami nepovažujeme za potrebné modely a ich odporúčania dopĺňať, pretože nenarušujú stanovené ciele. Ak sme však identifikovali, že určitá časť požiadaviek chýba, modely odporúčame doplniť, prípadne rozvinúť pre získanie adekvátnej úrovne ISMS v podnikoch.

Z pohľadu uplatnenia tvrdíme, že všetky modely možno v určitej miere aplikovať do prostredia podnikov, ktoré sú aktívne v elektronickom podnikaní. Avšak, nie všetky modely rovnakým spôsobom a na všetky procesy. Všeobecný model faktorov vplyvu spolu s PDCA hodnotíme ako najkomplexnejšie modely, ktoré môžeme využiť nielen v rámci manažmentu informačnej bezpečnosti podniku, ale vo všetkých procesoch elektronického podnikania bez obmedzení. Ostatné modely sú aplikovateľné buď na ISMS ako celok (TQISM, BMIS, Mapa procesov SRIB, Model podľa Rámca kybernetickej bezpečnosti) alebo na špecifické procesy ISMS, napríklad na ochranu kybernetického priestoru (Activate – Adapt – Anticipate) a riadenie informačných rizík (ISSRM, Confidentiality – Integrity – Availability). Z dostupných informácií vyplýva, že model BMIS je vhodné využívať aj pri strategickom riadení podniku.

1.3 Elektronické podnikanie

Hierarchicky najvyššou úrovňou pre podnikateľské aktivity realizované využitím IKT je elektronické podnikanie (e–business), ktorého aktivity sú prepojené s obchodnými a výrobnými činnosťami a činnosťami, ktoré sú potrebné na podporu, integráciu a riadenie oboch uvedených skupín s cieľom poskytovať služby zákazníkom.[85] Elektronické podnikanie predstavuje „vnútropodnikové a medzipodnikové procesy a transakcie medzi dodávateľmi, zákazníkmi, podnikmi a podnikovými tímami s minimálnym počtom medzičlánkov, čiže obchodné, pracovné procesy a podnikové interakcie s prostredím uskutočňované elektronicky. Je základným predpokladom úspešnej organizácie v novovznikajúcom, globálne na internete prepojenom a výkonnom podnikateľskom prostredí.“[86] Podľa Rousovej a tiež Rakovskej ide o vykonávanie obchodných procesov na internete. Tieto elektronické procesy zahŕňajú nákup a predaj produktov a služieb, servis zákazníkov, spracovanie platieb, riadenie výroby, spoluprácu s obchodnými partnermi, zdieľanie informácií, prevádzkovanie automatických služieb pre zamestnancov, nábor zamestnancov, atď.[87] [88] Stotožňujeme sa so zjednodušenou definíciou podľa Laudona a Travera, ktorí tvrdia, že elektronické podnikanie je digitálnym umožnením transakcií a procesov v rámci podniku vrátane informačných systémov pod kontrolou podniku.[89] Jeho rozvoj je pozitívne ovplyvňovaný informatizáciou spoločnosti, postupným celosvetovým rozširovaním internetu a popularitou mobilných technológií.

Elektronické podnikanie prebieha na elektronickom trhu, ktorý predstavuje obchodné fórum na internete, kde si kupujúci a predávajúci vymieňajú tovar a služby.[90] V dôsledku vysokej úrovne hospodárskej súťaže na tradičných trhoch, mnohé začínajúce, ale aj etablované podniky vstupujú do elektronického prostredia a dostávajú sa na nové trhy prostredníctvom online predajných aktivít, čím napokon zvyšujú svoje tržby.[91] Elektronický trh je prostredím na internete, ktoré otvára podnikateľom dodatočné obchodné príležitosti

[85] SUCHÁNEK, P. 2012. *E-commerce: Elektronické podnikání a koncepce elektronického obchodování.* Praha: Ekopress, 2012. s. 9-11. ISBN 978-80-86929-84-2.
[86] SIVÁK, R. a kol. 2011. *Slovník znalostnej ekonomiky*. Bratislava: Sprint 2, 2011. s. 59. ISBN 978-80-89383-45-9.
[87] ROUSE, M. 2014. *E-business (electronic business)*. [online]. 2014 [cit. 2017-06-17]. Dostupné na internete: <http://searchcio.techtarget.com/definition/e-business>.
[88] RAKOVSKÁ, E. 2016. New aspects and tasks of knowledge management in the e-business era. In *11th International workshop on knowledge management: conference proceedings*. Trenčín: Vysoká škola manažmentu v Trenčíne, 2016. ISBN 978-80-89306-33-6. p. 81.
[89] LAUDON, K. C., – TRAVER, C. G. 2014. *E-commerce: business, technology, society*. 10th ed. New Jersey: Pearson, 2014. s. 10. ISBN 978-0-13-302444-9.
[90] CHENG, C. B. – CHAN, C. C. H. – LIN, K. C. 2006. Intelligent agents for e-marketplace: Negotiation with issue trade-offs by fuzzy inference systems. In *Decision Support Systems*. ISSN 0167-9236, 2006, vol. 40, no. 2, p. 626.
[91] WIRADINATA, T. 2017. Nascent entrepreneurs in e-marketplace: The effect of founders' self-efficacy and personality. In *International Journal of Electronic Business*. ISSN 1470-6067, 2017, vol. 13, no. 2/3, p. 164.

(napríklad lepší dosah na cieľovú skupinu, efektívnejší marketing, viac zákazníkov) a umožňuje rozšírenie pôsobenia podniku z lokálnej úrovne na celoštátnu alebo až na globálnu úroveň.

Elektronický obchod (e–commerce) je súčasťou elektronického podnikania. Zahŕňa elektronickú výmenu digitálneho obsahu medzi viacerými subjektmi, ktorej výsledkom je peňažná výmena.[92] E–commerce sa „používa na označenie akýchkoľvek obchodných procesov a transakcií uskutočňovaných buď úplne, alebo čiastočne prostredníctvom elektronických komunikačných prostriedkov, predovšetkým internetu. Elektronický obchod znamená využitie informačno–komunikačných technológií na zvýšenie efektívnosti vzťahov medzi podnikmi a individuálnymi používateľmi.“[93] Stotožňujeme sa s definíciou, podľa ktorej elektronický obchod znamená využitie internetu, webových stránok a aplikácií na obchodné transakcie, čiže predstavuje digitálne umožnené transakcie medzi organizáciami a jednotlivcami.[94]

Najnižšou úrovňou elektronického podnikania a zároveň súčasťou elektronického obchodu je internetový obchod (e–shop), ktorý dodáva elektronickému obchodu komunikačné rozhranie prostredníctvom webových aplikácií. Dátová komunikácia prebieha v internom prostredí cez informačné systémy a LAN, v externom cez internet.[95] V prostredí internetového obchodu dostupného cez internetový prehliadač alebo webovú aplikáciu zákazníci prehliadajú tovar alebo služby a následne uskutočňujú ich nákup.

Podnikanie s implementovaným elektronickým obchodom klasifikujeme na štyri základné kategórie podľa subjektov, ktorí vstupujú do vzájomnej komunikácie. Základnými kategóriami z hľadiska orientácie na podniky a koncových spotrebiteľov sú:[96]

- *B2C* – predaj realizovaný cez webové aplikácie medzi podnikom a spotrebiteľom,
- *B2B* – elektronický predaj realizovaný medzi podnikmi a inštitúciami vo forme zásobovania, zákazníckej podpory, atď.,
- *C2C* – internetové aukcie a inzercie, ktoré umožňujú poskytovať tovar a služby medzi spotrebiteľmi,

[92] CHEN, S. 2005. *Strategic Management of E-business*. 2nd ed. Chichester: John Wiley & Sons, 2005. s. 3. ISBN 0-470-87073-7.
[93] SIVÁK, R. a kol. 2011. *Slovník znalostnej ekonomiky.* Bratislava: Sprint 2, 2011. s. 60. ISBN 978-80-89383-45-9.
[94] LAUDON, K. C., – TRAVER, C. G. 2014. *E-commerce: business, technology, society*. 10th ed. New Jersey: Pearson, 2014. s. 10. ISBN 978-0-13-302444-9.
[95] SUCHÁNEK, P. 2012. *E-commerce: Elektronické podnikání a koncepce elektronického obchodování.* Praha: Ekopress, 2012. s. 9-11. ISBN 978-80-86929-84-2.
[96] CHEN, S. 2005. *Strategic Management of E-business*. 2nd ed. Chichester: John Wiley & Sons, 2005. s. 2. ISBN 0-470-87073-7.

- *C2B* – spotrebitelia určujú vlastné ceny produktov, ktoré chcú nakúpiť cez webové aplikácie reverzných aukcií, prípadne sa spotrebiteľ podieľa na návrhu nových konceptov produktov a riešení s podnikom cez sociálne siete.[97]

Elektronické podnikanie sa vyznačuje mnohými výhodnými vlastnosťami pre podniky a ich zákazníkov, najmä v dobe konvergencie technológií. V nasledujúcich bodoch uvádzame vlastnosti, ktoré majú pre elektronické podnikanie najväčší význam:[98]

- *Všadeprítomnosť* – nakupovanie prebieha všade, kde je dostupný internet; zákazník má zvýšené pohodlie a nižšie ceny,
- *Globálny dosah* – trh, ktorý obsahuje milióny podnikov a miliardy zákazníkov, nie je vymedzený národnými a kultúrnymi hranicami,
- *Bohatstvo* – dojem zákazníka je vylepšený bohatstvom multimediálnych marketingových správ, ktoré obsiahnu video, audio, text, atď.,
- *Interaktivita* – spotrebiteľ je vzájomným pôsobením s technológiou podniku súčasťou procesu doručovania tovarov a služieb na trh,
- *Univerzálne štandardy* – skupina technických mediálnych štandardov je medzinárodne jednotná,
- *Hustota informácií* – technológia redukuje cenu informácie a zvyšuje jej kvalitu a dostupnosť,
- *Personalizácia* – možnosť doručovania prispôsobených marketingových správ a produktov podľa zákazníkových preferencií,
- *Technológia sociálnych sietí* – unikátny model komunikácie cez internet, ktorá vytvára nové sociálne siete a posilňuje existujúce.

Ak podniky chcú získať výhody uvedených vlastností, potrebujú vytvoriť a zaviesť vhodný proces elektronického podnikania. Ten pozostáva z vyriešenia viacerých oblastí, napríklad výberu technického riešenia, zabezpečenia marketingu, logistiky, vytvorenia obchodných a reklamačných podmienok, dodržiavania príslušných zákonov, výberu cieľovej skupiny, nákup a servis produktov, atď. Zároveň, proces elektronického podnikania má tvoriť súlad s ostatnými procesmi podniku.

Rozsah procesu elektronického podnikania so všetkými spomínanými oblasťami narastá s veľkosťou podniku. Navyše, spôsob riadenia elektronického podnikania sa líši

[97] ARLINE, K. 2015. *What is C2B?* [online]. 2015 [cit. 2015-12-10]. Dostupné na internete: <http://www.businessnewsdaily.com/5001-what-is-c2b.html>.
[98] LAUDON, K. C., – TRAVER, C. G. 2014. *E-commerce: business, technology, society*. 10th ed. New Jersey: Pearson, 2014. s. 13. ISBN 978-0-13-302444-9.

medzi jednotlivými kategóriami podnikov podľa ich veľkosti a právnej formy. Na základe nariadenia Európskej komisie členíme podniky v SR a EÚ podľa počtu zamestnancov, ročného obratu alebo celkovej ročnej súvahy. Toto členenie sa nachádza v tabuľke 8.

Tab. 8: Kritériá pre členenie podnikov podľa veľkosti

	Počet zamestnancov	Ročný obrat	Celková ročná súvaha
Mikropodnik	0 – 9	do 2 mil. €	do 2 mil. €
Malý podnik	10 – 49	2 – 10 mil. €	2 – 10 mil. €
Stredný podnik	50 – 249	10 – 50 mil. €	10 – 43 mil. €
Veľký podnik	250 a viac	nad 50 mil. €	nad 43 mil. €

Zdroj: EUR-LEX. 2014. *Nariadenie komisie (EÚ) č. 651/2014.* [online]. 2014. [cit. 2015-12-10]. Dostupné na internete: <http://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32014R0651>.

V niektorých prípadoch nie je jednoduché určiť, do ktorej kategórie podnik patrí. Preto sa v nasledujúcich častiach dizertačnej práce pridržiavame členenia podľa počtu zamestnancov. Aktuálny stav podnikania v SR, ktoré môže uskutočňovať jednotlivec alebo kolektív[99], sledujeme v tabuľke 9. Prehľad ukazuje celkový nárast v počte nových ekonomických subjektov v roku 2016 oproti predchádzajúcemu roku.

Tab. 9: Počet ekonomických subjektov v Slovenskej republike

Právna forma	2015				2016			
	Počet zamestnancov				Počet zamestnancov			
	0 – 49	50 – 249	≥ 250	Spolu[i]	0 – 49	50 – 249	≥ 250	Spolu[i]
Akciové spoločnosti	2 512	572	247	5 340	2 453	552	236	5 516
Spoločnosť s ručením obmedzeným	97 529	1 949	336	176 956	95 497	1 885	324	193 300
Ostatné obchodné spoločnosti	393	22	4	1 235	362	22	4	1 288
Družstvá	765	147	33	1 323	755	143	33	1 353
Štátne podniky	3	10	5	18	2	8	4	15
Príspevkové organizácie	413	202	18	638	403	207	23	641
Rozpočtové organizácie	5 205	1 095	82	6 395	5 187	1 090	83	6 372
Živnostníci	186 218	63	–	316 460	175 360	57	–	322 968
Fyzické osoby (bez živnostníkov)	12 181	–	–	22 007	13 409	57	–	24 024
Ostatné právne formy	11 020	206	79	15 750	11 040	206	82	19 625
Spolu	**316 239**	**4 266**	**804**	**546 122**	**304 468**	**4 170**	**789**	**575 102**

Poznámka: [i]vrátane ekonomických subjektov s nezisteným počtom zamestnancov
Zdroj: STATDAT. 2017. *Ekonomické subjekty v RO podľa vybraných právnych foriem a kategórie počtu zamestnancov.* [online]. 2017 [cit. 2017-03-04]. Dostupné na internete: <https://goo.gl/TAKlhc>.

Pre podnikanie v SR sú najviac využívané živnosti, nasledujú spoločnosti s ručením obmedzeným a akciové spoločnosti v oboch uvádzaných rokoch. V SR sú najpočetnejšie a zároveň nezastupiteľné mikro a malé podniky a organizácie, ktorých počet v roku 2016 poklesol o 3,8 % na 304 468 oproti roku 2015. V najväčšej miere ich v roku 2016 zastupujú

[99] ŠÚBERTOVÁ, E. a kol. 2014. *Podnikanie v malých a stredných podnikoch: modelové príklady.* Bratislava: KARTPRINT, 2014. s. 22. ISBN 978-80-89553-21-1.

živnostníci a spoločnosti s ručením obmedzeným. Medziročný pokles bol zaznamenaný aj pre stredné (o 2,9 %) a veľké podniky a organizácie (o 1,8 %). Stredné podniky a organizácie sú aktuálne najviac zastúpené spoločnosťami s ručením obmedzeným a rozpočtovými organizáciami. Spoločnosti s ručením obmedzeným spolu s akciovými spoločnosťami sú súčasnými najvýznamnejšími reprezentantmi veľkých podnikov a organizácií.

1.3.1 Súčasný stav elektronického podnikania

Elektronické podnikanie sa nachádza v štádiu rozmachu. Oproti roku 2011 sa globálne B2C elektronické predaje tovarov a služieb v roku 2014 zdvojnásobili. V roku 2015 narástli o ďalších 20 %. Význam tejto formy podnikania v globálnej ekonomike neustále rastie.[100] Predpokladáme, že trend bude v budúcich rokoch pokračovať.

Krajina, ktorá v roku 2015 zaznamenala najviac elektronických predajov v hodnote približne 514,37 miliárd €, je Čína. Nasleduje USA (318,98 mld.€), Veľká Británia (85,80 mld.€) a Japonsko (72,49 mld.€).[101] Z dôvodu nedostupnosti presných štatistických údajov na rok 2016 si dovoľujeme odhadnúť nezmenené poradie krajín a mierny nárast elektronických predajov pre všetky krajiny. Podľa odhadov asociácie SAEC, v roku 2016 sa celkový obrat z predaja produktov a služieb cez internetové obchody na Slovensku pohyboval na úrovni 900 miliónov €. V porovnaní so svetovými lídrami je to len nízka čiastka, avšak čísla sú ovplyvnené počtom obyvateľov v krajine.[102] Stotožňujeme sa s tvrdením Hasana a kol., že elektronické podnikanie vplýva na hospodárstvo SR.[103]

V roku 2015 porovnávač cien Heureka identifikoval 9355 existujúcich elektronických obchodov na Slovensku s nárastom o 1105 obchodov oproti predchádzajúcemu roku.[104] Týmto tempom bola hranica 10000 elektronických obchodov dosiahnutá už v roku 2016. Pre porovnanie, v roku 2015 bolo v ČR zaznamenaných až 36800 elektronických obchodov.[105] V SR stále vidíme priestor na znásobenie počtu elektronických obchodov, hoci dosiahnuť počty z ČR je problematické v dôsledku

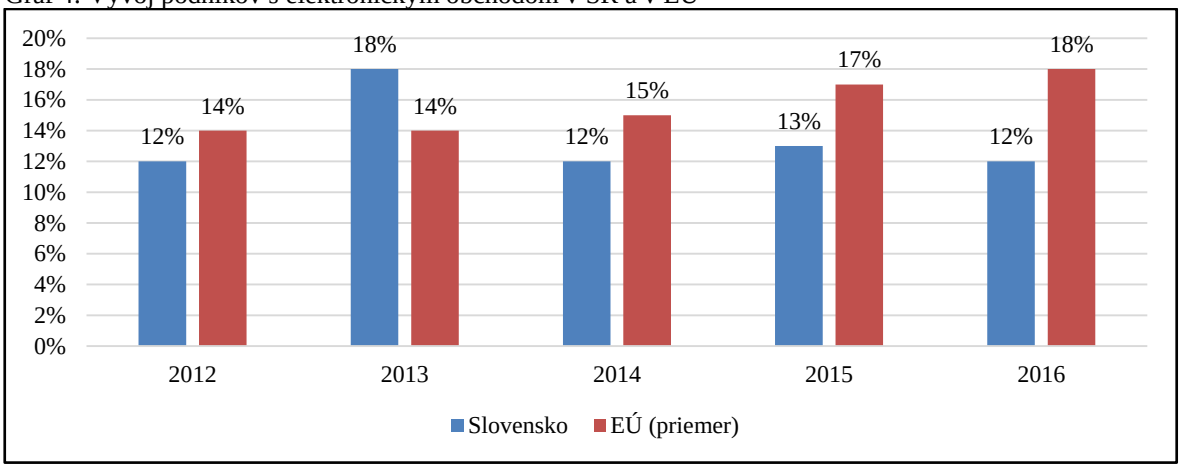
[100] ECOMMERCEFOUNDATION. 2015. *Global B2C E-commerce Report 2015.* [online]. 2015 [cit. 2015-12-10]. Dostupné na internete: <https://www.ecommercefoundation.org/report-info/45/Global-B2C-E-commerce-Report-2015-Light-Version>.
[101] KEITH, M. 2015. *Global ecommerce sales, trends and statistics 2015.* [online]. 2015 [cit. 2015-12-11]. Dostupné na internete: <http://www.remarkety.com/global-ecommerce-sales-trends-and-statistics-2015>.
[102] DVORSKÝ, J. 2016. *Internetový predaj na Slovensku.* [online]. 2016 [cit. 2017-03-06]. Dostupné na internete: <http://www.bezpecnynakup.sk/storage/file/ts_19_10_16.doc>.
[103] HASAN, J. – PÓYA, A. – KITA, P. 2016. E-commerce Impacts on Selected Economic Area in Slovakia. In *International Journal of Innovative Research in Computer and Communication Engineering.* ISSN 2320-9798, 2016, vol. 4, no. 8, p. 14959.
[104] HEUREKA. 2015 (a). *Obrat e-commerce 2015.* [online]. 2015 [cit. 2017-03-10]. Dostupné na internete: <https://www.heurekashopping.sk/resources/attachments/p0/20/heureka-obrat-2015-sk.jpg>.
[105] HEUREKA. 2015 (b). *Obrat e-commerce 2015.* [online]. 2015 [cit. 2017-03-10]. Dostupné na internete: <https://www.heurekashopping.cz/resources/attachments/p0/3/heureka-obrat-2015.pdf>.

dvojnásobne väčšieho počtu obyvateľstva. Množstvo obchodov závisí od slovenských legislatívnych požiadaviek na podnikateľov a elektronické obchody až po konkurenčnú situáciu na elektronickom trhu. Podľa aktuálneho trendu predpokladáme, že maximálny počet elektronických obchodov v SR dosiahne celkový počet 15000.

Štatistický úrad Eurostat zaznamenal, že v slovenských podnikoch s viac ako deviatimi zamestnancami narástol oproti roku 2014 podiel výnosov z elektronického podnikania k celkovému obratu o 5 % na celkových 21 % v roku 2015. Slovenské podniky začali využívať výhody elektronického predaja. Avšak, v roku 2016 bol zaznamenaný pokles na 18 %. Tento pokles pripisujeme väčšiemu nárastu počtu nových podnikov bez elektronického predaja ako podnikov s elektronickým obchodom a tiež zlepšeniu ekonomiky SR a hospodárskych výsledkov podnikov bez elektronického predaja. Priemer EÚ je 16 % s poklesom o 1 % oproti roku 2015. Ukazovateľ aktuálne vedie Írsko, ktorého podniky dosiahli 35 % podiel výnosov k celkovému obratu. Česká republika s Belgickom (31 %) sú ďalšie krajiny v poradí. Najnižší podiel výnosov dosiahli Grécko (6 %), Cyprus (4 %) a Bulharsko (4 %).[106] Podľa nášho názoru majú tieto a ekonomicky podobné krajiny (napr. Rumunsko) potenciál rozvoja elektronického podnikania, ktorý je výsledkom nárastu využívania nových IKT v podnikoch.

V grafe 4 sa nachádza vývoj podielu podnikov s predajom cez elektronický obchod v SR k celkovému počtu podnikov v porovnaní s priemerom EÚ.

Graf 4: Vývoj podnikov s elektronickým obchodom v SR a v EÚ



Zdroj: EUROSTAT. 2017 (b). *E-commerce sales.* [online]. 2017 [cit. 2017-03-09]. Dostupné na internete: <http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ec_eseln2&lang=en>.

Do prieskumu sú zahrnuté podniky mimo finančného sektora s viac ako deviatimi zamestnancami, ktorým elektronický obchod vynáša aspoň jedným percentom z celkového

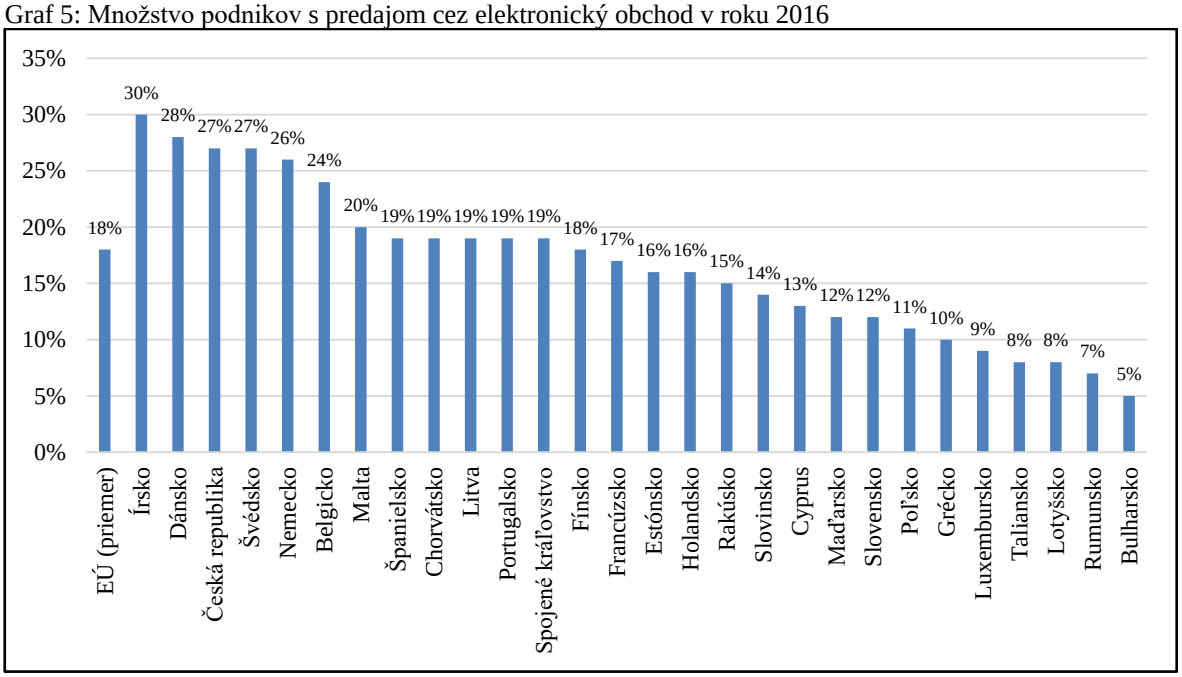
[106] EUROSTAT. 2016. *Share of enterprises´ turnover on e-commerce.* [online]. 2016 [cit. 2017-03-09]. Dostupné na internete: <http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&plugin=1 &language=en&pcode=tin00110>.

obratu. Tento ukazovateľ vylučuje podniky s neaktívnym elektronickým predajom, hoci elektronický obchod vlastniť môžu.

Najlepším rokom bol 2013, kedy až 18 % slovenských podnikov realizovalo predaj cez internet. V roku 2016 uskutočňovalo 12 % slovenských podnikov elektronický predaj tovaru a služieb. Podľa vývoja v SR je zrejmé, že podiel podnikov s elektronickým obchodom sa dlhodobo ustáli na úrovni 12 až 13 % zo všetkých podnikov. Slovenské podniky zaostávajú za priemerom EÚ (18 %) až o 6 %. Od roku 2012 v EÚ každoročne narastá počet podnikov s elektronickým obchodom. Z celkového hľadiska je vývoj elektronického podnikania v EÚ pozitívny. Ustálenú situáciu na slovenskom elektronickom trhu pripisujeme neochote vstupu nových podnikov v dôsledku už etablovaných podnikov v určitých oblastiach (elektronika, IT, kníhkupectvá, zľavové portály a i.) alebo kvôli vysokej konkurencii (móda, šport, cestovanie, atď.). Avšak predpokladáme, že s orientáciou na mobilné zariadenia, odklonom zákazníka od najnižších cien a s tým spojenými dodatočnými službami pre zákazníka (napr. kvalitný servis, poistenie, výhody cez získavanie bodov) bude počet nových podnikov na elektronickom trhu v najbližších rokoch stúpať.

Graf 5 ukazuje percentuálne množstvo podnikov poskytujúcich produkty prostredníctvom počítačových sietí v krajinách EÚ v roku 2016, kde opäť dominuje Írsko s 30 % podnikov s elektronickým obchodom.

Graf 5: Množstvo podnikov s predajom cez elektronický obchod v roku 2016

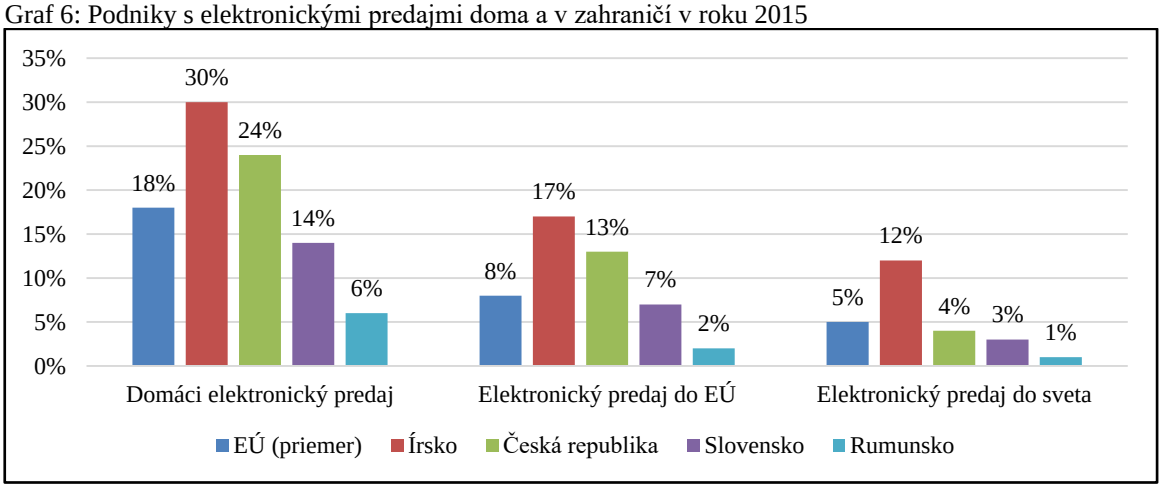


Zdroj: EUROSTAT. 2017 (a). *Digital single market - promoting e-commerce for businesses.* [online]. 2017 [cit. 2017-03-10]. Dostupné na internete: <http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bdek_sme&lang=en>.

Ďalšími krajinami s najviac rozvinutým elektronickým podnikaním v EÚ sú Dánsko (28 %), Česká republika (27 %) a Švédsko (27 %). Slovensko zdieľa 20. pozíciu spolu s Maďarskom s uvedenými 12 %. Na posledných miestach sú Rumunsko (7 %) a Bulharsko (5 %). Prekvapením je najnovšia členská krajina, Chorvátsko, v ktorej realizuje elektronický predaj 19 % podnikov.

Porovnanie vybraných krajín z pohľadu podnikov, ktoré využívajú domáci a zahraničný elektronický predaj v roku 2015, je zobrazené v grafe 6. Do prehľadu je okrem Slovenska zahrnuté Írsko ako dominantný reprezentant skupiny, Rumunsko ako krajina s najnižšími hodnotami, ČR a priemer EÚ. V SR uskutočňuje domáce elektronické obchodovanie 14 % podnikov, v susednej ČR až 24 % podnikov. V Írsku je elektronický predaj využívaný až 30 % podnikov. Slovenské elektronické podnikanie nie je orientované na zahraničný trh, čo dokazuje len 7 % podnikov s predajom do EÚ a 3 % do sveta. Krajinou, ktorá najviac obchoduje so zahraničím s využitím internetu je Írsko, 17 % podnikov predáva produkty do EÚ a 12 % do sveta. SR zaostáva za priemerom EÚ vo všetkých ukazovateľoch.

Graf 6: Podniky s elektronickými predajmi doma a v zahraničí v roku 2015



Zdroj: EUROSTAT. 2017 (b). *E-commerce sales.* [online]. 2017 [cit. 2017-03-09]. Dostupné na internete: <http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ec_eseln2&lang=en>.

Podľa uvedených údajov môžeme usúdiť, že Slovenské podniky zaostávajú za ekonomicky vyspelejšími krajinami EÚ a sveta v oblasti elektronického podnikania. V roku 2013 využívalo predaj na elektronickom trhu v SR najviac podnikov, odvtedy je zaznamenaný pokles. Globálny a európsky trend ukazuje, že sa situácia zlepší a zákazníci budú viac využívať služby elektronických obchodov, čo pravdepodobne ovplyvní aj SR. Výzvou podnikov na Slovensku je, aby zaviedli elektronické obchody a zvýšili elektronické predaje s orientáciou do zahraničia, pretože potenciál elektronického podnikania v zahraničí je veľký, najmä v krajinách, kde elektronický spôsob predaja ešte nie je rozvinutý a absentuje konkurencia.

1.3.2 Informačná bezpečnosť v elektronickom podnikaní

Informačno–komunikačné technológie okrem výhod pre podniky na elektronickom trhu (napr. rozšírenie trhu, nárast množstva objednávok, vyššie tržby, väčšia dostupnosť informácií, účinný marketing, nižšie náklady, ceny a i.) prinášajú mnohé riziká[107], ktoré ohrozujú na jednej strane podniky a poskytovateľov služieb a na druhej strane koncových používateľov. Z pohľadu podnikov sú riziká nasmerované na zraniteľnosti informačných aktív. Pri používateľoch je potrebné chrániť osobné údaje a iné utajované informácie, napríklad prístupové heslá a uložené údaje platobných kariet. Informačná bezpečnosť elektronického podnikania predstavuje ochranu informačných aktív podnikov pôsobiacich na elektronickom trhu pred neoprávneným použitím, zmenou, zničením a prístupom týchto aktív.[108] Podľa normy ISO/IEC 27005 s ohľadom na elektronické podnikanie rozdeľujeme informačné aktíva na primárne (informácie, obchodné procesy, činnosti, reputácia, osobné údaje, znalosti, kontakty, zdrojové kódy, atď.), ktoré sú ťažko nahraditeľné až nenahraditeľné, a podporné (dáta, hardvér, softvér, sieť, personál a lokalita), ktoré možno do istej miery nahradiť.[109]

Najvyšší stupeň ochrany informačných aktív podnikov dosahujeme vybudovaním bezpečného prostredia, ktoré obsahuje štyri úrovne podľa obrázka 11.

Obr. 11: Bezpečné prostredie elektronického podnikania
Zdroj: LAUDON, K. C., – TRAVER, C. G. 2014. *E-commerce: business, technology, society*. 10th ed. New Jersey: Pearson, 2014. s. 252. ISBN 978-0-13-302444-9.

Prvou úrovňou ochrany aktív sú technologické riešenia v podobe špecializovaného hardvéru, softvéru a zabezpečovacích zariadení. Politiky a procedúry podniku sú ďalšou úrovňou ochrany aktív. Do tejto oblasti patria všetky organizačné opatrenia vrátane

[107] REVATHI, C. – SHANTHI, K. – SARANYA, A. R. 2015. A Study on E-Commerce Security Issues. In *International Journal of Innovative Research in Computer and Communication Engineering*. ISSN 2320-9798, 2015, vol. 3, no. 12, p. 12896.
[108] NIRANJARAMURTHY, M. – DHARMENDRA, CH. 2013. The study of E-Commerce Security Issues and Solutions. In *International Journal of Advanced Research in Computer and Communication Engineering* [online]. 2013, vol. 2, no. 3 [cit. 2017-3-27]. Dostupné na internete: <http://www.ijarcce.com/upload/2013/july/69-o-Niranjanamurthy%20-The%20study%20of%20E-Commerce%20Security%20Issues%20and%20Solutions.pdf>. ISSN 2278-1021.
[109] STN ISO/IEC 27005: 2012: *Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti.*

bezpečnostných politík, plánov, prehlásení, SLA, školení, postupov, atď. Zákony a štandardy dopĺňajú strategickú úroveň bezpečného prostredia elektronického podnikania. Súlad s príslušnými zákonmi, normami a osvedčenými postupmi svedčí o informačnej bezpečnosti na primeranej úrovni nie len pre samotný podnik, ale aj pre interné alebo externé zainteresované strany (personál, dodávatelia, zákazníci, dotknuté organizácie, štátne orgány, inštitúcie, atď.).

Dosiahnuť bezpečné prostredie si vyžaduje veľa úsilia a dodatočných zdrojov podniku. Považujeme to za nevyhnutnosť, pretože akonáhle koncový používateľ (zákazník) prestane elektronickému obchodu plne dôverovať, prípadne má akúkoľvek pochybnosť o bezpečnosti obchodu či osobných údajov, v danom obchode peňažnú transakciu nezrealizuje. Zákazník je na informačnú bezpečnosť elektronického obchodu citlivý. Podľa Laudona a Travera, bezpečný elektronický obchod musí spĺňať nasledujúcich šesť dimenzií, ktorých súlad je zárukou primeranej informačnej bezpečnosti:[110]

- *Integrita* – schopnosť zaistiť, že zobrazovaná informácia na webovej stránke alebo prenášaná a prijímaná cez internet nebola pozmenená neautorizovanou stranou (napr. presmerovanie bankového prevodu na iný účet),
- *Nepopierateľnosť* – schopnosť zabezpečiť, že účastníci elektronického obchodu nemôžu odvolať (poprieť) svoje online činnosti (napr. dostupnosť e–mailového účtu zdarma s prezývkou umožňuje osobe komentovať, odosielať správy a neskôr tieto činnosti poprieť),
- *Autentickosť* – schopnosť identifikovať identitu fyzickej alebo právnickej osoby cez internet (napríklad aj schopnosť identifikácie pravosti podniku osobou),
- *Dôvernosť* – schopnosť zaistiť, že dáta a správy sa dostanú len k autorizovaným osobám na ich prehliadanie (napr. obnova zabudnutých prihlasovacích údajov),
- *Súkromie* – schopnosť riadiť využitie osobných údajov poskytnutých obchodníkovi (napr. možnosť dodatočného zmazania nepotrebných údajov po registrácii),
- *Dostupnosť* – schopnosť zabezpečiť prevádzku elektronického obchodu podľa zámerov podniku (napr. len pár minút výpadku globálneho elektronického obchodu môže spôsobiť závažný ušlý zisk).

Podľa Muthaiyaha a kol., špecialisti na tvorbu elektronických obchodov musia popri návrhu jednoduchosti ovládania a rozhrania zakomponovať riešenia znižujúce obavy

[110] LAUDON, K. C., – TRAVER, C. G. 2014. *E-commerce: business, technology, society*. 10th ed. New Jersey: Pearson, 2014. s. 253. ISBN 978-0-13-302444-9.

zákazníkov o bezpečnosť a súkromie[111], ktoré sú v konečnom dôsledku zakorenené v dôvere.[112] Práve dôvera zákazníkov je jedným z hlavných faktorov, ktoré brzdia vývoj elektronických obchodov[113] a rozhodnutie o nákupe.[114] Dosiahnutím uvedených šiestich dimenzií sa podnik stáva zabezpečeným z pohľadu všetkých zainteresovaných strán, čo zvyšuje dôveryhodnosť elektronického obchodu.

Prístup k informačnej bezpečnosti v elektronickom podnikaní je rozdielny podľa jednotlivých kategórií veľkosti podniku. Z pohľadu riadenia a presadzovania IB tvoria mikropodniky a MSP špecifické prostredie oproti veľkým podnikom. Čím je podnik menší, tým sú medzi nimi väčšie rozdiely, ktoré sa dotýkajú nasledujúcich oblastí:[115]

- MSP a mikropodniky majú minimálny alebo žiadny bezpečnostný tím,
- Manažment informačnej bezpečnosti je vykonávaný IT útvarom,
- Rozpočet na bezpečnosť je buď časťou rozpočtu na IT alebo neexistuje,
- MSP a mikropodniky disponujú nižším rozsahom finančných, časových a ľudských zdrojov pridelených na informačnú bezpečnosť,
- MSP a mikropodniky spravidla využívajú open–source projekty pre minimalizáciu výdavkov.

Na rozdiel od mikropodnikov a MSP, veľké podniky môžu jednoduchšie vyčleniť zdroje na vytvorenie samostatného útvaru IT bezpečnosti aj z dôvodu rizika väčších následkov bezpečnostných incidentov. Ďalej sú zaujímavé pre profesionálne konzultačné spoločnosti v oblasti ISMS, s ktorými ľahšie nadväzujú spoluprácu, sú si viac vedomé právnych požiadaviek v oblasti ochrany dôverných informácií[116] a môžu sa zamerať na sofistikovanejšie bezpečnostné riešenia, ktoré však vyžadujú väčší rozpočet oproti MSP a mikropodnikom. Veľké podniky, ktoré sú aktívne v oblasti elektronického podnikania, realizujú viac procesov, majú väčšiu IT infraštruktúru a ich organizačná štruktúra je

[111] MUTHAIYAH, S. – ERNEST, J. A. J. – WAI, C. K. 2004. Review Of E-commerce Issues: Consumes' Perception On Security And Privacy. In *International Business & Economics Research Journal*. ISSN 1535-0754, 2004, vol. 3, no. 9, p. 77.
[112] MANDIĆ, M. 2009. Privacy and security in e-commerce. In *Market-Tržište.* ISSN 0353-4790, 2009, vol. 21, no. 2, p. 255.
[113] WU, X. F. – ZHOU, J. – YUAN, X. 2012. The Research of Factors which Effect B2C E-commerce Trust – Based on the Mechanism of Process. In *Advanced Materials Research*. ISSN 1662-8985, 2012, vols. 591-593, p. 2583.
[114] AL RAWABDEH, W. – ZEGLAT, D. – ALZAWAHREH, A. 2012. The Importance of Trust and Security Issues in E-Commerce Adoption in the Arab World. In *European Journal of Economics, Finance and Administrative Sciences*. ISSN 1450-2275, 2012, vol. 52, p. 176.
[115] DEKÝŠ, P. 2010. *Správa informačnej bezpečnosti v malej a stredne veľkej spoločnosti.* [online]. 2010 [cit. 2015-12-10]. Dostupné na internete: <http://www.eset.com/sk/firmy/services/clanky/sprava-informacnej-bezpecnosti/>.
[116] SHREDIT. 2017. *Security Tracker – Australia.* [online]. 2017 [cit. 2017-03-06]. Dostupné na internete: <https://www.shredit.com.au/getmedia/a4a2f8e5-6f4c-4368-bffe-4e1e557267cd/Shred-it_Security_Tracker_AUS.aspx?ext=.pdf>.

rozsiahlejšia ako pri MSP, preto potrebujú zabezpečiť omnoho viac informačných aktív oproti MSP a mikropodnikom.

1.3.3 Bezpečnostné hrozby a opatrenia

V typickom systéme elektronického obchodu, kde zákazník navštívi webové stránky, prehliada katalóg produktov a uskutočňuje nákup, existujú štyria hlavní účastníci. Prvým je zákazník, ktorý prostredníctvom internetového prehliadača vyhľadá konkrétne webové sídlo. Sídlo je zvyčajne prevádzkované obchodníkom, ktorého cieľom je predaj tovaru alebo služby so ziskom. Keďže obchodník sa nešpecializuje na vývoj softvéru, nakúpi ho od poskytovateľa. Útočník je jediný nelegitímny účastník, ktorému zneužitie ostatných prináša výhody.[117] S využitím najrôznejších metód a techník útočník napáda zákazníka, obchodníka, komunikáciu, webový server, sieťové prvky a ostatnú IT infraštruktúru poskytovateľa.

Z iného pohľadu, existujú tri zraniteľné body elektronického obchodu, kde smerujú bezpečnostné hrozby (klient, server a vzájomná komunikácia). Laudon a Traver považujú za najbežnejšie a zároveň najškodlivejšie hrozby v prostredí podnikov s elektronickým obchodom malvér a potenciálne nechcené programy, ďalej phishing, neoprávnené vniknutie do systému, spam, krádež identity, útoky DoS a DDoS, slabo zabezpečený server a klientsky softvér, problémy bezpečnosti sociálnych sietí, mobilných zariadení a cloudu.[118] K zoznamu dopĺňame iné metódy sociálneho inžinierstva (napr. pharming), vzdialené špehovanie počítača zákazníka, odpočúvanie (napr. Man–in–the–middle útok), útoky na heslá (hádanie, resetovanie, zachytávanie, dúhové tabuľky, atď.), slabá autentifikácia, chybná bezpečnostná konfigurácia sieťových zariadení, serverov, klientov a protokolov, zneužitie zraniteľností webových aplikácií, predovšetkým validácie vstupov (napr. pretečenie vyrovnávacej pamäte, Cross–site scripting, SQL injection), a mnohé iné.[119] [120]

Norma ISO/IEC 27005 klasifikuje hrozby podľa typu a pôvodu. Prispôsobením na prostredie elektronického podnikania rozdeľujeme hrozby do kategórií fyzické poškodenie, strata základných služieb, únik informácií, technické zlyhanie, neautorizované činnosti,

[117] LOKHANDE, P. S. – MESHRAM, B. B. 2013. E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures. In *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*. ISSN 2278-1323, 2013, vol. 2, no. 2, p. 500.
[118] LAUDON, K. C., – TRAVER, C. G. 2014. *E-commerce: business, technology, society*. 10th ed. New Jersey: Pearson, 2014. s. 256. ISBN 978-0-13-302444-9.
[119] LOKHANDE, P. S. – MESHRAM, B. B. 2013. E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures. In *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*. ISSN 2278 – 1323, 2013, vol. 2, no. 2, p. 501 – 506.
[120] PCI SSC. 2013. *Information Supplement: PCI DSS E-commerce Guidelines*. [online]. 2013 [cit. 2017-03-28]. Dostupné na internete: <https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf>.

poškodenie funkcií, počítačová kriminalita, priemyselná špionáž a interné hrozby.[121] Tohto členenia sa pridržiavame v rámci spracovania ďalších častí dizertačnej práce.

V boji proti hrozbám namiereným na elektronické podnikanie možno využiť množstvo bezpečnostných opatrení, techník a osvedčených postupov. Opatrenia najčastejšie rozdeľujeme na organizačné (politiky, plány, metodiky, školenia, pravidlá, procesy a i.) a technické (systémy, zariadenia, techniky, špecializovaný softvér, hardvér, atď.). Organizácie a profesionáli v oblasti informačnej bezpečnosti odporúčajú podnikom široké spektrum technických alebo organizačných bezpečnostných opatrení na dosiahnutie primeranej bezpečnosti elektronického obchodu.

Organizácia PCI SSC definuje nasledujúce pravidlá, ktoré musia podniky s elektronickým obchodom dodržiavať, aby získali adekvátnu úroveň bezpečnosti:[122]

- Poznať umiestnenie všetkých dát držiteľov platobných kariet,
- Neukladať dáta držiteľov platobných kariet, ak nie sú potrebné,
- Posúdiť riziká spojené s vybranou technológiou elektronického obchodu,
- Spoznať, do ktorých systémov podniku vzdialene pristupuje poskytovateľ služieb,
- Uskutočňovať externé kontroly zraniteľností a penetračné testovanie,
- Implementovať bezpečnostné školenia personálu,
- Dodržiavať zásady bezpečného elektronického obchodu (využívať protokol TLS, aplikačný firewall WAF, konfigurovať pravidlá firewallu, pravidelne kontrolovať odkazy na platobné brány, využívať a aktualizovať antivírusový softvér, implementovať IDS/IPS, spravovať logy, segmentovať sieť, atď.),
- Dbať o zvyšovanie bezpečnostného povedomia zákazníkov (napr. nenakupovať cez nezabezpečené Wi–Fi siete, kontrolovať komunikáciu cez TLS protokol, vytvárať bezpečné heslá, chrániť dôvernosť prihlasovacích údajov na verejnosti a i.).

Úspech elektronického podnikania okrem jedinečnosti produktu, adekvátnej ceny, vhodného systému, správnej cieľovej skupiny a marketingových aktivít vo veľkej miere závisí od schopnosti čeliť hrozbám implementovaním primeraných bezpečnostných opatrení. Úroveň informačnej bezpečnosti a ochrana informačných aktív podniku je zásadná pre internetového zákazníka, ktorý je ochotný poskytnúť elektronickému obchodu osobné údaje a následne nakupovať produkty a služby.

[121] STN ISO/IEC 27005: 2012: *Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti.*
[122] PCI SSC. 2017. *Information Supplement: Best Practices for Securing E-commerce*. [online]. 2017 [cit. 2017-03-28]. Dostupné na internete: <https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf>.

1.3.4 Zhrnutie východísk elektronického podnikania

Využitie internetu sa každým rokom rapídne zväčšuje, dostupnosť lacných mobilných zariadení a rozširovanie internetu sa stali kľúčovými faktormi.[123] Elektronické podnikanie narastá priamo úmerne s rozširovaním internetu. Všade tam, kde je dostupný internet, vznikajú nové elektronické trhy. Elektronické podnikanie je na vzostupe, čo z pohľadu Európskej únie dosvedčuje štatistický úrad Eurostat a tiež krajiny ako Čína a USA, ktoré každý rok znásobujú dosiahnuté tržby z elektronického predaja tovarov a služieb. Slovensko potvrdzuje vzostupný trend, v priebehu najbližších rokov s najväčšou pravdepodobnosťou dosiahne celkový obrat 1 miliardu € z elektronického predaja tovaru a služieb. Každoročný nárast počtu elektronických obchodov a postupná informatizácia spoločnosti (napr. e–government, e–health) naznačujú, že rozvoj elektronického podnikania v SR bude pokračovať.

Avšak, rozvoj nebude možný, pokiaľ podniky nebudú dodržiavať základné dimenzie IB, čiže nevytvoria bezpečné prostredie pre svoje informačné aktíva. Hlavným dôvodom možného úpadku je zákazník, pretože je citlivý na bezpečnostné incidenty smerujúce na elektronické obchody. Každé neošetrené a realizované riziko (napr. únik prihlasovacích údajov), vedie k okamžitej strate množstva zákazníkov a takto až k existenčným problémom. V dobe veľkého množstva bezpečnostných hrozieb, útočných metód a techník si podniky nemôžu dovoliť IB ignorovať. Tvrdíme, že správnou cestou pre podniky je aplikovať procesný prístup k ISMS, ktorý zaručí primeranú informačnú bezpečnosť elektronického podnikania minimalizáciou následkov rizík náležitými bezpečnostnými opatreniami za akceptovateľné náklady.

ISMS elektronického podnikania je dôležitým procesom, ktorý určuje zdravie a trvalo udržateľný rozvoj podniku.[124] Narastajúca počítačová a kybernetická kriminalita a jej zjednodušovanie a sprístupňovanie pre neodborných používateľov IKT síce aktívne napáda informačné aktíva podnikov s elektronickým obchodom, ale z iného pohľadu ich núti aplikovať proaktívne alebo reaktívne technické a organizačné opatrenia, ktoré v konečnom dôsledku vedú k implementácii ISMS.

[123] YAZDANIFARD, R. – EDRES, N. A. H. – SEYEDI, A. P. 2011. In *International Proceedings of Computer Science and Information Technology*. [online]. 2011, vol. 16 [cit. 2017-03-28]. Dostupné na internete: <http://www.ipcsit.com/vol16/5-ICICM2011M008.pdf>. ISSN 2010-460X.

[124] JI, H. – ZOU, S. 2016. Electronic Commerce in China Information Security Management System Strategy Research. In *2nd International Conference on Humanities and Social Research (ICHSSR 2016)*. [online]. 2016 [cit. 2017-03-28]. Dostupné na internete: <http://www.atlantis-press.com/php/download_paper.php?id=25861735>. ISBN 978-94-6252-235-0.

2 Cieľ práce

Podniky obchodujúce na elektronickom trhu sú z dôvodu aktívneho využívania IKT vo viacerých činnostiach transformačného procesu vystavené rizikám informačnej bezpečnosti. Realizácia rizík obzvlášť spôsobuje škody v podnikoch, ktorým chýba ISMS, prípadne aspoň základný procesný prístup k manažmentu IB. Touto negatívnou vlastnosťou sa vyznačujú podniky, ktoré nedisponujú dostatočnými zdrojmi na zabezpečenie dôverných informácií. Ide predovšetkým o zdroje ľudské, ale aj o finančné a materiálne. Vysoké náklady a zložitosť zavedenia moderných nástrojov, techník, metód, prípadne odporúčaní plynúcich zo štandardov a legislatívy, nútia podniky vnímať IB len povrchne. V dôsledku minimalizácie nákladov je potrebné využívať open–source projekty[125]. Avšak, význam podnikateľských činností na elektronickom trhu núti podniky ku zvýšenej ochrane a opatrnosti zaobchádzania s informáciami. Z analýzy súčasného stavu vyplývajú nasledujúce predpoklady, ktoré použijeme pre stanovenie hlavného cieľa, čiastkových cieľov a formuláciu hypotéz:

- *Predpoklad A*: Podnikom, ktoré obchodujú na slovenskom elektronickom trhu, chýba ucelený systém riadenia informačnej bezpečnosti,[126] [127]
- *Predpoklad B*: Podniky s elektronickým obchodom nedisponujú dostatkom finančných zdrojov na primerané zabezpečenie informačných aktív, [128] [129] [130]
- *Predpoklad C*: Hrozby smerujúce na zraniteľnosti personálu sú významnou príčinou rizík informačnej bezpečnosti,[131] [132] [133] [134]

[125] DEKÝŠ, P. 2010. *Správa informačnej bezpečnosti v malej a stredne veľkej spoločnosti.* [online]. 2010 [cit. 2015-12-05]. Dostupné na internete: <http://www.eset.com/sk/firmy/services/clanky/sprava-informacnej-bezpecnosti/>.
[126] NETOLICKÁ, B. 2012 (b). *5 zásad pre riadenie a presadzovanie informačnej bezpečnosti v organizácii.* [online]. 2012 [cit. 2015-12-05]. Dostupné na internete: <http://www.eset.com/sk/firmy/services/clanky/5-zasad-informacnej-bezpecnosti/>.
[127] KRÁL, D. 2011. Information Security in Small and Medium-Sized Companies. In *ACTA VŠFS*. ISSN 1802-792X, 2011, roč. 5, č. 1, s. 61.
[128] ČERNÝ, M. 2014. *Prístup k informačnej bezpečnosti v malých a stredných podnikoch* [online]. 2014 [cit. 2015-12-05]. Dostupné na internete: <http://www.itnews.sk/2014-06-24/c163829-pristup-k-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch>.
[129] SINGH, A. N. et al. 2013. Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. In *Global Journal of Flexible Systems Management*. ISSN 0972-2696, 2013, vol. 14, no. 4, p. 225.
[130] STEHLÍKOVÁ, B. – HOROVČÁK, P. 2012. Manažment informačnej bezpečnosti v malých a stredných podnikoch. In *Security Revue* [online]. 2012 [cit. 2015-12-01]. Dostupné na internete: <http://www.securityrevue.com/article/2012/06/manazment-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch/>.
[131] PWC. 2015. *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016.* [online]. 2015 [cit. 2015-12-03]. Dostupné na internete: <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html>.
[132] EY. 2015. *Creating trust in the digital world: EY´s Global Information Security Survey 2015.* [online]. 2015 [cit. 2015-12-03]. Dostupné na internete: <http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf>.
[133] NETOLICKÁ, B. 2012 (a). *Sociálne inžinierstvo v kontexte informačnej bezpečnosti v organizácii.* [online]. 2012 [cit. 2015-12-03]. Dostupné na internete: <http://www.eset.com/sk/firmy/services/clanky/socialne-inzinierstvo-ib/>.
[134] ČERNÝ, M. – ROMANOVÁ, A. 2012. Interní zamestnanci ako hrozba bezpečnosti dát. In *Ekonomika a manažment podniku: vedecký časopis pre ekonomiku, riadenie a manažment slovenských podnikov*. ISSN 1336-4130, 2012, roč.10, č. 1-2, s. 7.

- *Predpoklad D*: Dáta z podnikového informačného systému sú pre podniky najvýznamnejším informačným aktívom. Strata dôverných dát vedie k závažným finančným stratám a k strate konkurencieschopnosti.[135] [136] [137]

2.1 Hlavný cieľ a čiastkové ciele

Hlavným cieľom dizertačnej práce je navrhnúť model manažmentu informačnej bezpečnosti elektronického podnikania so zameraním na podniky, ktoré pri obchodovaní využívajú elektronický trh. Implementovaním výsledného modelu podniky zvýšia zabezpečenie svojich informačných aktív pred existujúcimi hrozbami informačnej bezpečnosti. Kvalitatívny model pozostáva z procesov, ktoré chránia zraniteľné miesta v oblasti zabezpečenia informačných aktív a aplikujú primeranú informačnú bezpečnosť. Hlavný cieľ vychádza z komparácie poznatkov súčasného stavu problematiky a prináša chýbajúce riešenie pre skúmanú oblasť teórie a podnikovej praxe. Hlavný cieľ je podporený nasledujúcimi čiastkovými cieľmi, ktoré vedú k jeho dosiahnutiu:

- Analyzovať, porovnať a vytvoriť syntézu teoretických východísk manažmentu informačnej bezpečnosti so zameraním na elektronické podnikanie v domácom a zahraničnom prostredí,
- Analyzovať a porovnať vybrané modely manažmentu informačnej bezpečnosti,
- Identifikovať a vyhodnotiť súčasný stav úrovne manažmentu informačnej bezpečnosti podnikov s elektronickým obchodom na základe dostupných poznatkov, výskumných štúdií a vlastného prieskumu,
- Preskúmať vplyv nákladov vynaložených na informačnú bezpečnosť na podnikmi vnímanú úroveň informačnej bezpečnosti,
- Vyhodnotiť význam informačných aktív podnikov obchodujúcich na slovenskom elektronickom trhu,
- Preskúmať a vyhodnotiť pravdepodobnosti výskytu hrozieb informačnej bezpečnosti v podnikoch s elektronickým obchodom,
- Preskúmať a vyhodnotiť pravdepodobnosti výskytu hrozieb informačnej bezpečnosti smerujúcich na zraniteľnosti personálu,

[135] KASPERSKY. 2015. *Damage control: The cost of security breaches, IT security risks special report series* [online]. 2015. [cit. 2014-10-17]. Dostupné na internete: <http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf>.
[136] KOKLES, M. – KORČEK, F. 2015. Analýza rizík informačnej bezpečnosti v malých a stredných podnikoch. In *Ekonomika a manažment: Vedecký časopis Fakulty podnikového manažmentu Ekonomickej univerzity v Bratislave.* ISSN 1336-3301, 2015, roč. 12, č. 1, s. 50-52.
[137] ENTRUST. 2004. *Protecting Your Most Important Asset: Information – How Data Security Mitigates Risk and Enables Compliance.* [online]. 2004 [cit. 2015-12-03]. Dostupné na internete: <https://www.entrust.com/wp-content/uploads/2013/05/secure_data_wp.pdf>.

- Analyzovať, stanoviť miery a priorizovať riziká informačnej bezpečnosti,
- Preskúmať existujúce bezpečnostné opatrenia skúmaných podnikov a vybrať primerané opatrenia na zníženie rizík informačnej bezpečnosti.

Po úspešnom splnení čiastkových cieľov nasleduje návrh kvalitatívneho modelu manažmentu informačnej bezpečnosti elektronického podnikania, ktorým dosiahneme hlavný cieľ dizertačnej práce.

2.2 Formulácia výskumných hypotéz

Na účely komparácie a zosúladenia poznatkov výskumu s aktuálnym stavom vedeckého bádania v skúmanej problematike sú v nasledujúcej tabuľke sformulované výskumné hypotézy, ktoré testujeme a verifikujeme viacerými vedeckými metódami vo výsledkoch dizertačnej práce.

Tab. 10: Formulácia výskumných hypotéz

	Hypotéza	Odôvodnenie
1	**H_0:** Medzi nákladmi vynaloženými na informačnú bezpečnosť a úrovňou informačnej bezpečnosti stanovenou podnikmi neexistuje štatisticky významná stredne silná závislosť ($r > 0,3$) meraná korelačným koeficientom. **H_1:** Medzi nákladmi vynaloženými na informačnú bezpečnosť a úrovňou informačnej bezpečnosti stanovenou podnikmi existuje štatisticky významná stredne silná závislosť ($r > 0,3$) meraná korelačným koeficientom.	Hypotéza 1 vychádza zo štúdie Černého, Singha a kol., Stehlíkovej a Horovčáka. Predpokladáme, že množstvo vynaložených finančných prostriedkov na informačnú bezpečnosť súvisí s úrovňou informačnej bezpečnosti v podniku. Ak podnik vynaloží viac, má vyššiu úroveň a tým aj nižšiu mieru realizovaných rizík. Z iného pohľadu, pri vyššej úrovni predpokladáme vyššie náklady podniku na informačnú bezpečnosť. Štatistickú závislosť overujeme korelačnou analýzou.
2	**H_0:** Podniky, ktoré disponujú vyšším (1 smerodajná odchýlka nad priemerom) objemom finančných prostriedkov na informačnú bezpečnosť, sa štatisticky významne neodlišujú v riadení rizík informačnej bezpečnosti od tých, ktoré disponujú nižším (1 smerodajná odchýlka pod priemerom) objemom finančných prostriedkov na informačnú bezpečnosť. **H_1:** Podniky, ktoré disponujú vyšším (1 smerodajná odchýlka nad priemerom) objemom finančných prostriedkov na informačnú bezpečnosť, sa štatisticky významne odlišujú v riadení rizík informačnej bezpečnosti od tých, ktoré disponujú nižším (1 smerodajná odchýlka pod priemerom) objemom finančných prostriedkov na informačnú bezpečnosť.	Hypotéza 2 skúma, či existujú štatisticky významné rozdiely medzi podnikmi, ktoré majú viac vyčlenených finančných prostriedkov, a podnikmi, ktoré majú menej vyčlenených finančných prostriedkov na informačnú bezpečnosť. Predpokladáme, že podniky s vyšším rozpočtom na informačnú bezpečnosť viac zavádzajú a využívajú organizačné opatrenie riadenie rizík informačnej bezpečnosti. Na druhej strane, tie podniky, ktoré nevyčleňujú financie na ochranu informácií, zároveň ani neriadia riziká informačnej bezpečnosti. Hypotéza je podložená výsledkami výskumu PwC, Singha, Černého a iných. Hypotézu testujeme buď T–testom alebo Mann–Whitneyho U testom podľa rozdelenia dát.
3	**H_0:** Úroveň informačnej bezpečnosti vnímaná podnikmi s elektronickým obchodom nie je štatisticky signifikantným prediktorom významu dát z podnikového informačného systému. **H_1:** Úroveň informačnej bezpečnosti vnímaná podnikmi s elektronickým obchodom je štatisticky signifikantným prediktorom významu dát z podnikového informačného systému.	Hypotéza 3 je postavená na výsledkoch výskumu spoločností Kaspersky Lab a Entrust, že dáta uskladnené v informačnom systéme sú najvýznamnejším informačným aktívom. Predpokladáme, že úroveň informačnej bezpečnosti podnikov ovplyvňuje ich hodnotenie dát z informačného systému. Štatisticky významnú závislosť meriame regresnou analýzou.

Zdroj: vlastné spracovanie

3 Metodika práce a metódy skúmania

Spracovanie dizertačnej práce vychádza zo stanovených cieľov, ktoré dosahujeme zvolenými metódami vedeckej práce. Charakterizovanie objektu skúmania, určenie vhodnej metodiky, pracovného postupu a spôsobu získavania údajov napomáha pri nadobúdaní požadovaných výstupov v rámci dvoch podstatných častí, zhodnotenie súčasného stavu poznania manažmentu informačnej bezpečnosti, elektronického podnikania a vytvorenie vlastných návrhov riešenia skúmanej problematiky.

3.1 Charakteristika objektu skúmania

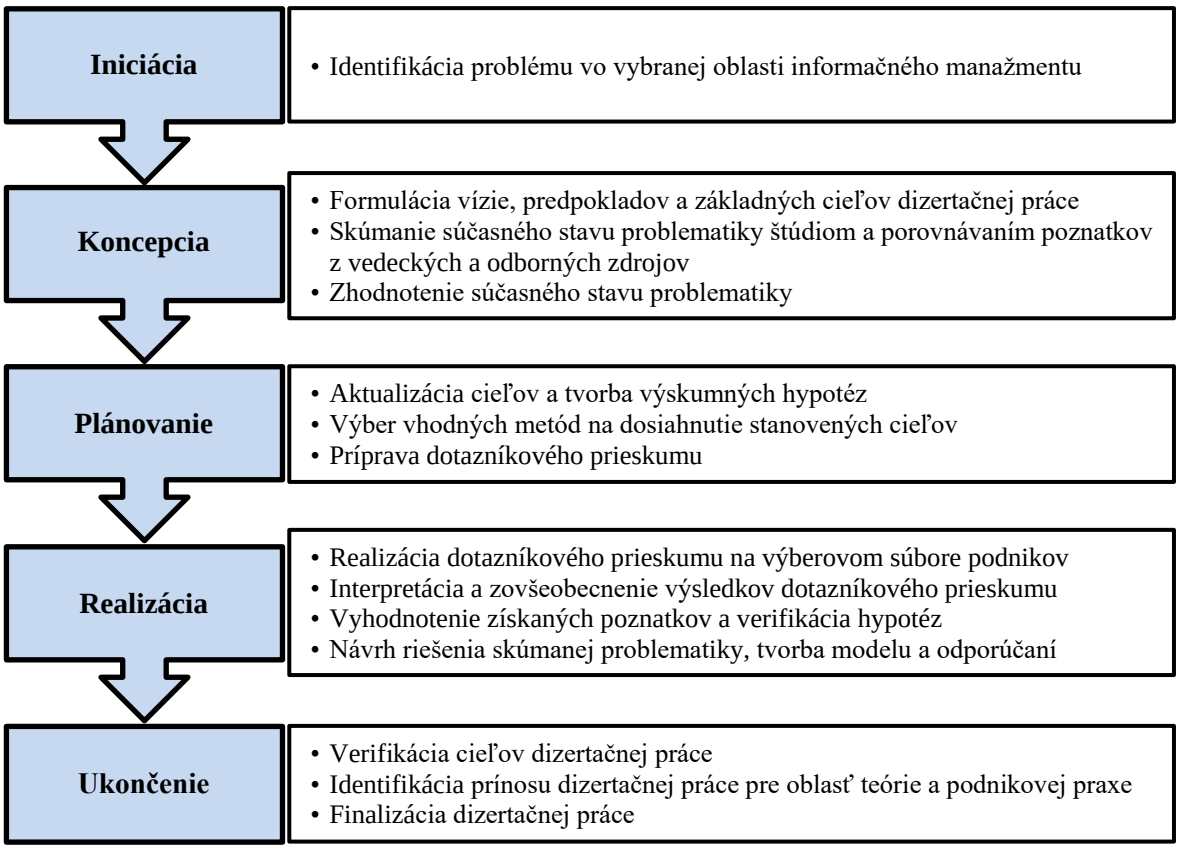
Objektom skúmania dizertačnej práce sú podniky obchodujúce na slovenskom elektronickom trhu. Hlavnou podmienkou zaradenia konkrétneho podniku do výskumu je, aby realizoval predaj tovaru alebo služieb prostredníctvom aplikácie elektronického obchodu a pri riešení dodávateľsko–odberateľských vzťahov využíval informačno–komunikačné technológie. Ďalšími charakteristikami sú:

- Predaj tovaru alebo služieb na území SR,
- Nezáleží na druhu ponúkaného tovaru alebo služby,
- Nezáleží na mieste sídla podniku,
- Nezáleží na veľkosti podniku,
- Nezáleží na veku podniku,
- Nezáleží na právnej forme podniku.

Zaradenie podnikov s uvedenými charakteristikami do výskumu je predpokladom na všeobecnú aplikovateľnosť výsledného modelu v prostredí podnikov, ktoré podnikajú na elektronickom trhu. Výber objektu vychádza zo skúmania súčasného stavu manažmentu informačnej bezpečnosti v elektronickom podnikaní, zo stanovených predpokladov a cieľov dizertačnej práce.

3.2 Pracovné postupy

Postup pri spracovaní dizertačnej práce môžeme zhrnúť do piatich fáz, konkrétne iniciácia, koncepcia, plánovanie, realizácia a ukončenie. Fázy pozostávajú z viacerých činností, ktorých postupné vykonanie vedie k úspešnej finalizácii dizertačnej práce. Pracovný postup vyjadrený jednotlivými fázami spolu s uskutočnenými činnosťami je zobrazený na obrázku 12.



Obr. 12: Fázy spracovania dizertačnej práce
Zdroj: vlastné spracovanie

Výstupom úvodnej fázy, iniciácie, je výber témy inšpirovanej nedostatočným riešením IT bezpečnosti v oblasti elektronického podnikania. Fáza koncepcie formuluje víziu, predpoklady, základné ciele a pre získanie uceleného prehľadu rozširuje naše chápanie problematiky o nové poznatky z viacerých zdrojov. Tretia fáza je kompletným naplánovaním výskumných aktivít a spôsobov ich realizácie. Realizácia je fázou, v ktorej sú uskutočňované výskumné aktivity, vyhodnocované získané poznatky a navrhované riešenia problematiky. V poslednej, finalizačnej fáze verifikujeme stanovené ciele a určujeme významné prínosy dizertačnej práce pre teoretickú, pedagogickú a podnikovú oblasť.

3.3 Spôsob získavania údajov a ich zdroje

Prvá časť dizertačnej práce sa zameriava na preskúmanie poznatkov problematiky z vedeckých zdrojov, noriem, smerníc, predpisov a odporúčaní organizácií pôsobiacich v oblasti manažmentu informačnej bezpečnosti, informačnej bezpečnosti, informačného manažmentu a elektronického podnikania. Údaje a poznatky sú získané zo zahraničných a domácich literárnych zdrojov zaradených do citačných databáz (napr. Web of Science, Scopus), ďalej z vedeckých monografií, statí a štúdií, odborných časopisov, európskych

a slovenských štatistických databáz a aktuálnych prieskumov organizácií zaoberajúcich sa IB (ENISA, NIST, ISACA, CSIRT.SK, Ernst & Young, PwC, Kaspersky Lab, ESET a i.).

Druhá časť práce priamo nadväzuje na prvú časť a predkladá vlastné návrhy a prínosy riešenia identifikovanej problémovej oblasti informačného manažmentu. Získavanie údajov prebehlo formou štruktúrovaného dotazníkového prieskumu v skúmaných podnikoch, ktorý bol uskutočnený od októbra 2016 do januára 2017. Cieľovou skupinou na vyplnenie dotazníka sú osoby, ktoré v podnikoch zodpovedajú predovšetkým za manažment informačnej bezpečnosti, informačný manažment, správu podnikovej informatiky, prípadne správu počítačových sietí. Preferované pozície sú riaditelia podniku, IT manažéri, manažér informačnej bezpečnosti, manažér elektronického obchodu, systémový inžinier, správca IKT podniku, elektronického obchodu, počítačovej siete, a podobne. Uvedomujeme si, že čím je podnik menší, tým je menšia pravdepodobnosť vyplnenia dotazníka osobou z cieľovej skupiny. Dotazník je preto navrhnutý zrozumiteľne a štruktúrovaný logicky tak, aby bol jednoducho a kvalitne vyplniteľný aj menej zbehlými osobami v skúmanej problematike a pojmoch, napríklad riaditeľmi a zamestnancami mikropodnikov.

Tvorba otázok premenných v dotazníku je cielená na základné charakteristiky a na konkrétne problematické časti manažmentu informačnej bezpečnosti podľa stanovených cieľov práce. Dotazník je navrhnutý v prostredí webového nástroja surveygizmo.com, ktorého výstupom je prehľadný a jednoducho vyplniteľný elektronický formulár. Distribúciu prieskumu sme uskutočnili prostredníctvom elektronickej komunikácie, telefonicky alebo osobne. Spoľahlivosť dotazníka je overená analýzou reliability a spoľahlivosť výsledkov štatistického spracovania zozbieraných údajov reprezentatívnou vzorkou dát z výberového súboru. V rámci prieskumu sme oslovili vyše 1100 vyhovujúcich podnikov. Počet úspešne vyplnených dotazníkov je 91, čo považujeme za dostatočne reprezentatívnu vzorku nielen z hľadiska štatistickej analýzy, ale aj z dôvodu vysokej citlivosti získavaných informácií od respondentov. Exaktnosť dát zaručujeme výberom vhodných škál premenných. Dotazník je anonymný a prenos dát sme zabezpečili šifrovanou komunikáciou, čím sme zachovali dôvernosť poskytnutých informácií.

Premenné, ktoré vstupujú do modelu a štatistickej analýzy, sú stanovené na základe zhodnotenia súčasného stavu problematiky, odporúčaní normy ISO/IEC 27005 o metódach posúdenia rizika IB, normy ISO/IEC 27002 o pravidlách dobrej praxe ISMS a organizácií a odborníkov v oblasti ISMS. Premenné delíme do 5 skupín týkajúcich sa charakteristiky skúmaného objektu, systému riadenia IB, informačných aktív podniku, hrozieb IB a existujúcich opatrení. Prehľad premenných sa nachádza v tabuľke 11.

Tab. 11: Analyzované premenné

CH. Charakteristika podniku			
CH01	Právna forma	CH04	Počet zamestnancov
CH02	Ekonomická činnosť (SK NACE Rev.2)	CH05	Hlavní odberatelia e–commerce
CH03	Kraj sídla podniku		
SY. Systém riadenia informačnej bezpečnosti			
SY01	Nutnosť riešenia ISMS v rámci e–business	SY07	Dostatok finančných zdrojov na IB
SY02	Možnosť ochrany e–business bez ISMS	SY08	Pravidelnosť vyhodnocovania rizík IB
SY03	Možnosť ISMS zlepšiť výsledky e–business	SY09	Pravidelnosť aktualizácie politiky IB
SY04	Potreba ISMS v e–business respondenta	SY10	Spokojnosť s úrovňou IB podniku
SY05	Praktizovanie ISMS v podniku	SY11	Úroveň IB v podniku
SY06	Podiel nákladov na IB z celkových nákladov		
IA. Význam informačných aktív podniku			
IAPA Primárne aktíva			
IA01	Obchodné činnosti, procesy	IA05	Strategické a obchodné informácie
IA02	Obchodné tajomstvo, know–how	IA06	Osobné údaje
IA03	Dobré meno podniku, reputácia	IA07	Kľúčové kontakty, vzťahy a zmluvy
IA04	Znalosti zamestnancov	IA08	Zdrojové kódy
IADA Dáta			
IA09	Dáta z informačného systému podniku	IA11	Dáta z bezpečnost. systémov (záznamy, logy)
IA10	Dáta z elektronického obchodu	IA12	Zálohy, archívne dáta a dokumentácia
IAHA Hardvér			
IA13	Servery a disky serverov (HDD, SSD)	IA16	Hardvérové zariadenia (kopírka, tlačiareň)
IA14	Pracovné stanice (počítače, notebooky)	IA17	Záložné zdroje UPS
IA15	Mobilné zariadenia (smartfóny, tablety)		
IASO Softvér			
IA18	Operačný systém serveru	IA22	E–commerce (aplikácia, CMS, CRM)
IA19	Operačný systém počítača	IA23	Antivírusový softvér
IA20	Softvér na správu systémov (konfigurácia)	IA24	Kancelársky softvér (Microsoft Office a i.)
IA21	Informačný systém podniku (ERP)	IA25	Aplikácie mobilných zariadení
IASI Sieť			
IA26	Telekomunikačná sieť	IA28	Internetové pripojenie
IA27	Počítačová sieť (kabeláž, aktívne prvky)	IA29	Pripojenie k podnikovej počítačovej sieti
IAPE Personál			
IA30	Zamestnanci – používatelia informácií	IA32	Zamestnanci – prevádzka a údržba IKT
IA31	Zamestnanci – obsluha a vývoj e–commerce		
IALO Lokalita			
IA33	Okolie podniku (mestská oblasť a i.)	IA36	Zabezpečovací systém (EZS, EPS, CCTV a i.)
IA34	Areály a budovy podniku	IA37	Klimatizácia
IA35	Bezpečnostné zóny (serverovne, archív a i.)	IA38	Inžinierske siete (elektrika, plyn, voda a i.)
HR. Pravdepodobnosť výskytu hrozieb IB v podniku			
HRFP Fyzické poškodenie zariadení alebo médií			
HR01	Požiar	HR04	Klimatický a meteorologický jav
HR02	Poškodenie vodou, povodeň	HR05	Elektromagnetická radiácia a impulzy
HR03	Znečistenie, prach, korózia, mrznutie	HR06	Termálna radiácia
HRSZ Strata základných služieb			
HR07	Porucha klimatizácie alebo inžinierskych sietí	HR09	Porucha telekomunikačného zariadenia
HR08	Strata energetického napájania		
HRUI Únik informácií			
HR10	Vzdialené špehovanie, odpočúvanie	HR14	Prezradenie osobných údajov
HR11	Krádež zariadenia, médií, dokumentov	HR15	Údaje z nedôveryhodných zdrojov
HR12	Vyhľadávanie vyradených, recyklovaných médií	HR16	Manipulácia s hardvérom
HR13	Prezradenie dôverných dát, obchod. tajomstva	HR17	Manipulácia so zdrojovými kódmi
HRTZ Technické zlyhanie			
HR18	Zlyhanie alebo porucha zariadenia	HR20	Saturácia a porušenie udržiavateľnosti IS
HR19	Softvérová porucha		
HRNC Neautorizované činnosti			
HR21	Neautorizované použitie zariadenia a softvéru	HR24	Poškodenie dát

HR22	Nelegálne kopírovanie systému, softvéru	HR25	Falšovanie a nelegálne spracovanie dát
HR23	Použitie falošného, kopírovaného softvéru		
HRPF Poškodenie funkcií			
HR26	Chyba pri použití softvéru, systémové chyby	HR28	Prerušenie dostupnosti webových služieb
HR27	Odopretie činnosti softvéru	HR29	Prerušenie dostupnosti e–commerce
HRPK Počítačová kriminalita			
HR30	Sociálne inžinierstvo (phishing a i.)	HR34	Nelegálne konanie (zmena osob. údajov a i.)
HR31	Nežiadúci obsah (defacement, spam a i.)	HR35	Botnet
HR32	Neoprávnený prístup, vniknutie do IS	HR36	Útok na systém, nedostupnosť (DDoS a i.)
HR33	Počítačový zločin, terorizmus	HR37	Škodlivý kód
HRPS Priemyselná špionáž			
HR38	Krádež informácií a dát	HR41	Politické vydieranie
HR39	Zásah do súkromia	HR42	APT
HR40	Ekonomické vydieranie		
HRIH Interné hrozby			
HR43	Vydieranie bývalým zamestnancom	HR47	Podplácanie
HR44	Útok na zamestnanca	HR48	Predaj dôverných a osobných údajov
HR45	Prezeranie dôverných informácií	HR49	Sabotáž systému a zariadení
HR46	Podvod		
OP. Opatrenia IB v podniku			
OPOO Organizačné opatrenia			
OP01	Riadenie rizík IB	OP10	Preverovanie zamestnancov pred nástupom
OP02	Dokument politiky IB	OP11	Dohody o zachov. mlčanlivosti zamestnancov
OP03	Stanovenie rolí IB (špecialista, školiteľ a i.)	OP12	Detekcia, reakcia na bezpečnostné incidenty
OP04	Vloženie pravidiel IB do dodávateľ. zmlúv	OP13	Plán zálohovania dát
OP05	Riadenie dodávok služieb (SLA)	OP14	Riadenie a kontrola sieťových zariadení
OP06	Politika čistej obrazovky a čistého stola	OP15	Pravidlá pridelenia prístupových práv k aktívam
OP07	Systém tvorby a správy hesiel	OP16	Pravidlá používania mobilných zariadení
OP08	Plán rozvoja bezpečnostného povedomia	OP17	Postupy k zaisteniu kontinuity (kríza a i.)
OP09	Školenia zamestn. k IB (vstupné, pravidelné)		
OPTO Technické opatrenia			
OP18	Antivírusový softvér	OP37	Pravidelná aktualizácia IS, OS, softvérov
OP19	Demilitarizovaná zóna	OP38	Šifrovanie dát, informácií a komunikácie
OP20	VPN	OP39	Elektronický podpis
OP21	Kontrola, ochrana prístupu k podnikovej sieti	OP40	Bezpečnostné protokoly, certifikáty (TLS)
OP22	Firewall	OP41	Zálohovanie na diskoch
OP23	Vyhodnocovanie, manažment, archivácia logov	OP42	Zálohovanie na cloude
OP24	IDS	OP43	Likvidácia médií a dát (skartovanie a i.)
OP25	IPS	OP44	Záložné zdroje UPS
OP26	SIEM	OP45	EZS
OP27	DLP	OP46	EPS
OP28	Penetračné testovanie	OP47	CCTV
OP29	Forenzná analýza	OP48	Hasiace prístroje
OP30	Overovanie identity cez heslo	OP49	Zabezpeč. kancelárií (uzamyk. šuplíky, dvere)
OP31	Čipové karty zamestnancov	OP50	Ochrana neobsluhovaného zariadenia
OP32	Bezpečnostné tokeny	OP51	Kontrola vstupu (vrátnica, turnikety a i.)
OP33	SMS autorizácia	OP52	Bezpečnostné dvere, okná
OP34	Overovanie identity cez biometrické prostriedky	OP53	Klimatizovaná serverovňa
OP35	SSO (Systém jednotného prihlasovania)	OP54	Ochrana kabeláže
OP36	Nastavenie bezpečnosti Wi–Fi sietí	OP55	Ochrana inžinierskych sietí

Zdroj: vlastné spracovanie

Premenné zo skupiny CH sú buď diskrétne (CH04) alebo kategorické (CH01, CH02, CH03, CH05), ktoré meriame na nominálnych škálach. Pre CH04 je určená pomerová škála a jej účelom je triedenie respondentov podľa veľkosti podniku. Všetky ostatné premenné

skupín SY, IA, HR a OP, okrem SY08 a SY09, sú spojité premenné merané na pomerovej škále od 0 po 100 bodov. SY08 a SY09 sú kategorickými premennými na ordinálnej škále.

Po získaní dát z prieskumu nasleduje analýza reliability dotazníka a štruktúry dát, analýza rizík, verifikácia hypotéz, efektov vybraných faktorov a analýza existujúcich opatrení, čím dostaneme kompletný prehľad o stave problematiky v skúmaných podnikoch. Ďalším krokom je návrh modelu manažmentu informačnej bezpečnosti elektronického podnikania, ktorý pozostáva z procesov riadenia IB a ich vzájomných vzťahov.

3.4 Použité metódy vyhodnotenia a interpretácie výsledkov

Pri spracovaní dizertačnej práce sme využívali viaceré metódy vedeckej práce. Predovšetkým ide o všeobecné vedecké metódy (indukcia, dedukcia, analýza, syntéza, komparácia, generalizácia, abstrakcia a analógia) a špeciálne metódy (matematicko–štatistické metódy, metóda dotazníkového prieskumu, metóda analýzy rizík podľa ISO/IEC 27005). Prehľad metód pri spracovaní konkrétnych častí práce sa nachádza v tabuľke 12.

Tab. 12: Prehľad vybraných metód

Časť práce	Činnosť	Druh metód	Použitá metóda
Súčasný stav problematiky	Skúmanie a zhodnotenie	Všeobecné	Analýza, komparácia, syntéza
Cieľ práce	Formulácia cieľov a hypotéz	Všeobecné	Indukcia, dedukcia, analógia
Dotazníkový prieskum	Stanovenie premenných	Všeobecné	Indukcia, dedukcia, abstrakcia
	Meranie vnútornej konzistencie dotazníka	Analýza reliability	Cronbachova alfa
Výsledky práce	Skúmanie štruktúry dátového súboru	Deskriptívna štatistika	Priemer, medián, modus, smerodajná odchýlka, kvantily, interval spoľahlivosti, variačné rozpätie
		Testy o rozdelení dátového súboru, testy homogenity rozptylov	Kolmogorovov–Smirnovov test, Levenov test
	Vyhodnotenie miery rizika	Posúdenie rizika	Analýza rizík podľa ISO/IEC 27005
	Skúmanie vzťahov medzi premennými v prípade normálneho rozdelenia	Testy zhody, korelačné testy	T–test, Pearsonov korelačný koeficient
	Skúmanie vzťahov medzi premennými v prípade iných rozdelení	Neparametrické testy, korelačné testy	Mann–Whitneyho U test, Spearmanovo rho, Kendallovo tau–c, Goodmanova–Kruskalova gamma, Somersove d
	Verifikácia a falzifikácia hypotéz	Neparametrické testy, regresia, korelačné testy, analýza rozptylu	Mann–Whitneyho U test, regresná analýza, korelačný koeficient, ANOVA
	Zostavenie modelu	Všeobecné	Syntéza, abstrakcia, generalizácia
Diskusia	Interpretácia výsledkov a tvorba záverov	Všeobecné	Syntéza, generalizácia, indukcia, dedukcia

Zdroj: vlastné spracovanie

Štatistické analýzy, testy a podrobné agregácie a vizualizácie dát sme uskutočnili v prostredí softvérov PSPP a Microsoft Excel. Pre spracovanie analýzy rizík IB sme vybrali

jednu z viacerých metód podľa normy ISO/IEC 27005, ktorá kalkuluje mieru rizika vynásobením pravdepodobnosti výskytu hrozby s významom aktíva, na ktoré daná hrozba pôsobí. Metóda následne zoraďuje, priorizuje riziká IB podľa veľkosti vypočítaných mier. Výhodou oproti iným metódam je jej jednoduchosť, univerzálnosť použitia a výpočet miery rizika len s dvomi premennými. Túto metódu sme podľa odporúčania normy prispôsobili potrebám výskumu dizertačnej práce a získaných dát. Stanovili sme kvalitatívne stupnice pre hodnotu aktíva a pravdepodobnosť hrozby, intervaly pre mieru rizika (tabuľka 13) a aplikovaním vzorca sme vytvorili maticu mier rizík informačnej bezpečnosti (tabuľka 14).

Tab. 13: Stupnice analýzy rizík

Stupnica	Význam aktíva	1	Nízka
		2	Stredná
		3	Vysoká
		4	Kritická
	Hrozba	1	Nepravdepodobná
		2	Málo pravdepodobná
		3	Pravdepodobná
		4	Viac–menej istá
	Miera rizika	<1, 4)	Nízka
		<4, 8)	Stredná
		<8, 12)	Vysoká
		<12, 16>	Kritická

Zdroj: STN ISO/IEC 27005: 2012: Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti.

Hodnoty premenných, ktoré sa týkajú významu informačných aktív a pravdepodobnosti výskytu hrozieb, sme rovnomerne prispôsobili zo škály od 0 po 100 bodov na škálu od 1 po 4 pre každého respondenta individuálne. Jedna úroveň predstavuje 25 bodov. Súčinom hodnôt súvisiacich významov aktív a pravdepodobností hrozieb každého respondenta boli identifikované a vyhodnotené individuálne miery rizík.

Tab. 14: Matica miery rizika

Matica miery rizika	Pravdepodobnosť výskytu hrozby	1	2	3	4
Význam aktíva	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

Zdroj: vlastné spracovanie

Na vytvorenie celkovej analýzy rizík IB v skúmaných podnikoch boli v matici miery rizika vypočítané aritmetické priemery získaných mier rizík jednotlivých respondentov s následným určením poradia rizík. Priemerné miery rizika sme kvalitatívne ohodnotili podľa intervalov v tabuľke 13. Analýzou rizík identifikujeme kritické riziká v skúmanom prostredí a zároveň je východiskom pre navrhovaný model.

4 Výsledky práce

V nasledujúcej kapitole analyzujeme, vyhodnocujeme a generalizujeme výsledky dotazníkového prieskumu v podnikoch s elektronickým obchodom na Slovensku podľa stanovených cieľov a metodiky dizertačnej práce. Výsledné analýzy, verifikácie alebo falzifikácie hypotéz a vlastné návrhy riešenia rôznych oblastí skúmanej problematiky sú východiskovými bodmi pre návrh modelu manažmentu informačnej bezpečnosti v elektronickom podnikaní.

4.1 Analýza reliability dotazníka

Na posúdenie celkovej reliability distribuovaného dotazníka sme zvolili Cronbachovu alfu, ktorá meria vnútornú konzistenciu škál dotazníka. Vypočítané hodnoty sa nachádzajú v tabuľke 15. Ako prvé sme analyzovali premenné v jednotlivých podskupinách a následne celé skupiny premenných. Do výpočtu Cronbachovej alfy vstupujú len premenné s číselnými hodnotami, preto sú kategorické premenné z výpočtu vylúčené. Vylúčili sme aj premennú počet zamestnancov (CH04), pretože nevstupuje do ďalších analýz a je jedinou diskrétnou premennou skupiny charakteristika podniku (CH). Hodnotu Cronbachovej alfy pre skupinu premenných CH nie je možné získať.

Tab. 15: Analýza reliability škál dotazníka

Škála	Počet premenných	Cronbachova alfa	Reliabilita škály
SY	**9**	**0,64**	**Akceptovateľná**
IA	**38**	**0,96**	**Excelentná**
IAPA	8	0,85	Veľmi dobrá
IADA	4	0,79	Dobrá
IAHA	5	0,84	Veľmi dobrá
IASO	8	0,88	Veľmi dobrá
IASI	4	0,76	Dobrá
IAPE	3	0,92	Excelentná
IALO	6	0,90	Excelentná
HR	**49**	**0,97**	**Excelentná**
HRFP	6	0,91	Excelentná
HRSZ	3	0,85	Veľmi dobrá
HRUI	8	0,92	Excelentná
HRTZ	3	0,92	Excelentná
HRNC	5	0,95	Excelentná
HRPF	4	0,87	Veľmi dobrá
HRPK	8	0,96	Excelentná
HRPS	5	0,94	Excelentná
HRIH	7	0,93	Excelentná
OP	**55**	**0,98**	**Excelentná**
OPOO	17	0,97	Excelentná
OPTO	38	0,96	Excelentná

Zdroj: vlastné spracovanie

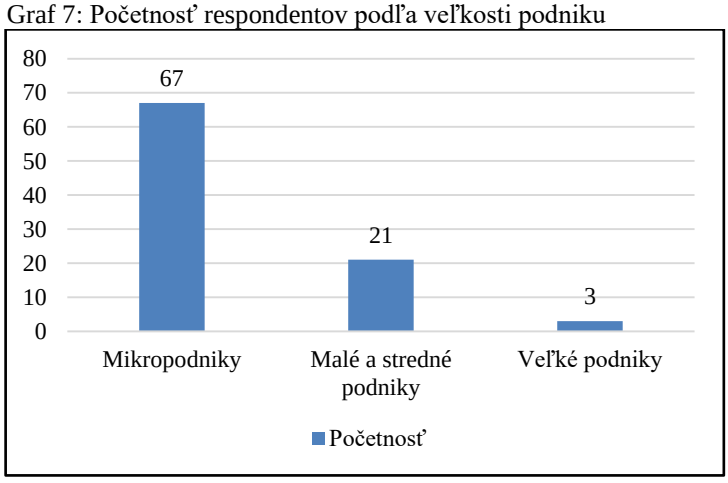
Reliabilita škál podľa Cronbachovej alfy pre jednotlivé podskupiny premenných sa pohybuje od dobrej úrovne (0,76) pre informačné aktíva podskupiny sieť (IASI) až po excelentnú úroveň (0,97) pre organizačné opatrenia (OPOO). Dôležité sú vynikajúce hodnoty súhrnných skupín premenných, pre škálu významu informačných aktív (IA) $\alpha = 0,96$, pre pravdepodobnosť výskytu hrozieb (HR) $\alpha = 0,97$ a pre opatrenia informačnej bezpečnosti (OP) $\alpha = 0,98$. Skupina systému riadenia informačnej bezpečnosti (SY) síce zaostáva za ostatnými škálami, avšak dosahuje aspoň akceptovateľnú úroveň (0,64). Ani jedna škála nedosahuje slabú, prípadne neakceptovateľnú úroveň. Výsledky Cronbachovej alfy ukazujú, že väčšina škál bola navrhnutá na excelentnej úrovni. Z tohto dôvodu považujeme dáta za kvalitné a dotazník vysoko reliabilný.

4.2 Štruktúra dátového súboru

Z výberového súboru, ktorý predstavuje podniky s elektronickým obchodom využívajúce slovenský elektronický trh, bol získaný reprezentatívny dátový súbor. Ide o vzorku 91 podnikov rôznej veľkosti, právnej formy, ekonomickej činnosti, zamerania a miesta svojho sídla.

Vychádzajúc z premennej CH04, ktorá obsahuje počty zamestnancov, sme začlenili podniky podľa veľkosti. Početnosť skúmaných podnikov sa nachádza v grafe 7. Najpočetnejšou kategóriou sú mikropodniky (73,63 %), nasledujú malé a stredné podniky (23,08 %) a veľké podniky (3,30 %). Štruktúra dátového súboru kopíruje poradie podľa aktuálneho stavu členenia podnikov podľa veľkosti v SR.

Graf 7: Početnosť respondentov podľa veľkosti podniku



Zdroj: vlastné spracovanie

Všeobecne, najviac elektronických obchodov v SR prevádzkujú mikropodniky. Pre mnohé z nich tvorí až 100 % z čistého obratu. Na druhej strane, na Slovensku je malý počet

veľkých podnikov a z nich len malá časť využíva elektronický obchod, častokrát len ako formu podnikovej prezentácie a dodatočných tržieb.

V tabuľke 16 sú dáta triedené podľa právnej formy vo vzťahu k veľkosti podniku. Spoločnosť s ručením obmedzeným predstavuje najväčšiu časť zo všetkých právnych foriem, 58,24 % z celku. Nasledujú živnostníci (28,57 %), akciové spoločnosti (5,49 %) a družstvá (4,40 %). Európske spoločnosti, organizačné zložky zahraničnej osoby a verejné obchodné spoločnosti predstavujú 1,10 % respondentov.

Tab. 16: Štruktúra dátového súboru podľa právnej formy a veľkosti podniku

Právna forma (CH01)	**Veľkosť podniku podľa počtu zamestnancov (CH04)**			**Spolu**
	Mikropodniky	Malé a stredné podniky	Veľké podniky	
Akciová spoločnosť	1,10 %	2,20 %	2,20 %	5,49 %
Družstvo	0,00 %	3,30 %	1,10 %	4,40 %
Európska spoločnosť	0,00 %	1,10 %	0,00 %	1,10 %
Organizačná zložka zahraničnej osoby	0,00 %	1,10 %	0,00 %	1,10 %
Spoločnosť s ručením obmedzeným	43,96 %	14,29 %	0,00 %	58,24 %
Verejná obchodná spoločnosť	1,10 %	0,00 %	0,00 %	1,10 %
Živnostník	27,47 %	1,10 %	0,00 %	28,57 %
Spolu	73,63 %	23,08 %	3,30 %	100,00 %

Zdroj: vlastné spracovanie

Až 43,96 % mikropodnikov má právnu formu spoločnosti s ručením obmedzeným a 27,47 % mikropodnikov sú živnosťou. 1,10 % mikropodnikov sú akciovými spoločnosťami a verejnými obchodnými spoločnosťami. 14,29 % MSP podniká ako spoločnosť s ručením obmedzeným, 3,30 % ako družstvo a 2,20 % ako akciová spoločnosť. Nasleduje živnosť, organizačná zložka zahraničnej osoby a európska spoločnosť (1,10 % malých a stredných podnikov). Z veľkých podnikov sú zastúpené len akciové spoločnosti (2,20 %) a družstvá (1,10 %).

Štruktúra dátového súboru podľa kraja sídla podniku vo vzťahu k jeho veľkosti je zobrazená v tabuľke 17. Najviac respondentov pochádza z Bratislavského kraja (38,46 %), z toho 28,57 % mikropodnikov, 8,79 % MSP a 1,10 % veľkých podnikov. Nasleduje Nitriansky kraj (10,99 %), z toho 6,59 % mikropodnikov a 4,40 % MSP. Tretím najpočetnejším je Prešovský kraj (9,89 %), kde 8,79 % tvoria mikropodniky a 1,10 % MSP. Najmenej respondentov sme získali z Košického kraja (4,40 %), kde sú zastúpené iba mikropodniky. Veľké podniky v prieskume okrem Bratislavského kraja pochádzajú aj z Banskobystrického kraja a zahraničia, konkrétne z Európskej únie (po 1,10 %). Pozitívnym faktom je, že prieskum obsiahol respondentov z každého kraja Slovenska a niektorých tiež

z Európskej únie (5,49 %). Ide o podnikateľov, ktorí využívajú elektronický obchod aj na území Slovenskej republiky.

Tab. 17: Štruktúra dátového súboru podľa kraja sídla a veľkosti podniku

Kraj sídla podniku (CH03)	**Veľkosť podniku podľa počtu zamestnancov (CH04)**			**Spolu**
	Mikropodniky	Malé a stredné podniky	Veľké podniky	
Banskobystrický	2,20 %	2,20 %	1,10 %	5,49 %
Bratislavský	28,57 %	8,79 %	1,10 %	38,46 %
Košický	4,40 %	0,00 %	0,00 %	4,40 %
Nitriansky	6,59 %	4,40 %	0,00 %	10,99 %
Prešovský	8,79 %	1,10 %	0,00 %	9,89 %
Trenčiansky	8,79 %	0,00 %	0,00 %	8,79 %
Trnavský	5,49 %	3,30 %	0,00 %	8,79 %
Žilinský	5,49 %	2,20 %	0,00 %	7,69 %
Zahraničie – EÚ	3,30 %	1,10 %	1,10 %	5,49 %
Spolu	73,63 %	23,08 %	3,30 %	100,00 %

Zdroj: vlastné spracovanie

Početnosť podnikov v prieskume podľa ekonomickej činnosti sledujeme v tabuľke 18. Najviac skúmaných podnikov pochádza zo skupiny G (50,55 %), skupiny S (21,98 %) a skupiny M (6,59 %). Všetky ekonomické činnosti v prieskume nie sú zastúpené. Výsledky potvrdzujú, že väčšina elektronických obchodov je zameraná práve na maloobchodný alebo veľkoobchodný predaj.

Tab. 18: Štruktúra dátového súboru podľa ekonomickej činnosti

Ekonomická činnosť podľa SK NACE Rev. 2 (CH02)	**Početnosť**	**%**
A – Poľnohospodárstvo, lesníctvo a rybolov	5	5,49 %
C – Priemyselná výroba	2	2,20 %
F – Stavebníctvo	2	2,20 %
G – Veľkoobchod a maloobchod; oprava motorových vozidiel a motocyklov	46	50,55 %
H – Doprava a skladovanie	1	1,10 %
I – Ubytovacie a stravovacie služby	1	1,10 %
J – Informácie a komunikácia	2	2,20 %
K – Finančné a poisťovacie činnosti	1	1,10 %
M – Odborné, vedecké a technické činnosti	6	6,59 %
O – Verejná správa a obrana; povinné sociálne zabezpečenie	1	1,10 %
P – Vzdelávanie	2	2,20 %
R – Umenie, zábava a rekreácia	2	2,20 %
S – Ostatné činnosti	20	21,98 %
Spolu	**91**	**100,00 %**

Zdroj: vlastné spracovanie

Jedna z otázok prieskumu bola zameraná na určenie hlavných odberateľov elektronického obchodu podniku. Respondenti mali možnosť vyberať z kategórií B2C, B2B a B2G. Avšak, štátnu správu nepovažuje ani jeden respondent za hlavného odberateľa. Štruktúra odpovedí sa nachádza v tabuľke 19. Až 89,01 % podnikov s elektronickým obchodom poskytuje tovar a služby primárne jednotlivcom, z toho 68,13 % mikropodnikov,

18,68 % MSP a 2,20 % veľkých podnikov. 10,99 % skúmaných podnikov sa zameriava na podniky a organizácie, z toho 5,49 % mikropodnikov, 4,40 % MSP a 3,30 % veľkých podnikov. Výsledky zobrazujú realitu, kde väčšina elektronických obchodov cieli na koncového spotrebiteľa v podobe fyzickej osoby.

Tab. 19: Štruktúra dátového súboru podľa hlavných odberateľov a veľkosti podniku

Hlavní odberatelia (CH05)	**Veľkosť podniku podľa počtu zamestnancov (CH04)**			**Spolu**
	Mikropodniky	Malé a stredné podniky	Veľké podniky	
Jednotlivci (B2C)	68,13 %	18,68 %	2,20 %	89,01 %
Podniky a organizácie (B2B)	5,49 %	4,40 %	1,10 %	10,99 %
Spolu	73,63 %	23,08 %	3,30 %	100,00 %

Zdroj: vlastné spracovanie

Dátový súbor je z pohľadu charakteristík podniku rozmanitý a zároveň adekvátne štruktúrovaný. Všetky dáta premenných, ktoré sú podstatné pre ďalšie skúmanie, sú získané v požadovanej kvalite. V prieskume máme zastúpených respondentov z každého kraja SR a každej kategórie veľkosti podniku. Najviac podnikov s elektronickým obchodom sú maloobchodmi alebo veľkoobchodmi s hlavným zameraním na jednotlivcov. Zároveň sú v dostatočnom počte zastúpené najvyužívanejšie právne formy podnikov v SR (živnosti, spoločnosti s ručením obmedzeným a akciové spoločnosti).

4.3 Vyhodnotenie systému riadenia informačnej bezpečnosti

V podkapitole skúmame výsledky skupiny premenných so zameraním na systém riadenia informačnej bezpečnosti, na základe ktorých určíme aktuálny stav manažmentu informačnej bezpečnosti v podnikoch s elektronickým obchodom. Deskriptívna štatistika premenných, okrem kategorických premenných pravidelnosť vyhodnocovania rizík IB (SY08) a pravidelnosť aktualizácie rizík IB (SY09), sa nachádza v tabuľke 20.

Tab. 20: Deskriptívna štatistika premenných skupiny SY

Premenná	**N**	**Min**	**Max**	**Variačné rozpätie**	**Špicatosť**	**Šikmosť**	**Modus**	**Medián**	**M**	**SD**
SY01	91	0	100	100	-0,73	-0,51	100	70	**64,89**	**30,02**
SY02	91	0	100	100	-1,03	0,23	50	49	**45,02**	**30,23**
SY03	91	0	100	100	-0,79	-0,09	50	50	**51,75**	**29,38**
SY04	91	1	100	99	-0,74	-0,41	100	60	**61,26**	**29,33**
SY05	91	0	100	100	-0,70	0,66	0	24	**30,08**	**28,59**
SY06	91	0	77	77	4,64	2,04	5	6	**12,63**	**15,11**
SY07	91	0	100	100	-1,03	0,48	–	29	**36,95**	**32,15**
SY10	91	1	100	99	-0,54	-0,61	50	70	**66,63**	**27,09**
SY11	91	1	100	99	-0,68	-0,52	80	70	**62,93**	**27,68**

Zdroj: vlastné spracovanie

Premenná s názvom nutnosť riešenia ISMS v rámci e–business (SY01) určuje, či je potrebné zaoberať sa oblasťami ISMS v elektronickom podnikaní, kde 0 bodov predstavuje rozhodne nie a 100 bodov určite áno. Priemerná hodnota dosahuje M = 64,89 bodov; smerodajná odchýlka SD = 30,02 bodov. Z údajov vyplýva, že podniky sa na 64,89 % prikláňajú k tvrdeniu, že ISMS by mal byť riešený v rámci elektronického podnikania. Najčastejšou hodnotou je 100 bodov. 50 % respondentov uviedlo počet bodov viac a menej ako 70 a zároveň až 25% respondentov ohodnotilo premennú viac ako 93 bodmi. Podniky s elektronickým obchodom si dôležitosť ISMS uvedomujú. Podľa špicatosti je v súbore viac extrémnejších hodnôt (-0,73) a podľa šikmosti hodnoty smerujú bližšie k 100 (-0,51). Ide o plochejšie, vpravo zošikmené rozdelenie. Pretože výsledky Kolmogorovovho–Smirnovovho testu na hladine významnosti $\alpha = 0,05$ potvrdzujú, že dáta sú rozložené normálne ($Z = 1,16$; $p = 0,120$), môžeme tvrdiť, že s 95 % spoľahlivosťou je interval pre strednú hodnotu potreby riešenia ISMS v oblasti elektronického podnikania medzi 58,64 a 71,14 bodmi.

Ďalšou premennou je možnosť ochrany e–business bez ISMS (SY02), ktorou sme skúmali, či elektronické podnikanie dokáže byť chránené pred informačnými rizikami bez uceleného ISMS, kde 0 bodov znamená rozhodne nedokáže a 100 bodov určite dokáže. Výsledky dokazujú nerozhodnosť predstaviteľov podnikov v tejto problematike ($M = 45,02$; $SD = 30,23$; Modus = 50; Medián = 49), aj keď viac respondentov je podľa šikmosti (0,23) naklonených k menším hodnotám, čiže k nutnosti ISMS v elektronickom podnikaní. 10 % respondentov uviedlo viac ako 88 bodov. Títo respondenti tvrdia, že chrániť elektronické podnikanie je určite možné aj bez ISMS. Podľa špicatosti (-1,03) je rozdelenie plochejšie. Dáta sú rozložené normálne (K–S test; $Z = 1,00$; $p = 0,269$), preto môžeme určiť 95 % interval spoľahlivosti pre strednú hodnotu normálneho rozdelenia (38,73; 51,32).

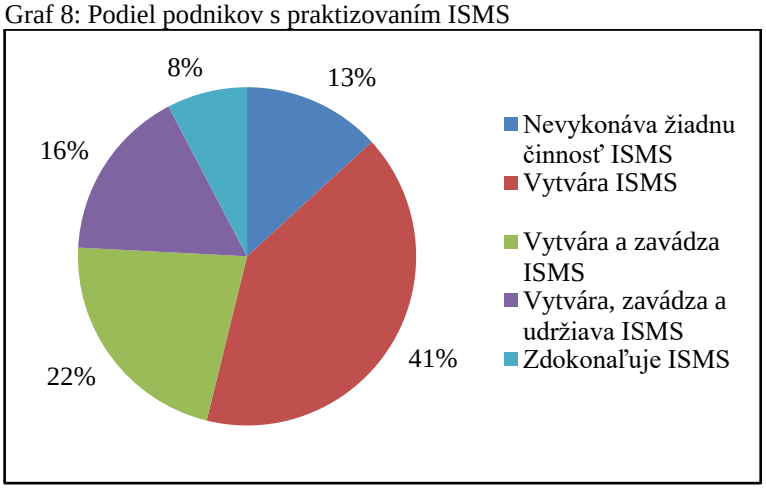
Ďalšia premenná, možnosť ISMS zlepšiť výsledky e–business (SY03), skúma názor, či zavedený systém riadenia IB môže zlepšiť hospodárske výsledky elektronického podnikania od 0 (rozhodne nemôže) po 100 bodov (určite môže). Výsledky sú v tomto prípade opäť nerozhodné ($M = 51,75$; $SD = 29,38$; Modus = 50; Medián = 50). Respondenti nedokážu posúdiť, či ISMS vplýva na hospodárske výsledky podniku alebo nie. Dáta sú plochejšie (-0,79), mierne zošikmené k menším hodnotám (-0,09) a sú normálne rozdelené (K–S test; $Z = 0,86$; $p = 0,465$). 95% interval spoľahlivosti pre strednú hodnotu základného súboru je medzi 45,63 a 57,87 bodmi.

Štvrtá premenná skupiny SY s názvom potreba ISMS v e–business respondenta (SY04) meria potrebu vytvoriť, zaviesť, udržiavať a stále zlepšovať ISMS v skúmanom

podniku s elektronickým obchodom. Škálu sme definovali od 0 (rozhodne nie) po 100 bodov (určite áno). 50 % respondentov ohodnotilo túto potrebu na viac alebo menej ako 60 bodov. Najčastejšie uvedenou hodnotou je 100 bodov a týchto respondentov je až 15,38 %. Účastníci prieskumu sa v priemere prikláňajú k potrebe zdokonaľovania ISMS v ich podniku (M = 61,26; SD = 29,33). 75 % respondentov uviedlo viac ako 46,5 bodov. Dáta sú prevažne plocho distribuované (-0,74) a vpravo zošikmené (-0,41). Podľa výsledkov K–S testu na hladine významnosti α = 0,05 sú dáta normálne rozložené (Z = 0,89; p = 0,407), preto môžeme tvrdiť, že stredná hodnota rozdelenia sa s 95 % spoľahlivosťou nachádza medzi 55,16 a 67,37 bodmi.

V prieskume nasleduje premenná praktizovanie ISMS v podniku (SY05), ktorá skúma či podniky vytvárajú, zavádzajú, udržiavajú a zdokonaľujú ISMS vo svojom prostredí. Premenná je špecifická, pretože sme jej hodnoty v slovnom popise kategorizovali do štyroch intervalov, s čím boli respondenti oboznámení. Hodnoty sú rozdelené v kategóriách od 0 do 25 % (podniky vytvárajú ISMS), ďalej do 50 % (vytvárajú a zavádzajú ISMS), do 75 % (vytvárajú, zavádzajú a udržiavajú ISMS) a až do 100 % (zdokonaľujú ISMS). 0 % predstavuje, že podniky nevykonávajú žiadnu činnosť v oblasti ISMS. Graf 8 ukazuje podiely v daných kategóriách.

Graf 8: Podiel podnikov s praktizovaním ISMS



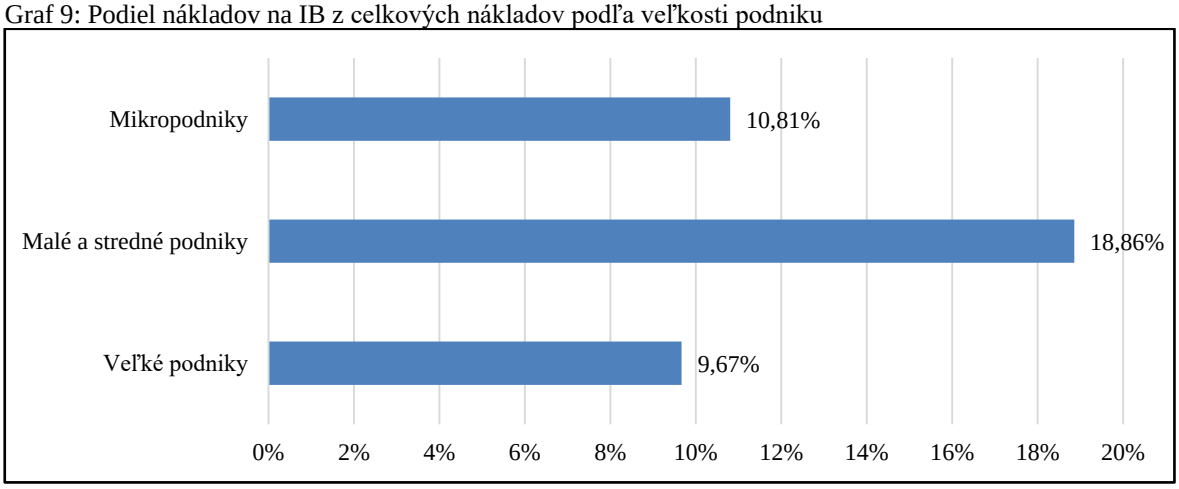
Zdroj: vlastné spracovanie

Najviac podnikov vytvára len základnú formu manažmentu informačnej bezpečnosti (41 %), je teda len v začiatočnej fáze ISMS. Avšak, až 13 % podnikov nevykonáva žiadnu činnosť v tejto oblasti. Zaujímavosťou je, že 8 % podnikov už má ISMS zavedené a zdokonaľuje, teda zlepšuje tento systém. V priemere podniky dosahujú M = 30,08 bodov; SD = 28,59 bodov. Dáta sú naklonené skôr k menším hodnotám (0,66) a sú skôr plochejšie (-0,70). Až 25 % respondentov uviedlo hodnotu menšiu alebo rovnú 2, čo znamená, že tieto

podniky sa ISMS vôbec nevenujú. Medián predstavuje iba 24 bodov. Až 75 % hodnôt sa zmestí do 50 bodov. Z týchto údajov vyplýva, že podniky manažment informačnej bezpečnosti skôr nezavádzajú a nevenujú mu dostatok pozornosti. Pretože dáta nie sú rozložené podľa normálneho rozdelenia (K–S test; Z = 1,47; p = 0,018), 95 % interval spoľahlivosti strednej hodnoty základného súboru nie je možné hodnoverne určiť.

Nasleduje premenná podiel nákladov na IB z celkových nákladov (SY06), ktorú sme merali v percentách. Podniky v priemere investujú do IB 12,63 % z celkových nákladov (M = 12,63; SD = 15,11). Prehľad nákladov na IB z pohľadu veľkosti podniku sa nachádza v grafe 9.

Graf 9: Podiel nákladov na IB z celkových nákladov podľa veľkosti podniku



Zdroj: vlastné spracovanie

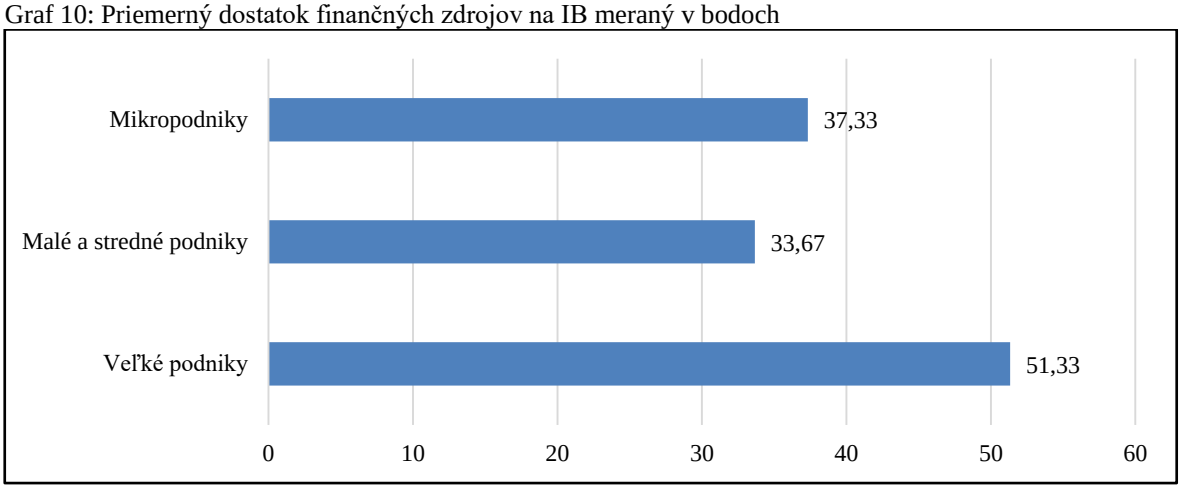
Malé a stredné podniky investujú najviac, až 18,86 % z celkových nákladov. Nasledujú mikropodniky (10,81 %) a veľké podniky (9,67 %). Podiely nákladov všetkých kategórií považujeme za nadbytočne vysoké, avšak výsledky môžu byť skreslené nízkym počtom respondentov v kategóriách MSP a veľké podniky a tiež niekoľkými vysokými hodnotami zo súboru dát, čo zisťujeme podľa modusu, mediánu, špicatosti a šikmosti.

Hodnota modusu vyjadruje, že najväčší počet podnikov využíva 5 % nákladov na IB. Až polovica hodnôt je menej ako 6 %. Dáta sú podľa očakávania výrazne zošikmené k nízkym hodnotám (2,04) a podľa špicatosti majú väčšinu hodnôt blízko priemeru (4,64). Tri štvrtiny podnikov míňa na IB maximálne do 20 % z celkových nákladov. Iba 10 % podnikov investuje do problematiky viac ako 30 % zo svojich celkových nákladov. Už podľa deskriptívnej štatistiky vidieť, že dáta nie sú normálne rozdelené. To potvrdzuje aj K–S test (Z = 2,49; p < 0,001). Podľa štatistík vidíme, že relatívne vysoký priemer je ovplyvnený niekoľkými vysokými hodnotami. Modus a medián nám ukazujú reálnejší obraz o rozložení

dát. Preto tvrdíme, že podniky investujú do IB okolo 5 % z celkových nákladov, čo považujeme za adekvátnu výšku nákladov určených na IB.

Premennou dostatok finančných zdrojov na IB (SY07) sledujeme, či podnik disponuje finančnými prostriedkami, ktoré môže využiť na primeranú ochranu podnikových informácií na stupnici od 0 (rozhodne nie) po 100 bodov (určite áno). 50 % hodnôt predstavovalo viac alebo menej ako 29 bodov. Súbor dát podľa špicatosti obsahuje viac extrémnejších hodnôt (-1,03), ale podľa šikmosti je viac hodnôt menších (0,48). Respondenti v priemere určili, že skúmané podniky dostatkom voľných finančných zdrojov na IB skôr nedisponujú, len na M = 36,95 bodov; SD = 32,15 bodov. Priemery podľa jednotlivých veľkostí podniku môžeme sledovať v grafe 10. Podľa predpokladov, veľké podniky majú najviac voľných finančných prostriedkov, v priemere 51,33 bodov. Nasledujú mikropodniky (37,33 bodov) a MSP (33,67 bodov), ktoré takýmito prostriedkami skôr nedisponujú.

Graf 10: Priemerný dostatok finančných zdrojov na IB meraný v bodoch



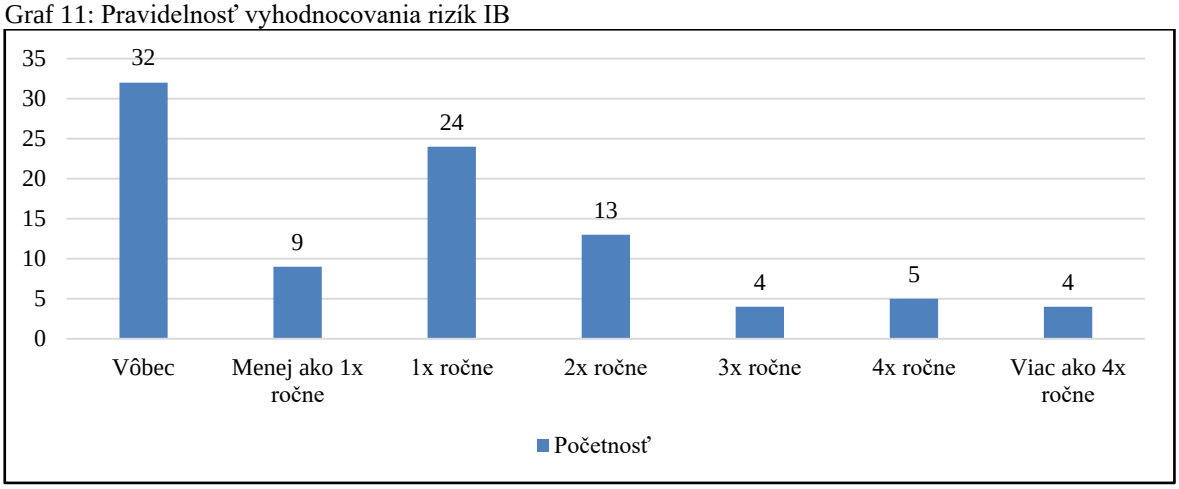
Zdroj: vlastné spracovanie

Podľa nášho názoru, ideálnym intervalom hodnotenia dostatku finančných prostriedkov je 75 a viac bodov. Avšak, takéto hodnoty uviedlo len 19 % podnikov. Iba 25 % podnikov má skôr dostatok voľných zdrojov, konkrétne nad 59 bodov. Až 10 % respondentov určilo hodnotu 0 alebo 1. To znamená, že približne jedna desatina podnikov s elektronickým obchodom nemá vôbec dostatok prostriedkov na zabezpečenie podnikových informácií. 95 % interval spoľahlivosti neurčujeme, pretože dáta nie sú normálne rozložené, čo indikujú výsledky štatistík a K–S testu (Z = 1,33; p = 0,043). Modus nie je možné určiť z dôvodu dvoch hodnôt s najvyššou početnosťou (1 a 50).

V grafe 11 sa nachádzajú frekvencie premennej pravidelnosť vyhodnocovania rizík IB (SY08) v skúmaných podnikoch. Najviac podnikov nevyhodnocuje riziká vôbec, až

35,16 % zo všetkých podnikov. Nasledujú podniky, ktoré vyhodnocujú riziká jedenkrát ročne (26,37 %) a dvakrát ročne (14,29 %).

Graf 11: Pravidelnosť vyhodnocovania rizík IB



Zdroj: vlastné spracovanie

Všeobecne platí, že čím častejšie sa podniky rizikami zaoberajú, tým sú viac pripravené na možné hrozby a incidenty IB. Podľa nášho názoru, podniky by mali vyhodnocovať riziká IB minimálne aspoň raz ročne. V prieskume to predstavuje 54,95 % podnikov. Uvedené percento je síce na podmienky SR prekvapujúco vysoké, avšak stále nízke v porovnaní s možnými dopadmi rizík IB. Pravidelnosť vyhodnocovania rizík vyjadrená v percentách podľa troch kategórií veľkosti podniku je uvedená v tabuľke 21.

Tab. 21: Pravidelnosť vyhodnocovania rizík IB vo vzťahu k veľkosti podniku

Pravidelnosť vyhodnocovania rizík IB (SY08)	**Veľkosť podniku podľa počtu zamestnancov (CH04)**			**Spolu**
	Mikropodniky	Malé a stredné podniky	Veľké podniky	
Vôbec	26,37 %	7,69 %	1,10 %	35,16 %
Menej ako 1x ročne	6,59 %	3,30 %	0,00 %	9,89 %
1x ročne	21,98 %	4,40 %	0,00 %	26,37 %
2x ročne	9,89 %	3,30 %	1,10 %	14,29 %
3x ročne	3,30 %	1,10 %	0,00 %	4,40 %
4x ročne	3,30 %	1,10 %	1,10 %	5,49 %
Viac ako 4x ročne	2,20 %	2,20 %	0,00 %	4,40 %
Spolu	73,63 %	23,08 %	3,30 %	100,00 %

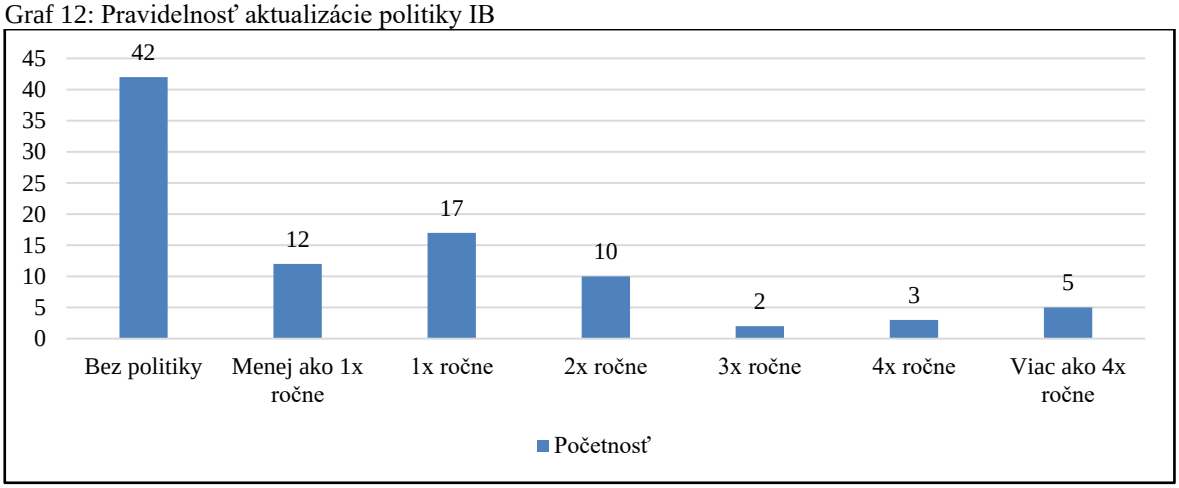
Zdroj: vlastné spracovanie

Až 26,37 % mikropodnikov, 7,69 % malých a stredných podnikov a 1,10 % veľkých podnikov z celkového súboru nevyhodnocuje riziká IB. V tomto priestore je potrebné zvyšovať bezpečnostné povedomie a upozorňovať na následky, ktoré môžu spôsobiť realizované riziká IB v podniku. Zaujímavý údaj je 21,98 %, ktorý predstavuje mikropodniky vyhodnocujúce riziká aspoň raz ročne, čo považujeme za mimoriadne dobré. Zvlášť upozorňujeme, že prieskum odhalil až 18,69 % mikropodnikov, 7,70 % MSP a 2,20 % veľkých podnikov z celkového súboru, ktorí sa zaoberajú rizikami viac ako

jedenkrát za rok. Tieto percentuálne údaje sú síce neočakávane vysoké, ale v najbližších rokoch by mali ešte významne narásť, aby boli riziká IB v podnikoch dostatočne riešené.

V premennej pravidelnosť aktualizácie politiky IB (SY09) sme skúmali, či podniky vypracovali politiku informačnej bezpečnosti a v akých časových intervaloch ju obnovujú. V grafe 12 sa nachádza početnosť konkrétnych kategórií. Podľa predpokladov, veľká časť podnikov nemá túto politiku vypracovanú, čo predstavuje 46,15 % podnikov.

Graf 12: Pravidelnosť aktualizácie politiky IB



Zdroj: vlastné spracovanie

Na druhej strane, 53,85 % podnikov má nejakú formu politiky IB, ktorú aktualizuje viac či menej pravidelne. Jedenkrát ročne politiku aktualizuje 18,68 % podnikov a viac ako raz ročne až 21,98 % podnikov. Z pohľadu veľkosti podniku, pravidelnosť vylepšovania politiky IB sledujeme v tabuľke 22.

Tab. 22: Pravidelnosť aktualizácie politiky IB vo vzťahu k veľkosti podniku

Pravidelnosť aktualizácie politiky IB (SY09)	**Veľkosť podniku podľa počtu zamestnancov (CH04)**			**Spolu**
	Mikropodniky	Malé a stredné podniky	Veľké podniky	
Bez politiky	38,46 %	6,59 %	1,10 %	46,15 %
Menej ako 1x ročne	7,69 %	5,49 %	0,00 %	13,19 %
1x ročne	12,09 %	6,59 %	0,00 %	18,68 %
2x ročne	8,79 %	2,20 %	0,00 %	10,99 %
3x ročne	1,10 %	0,00 %	1,10 %	2,20 %
4x ročne	2,20 %	0,00 %	1,10 %	3,30 %
Viac ako 4x ročne	3,30 %	2,20 %	0,00 %	5,49 %
Spolu	73,63 %	23,08 %	3,30 %	100,00 %

Zdroj: vlastné spracovanie

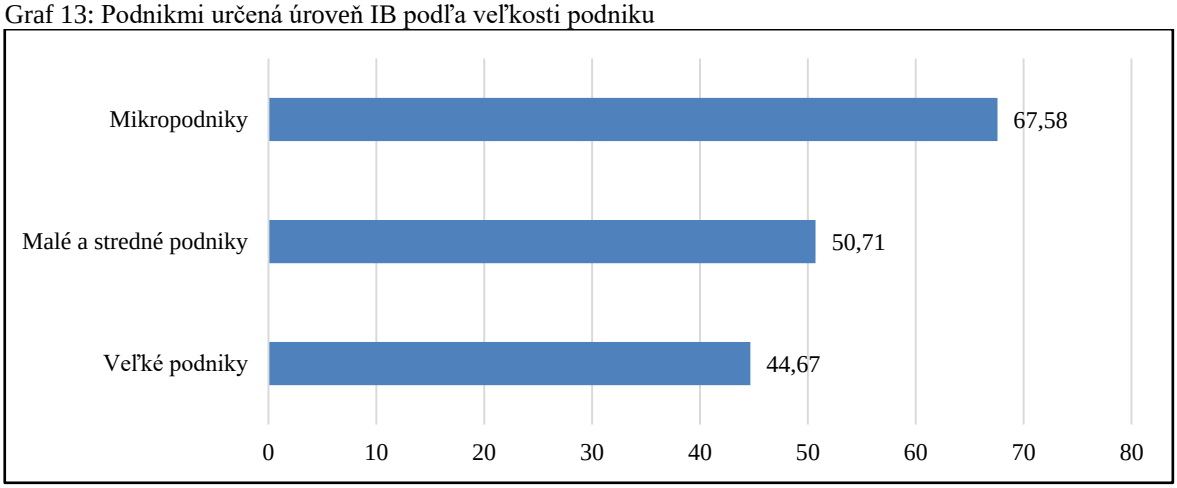
38,46 % mikropodnikov, 6,59 % MSP a 1,10 % veľkých podnikov z celého súboru dát nemá vypracovanú politiku informačnej bezpečnosti. Na tieto skupiny je potrebné zacieliť v súvislosti so vzdelávaním v oblasti IB. Podniky by mali aktualizovať svoju politiku IB minimálne aspoň raz ročne. Pretože hrozby IB sa neustále vyvíjajú, častejšia aktualizácia je viac odporúčaná. Ideálna frekvencia aktualizácie politiky IB závisí od

podmienok a potrieb konkrétneho podniku. Napríklad, veľké podniky by mali politiku vylepšovať častejšie ako raz ročne.

Nasleduje premenná spokojnosť s úrovňou IB podniku (SY10), ktorá zisťuje, do akej miery sú podniky spokojné s bezpečnosťou ich dôverných a citlivých informácií. Respondenti hodnotili na škále od 0 (rozhodne nespokojný) po 100 bodov (určite spokojný). V priemere sú reprezentanti podnikov skôr spokojní (M = 66,63; SD = 27,09), až 50 % hodnôt je nad 70 bodov. Špicatosť určuje viac ploché dáta (-0,54), ktoré sú vpravo zošikmené (-0,61), čiže obsahujú viac väčších hodnôt. Podľa K–S testu ide o dáta, ktoré nespĺňajú podmienku normálneho rozdelenia (Z = 1,33;p = 0,043). Aj keď najviac respondentov je nerozhodných (Modus = 50; 15,38 % podnikov), až 25 % respondentov ohodnotilo premennú viac ako 90 bodmi. Sumárne, väčšina podnikov s elektronickým obchodom je skôr spokojná so svojou úrovňou informačnej bezpečnosti.

Premenná úroveň IB v podniku (SY11) sa viaže k predchádzajúcej premennej, pretože meria vnímanú úroveň ochrany informácií v podniku. Respondenti na škále od 0 (minimálna) po 100 bodov (maximálna) hodnotili úroveň informačnej bezpečnosti v podniku. Priemernou hodnotou je M = 62,93 bodov; smerodajná odchýlka SD = 27,68 bodov. Informačná bezpečnosť v elektronickom podnikaní je na úrovni 62,93 %. Podniky tvrdia, že ich úroveň je dostačujúca. Z dôvodu aktuálnosti hrozieb IB by mala byť úroveň ešte oveľa vyššia. Úroveň IB určená respondentmi a zoskupená podľa veľkosti podniku sa nachádza v grafe 13.

Graf 13: Podnikmi určená úroveň IB podľa veľkosti podniku



Zdroj: vlastné spracovanie

Mikropodniky majú spomedzi ostatných podnikov najvyššiu pozorovanú úroveň IB, v priemere 67,58 bodov. Nasledujú MSP s 50,71 bodmi. Úroveň IB veľkých podnikov je skôr nedostatočná (44,67 bodov). S veľkou pravdepodobnosťou si veľké podniky viac

uvedomujú potrebu chrániť informácie ako podniky ostatných veľkostí a tým viac identifikujú svoje nedostatky. Navyše, oproti iným podnikom potrebujú zabezpečiť omnoho viac oblastí, systémov a procesov.

Respondenti najčastejšie ohodnotili úroveň IB 80 bodmi a polovica ohodnotila úroveň viac alebo menej ako 70 bodmi. Iba 25 % podnikov má úroveň nižšiu alebo rovnú 47,50 bodov. Dáta sú viac ploché ako špicaté (-0,68), zošikmené vpravo (-0,61) a nie sú normálne rozložené (K–S test; Z = 1,63; p = 0,006). Hodnoty úrovne IB môžeme vysvetliť dvomi spôsobmi. Buď je úroveň informačnej bezpečnosti v podnikoch skutočne na dostačujúcej úrovni a výsledky odzrkadľujú reálny stav, alebo podnikom chýba dostatočné vzdelanie a bezpečnostné povedomie, zatiaľ čo respondenti veria, že úroveň informačnej bezpečnosti podniku je dobrá.

Podľa výsledkov analýzy premenných skupiny systém riadenia informačnej bezpečnosti (SY) konštatujeme, že podniky majú základný prehľad o IB a sú pripravené na hrozby informačnej bezpečnosti len na základnej, dostačujúcej úrovni. Avšak, stále existuje veľká skupina podnikov, ktoré potrebujú manažment informačnej bezpečnosti zaviesť a vylepšovať, ideálne implementovaním vhodného systému. Naše tvrdenia budeme skúmať aj v nasledujúcich podkapitolách, ktorých analýzy a výsledky nám reálny stav manažmentu informačnej bezpečnosti v elektronickom podnikaní ešte viac objasnia.

4.3.1 Korelačný výskum systému riadenia informačnej bezpečnosti

V predchádzajúcej časti sme pomocou Kolmogorovovho–Smirnovovho testu zistili, že dáta intervalových premenných (škál) SY01, SY02, SY03 a SY04 sú normálne rozložené. Vzájomnú závislosť premenných preto overujeme Pearsonovým korelačným koeficientom, ktorého výsledky sa nachádzajú v tabuľke 23.

Tab. 23: Korelačná matica premenných s normálne rozloženými dátami

		SY01	**SY02**	**SY03**	**SY04**
SY01	Pearson Correlation	–	0,24	0,39	0,42
	Sig. (2-tailed)		0,020	0,000	0,000
	N		91	91	91
SY02	Pearson Correlation	0,24	–	0,00	-0,24
	Sig. (2-tailed)	0,020		0,966	0,022
	N	91		91	91
SY03	Pearson Correlation	0,39	0,00	–	0,39
	Sig. (2-tailed)	0,000	0,966		0,000
	N	91	91		91
SY04	Pearson Correlation	0,42	-0,24	0,39	–
	Sig. (2-tailed)	0,000	0,022	0,000	
	N	91	91	91	

Zdroj: vlastné spracovanie

Škála nutnosť riešenia ISMS v rámci e–business (SY01) koreluje so škálami možnosť ochrany e–business bez ISMS (SY02), r = 0,24; p = 0,020, a možnosť ISMS zlepšiť výsledky e–business (SY03), r = 0,39; p < 0,001, len slabo. Sila vzájomnej závislosti týchto škál je malá. Medzi premennými nutnosť riešenia ISMS v rámci e–business (SY01) a potreba ISMS v e–business respondenta (SY04) existuje stredne silná priama vzájomná závislosť, r = 0,42; p < 0,001. Z toho vyplýva, že premenné majú stredne silný vzájomný vzťah. Medzi škálami SY02 a SY03 neexistuje vzájomná závislosť (r = 0,00; p = 0,966). To znamená, že možnosť ochrany elektronického podnikania bez ISMS a zlepšovanie hospodárskych výsledkov elektronického podnikania zásluhou ISMS spolu nesúvisia. Škály premenných SY02 a SY04, r = -0,24; p = 0,022, rovnako ako škály SY03 a SY04, r = 0,39; p < 0,001, korelujú slabo.

Pretože podľa výsledkov K–S testu hodnoty intervalových premenných SY05, SY06, SY07, SY10 a SY11 nie sú normálne rozdelené a SY08 spolu s SY09 sú ordinálnymi premennými, na skúmanie vzájomných vzťahov využijeme Spearmanovo rho a Kendallovo tau–c. Výsledky sa nachádzajú v tabuľke 24, v ktorej sme zvýraznili hodnoty vzťahov premenných s viac ako slabou vzájomnou závislosťou.

Tab. 24: Výsledky Spearmanovej korelácie a Kendallovho tau–c

	Statistic	SY01	SY02	SY03	SY04	SY05	SY06	SY07	SY08	SY09	SY10	SY11
SY05	Kendall's tau–c	0,16	0,08	0,11	0,22	–	0,31	0,30	-0,29	-0,31	0,05	0,18
	Spearman Correlation	0,22	0,10	0,14	0,30		**0,42**	**0,41**	-0,38	-0,39	0,05	0,26
SY06	Kendall's tau–c	-0,06	-0,01	0,08	0,07	0,31	–	0,18	-0,15	-0,24	-0,09	0,06
	Spearman Correlation	-0,10	-0,01	0,11	0,11	**0,42**		0,24	-0,21	-0,34	-0,13	0,08
SY07	Kendall's tau–c	0,05	0,15	0,01	0,12	0,30	0,18	–	-0,19	-0,17	0,12	0,22
	Spearman Correlation	0,09	0,21	0,02	0,16	**0,41**	0,24		-0,25	-0,23	0,17	0,32
SY08	Kendall's tau–c	-0,08	-0,17	-0,12	-0,05	-0,29	-0,15	-0,19	–	–	0,12	-0,01
	Spearman Correlation	-0,11	-0,23	-0,15	-0,07	-0,38	-0,21	-0,25			0,15	-0,02
SY09	Kendall's tau–c	-0,01	-0,13	-0,10	0,00	-0,31	-0,24	-0,17	–	–	0,08	0,02
	Spearman Correlation	-0,01	-0,18	-0,13	0,01	-0,39	-0,34	-0,23			0,11	0,02
SY10	Kendall's tau–c	0,03	0,13	-0,04	-0,01	0,05	-0,09	0,12	0,12	0,08	–	**0,51**
	Spearman Correlation	0,04	0,18	-0,06	-0,04	0,05	-0,13	0,17	0,15	0,11		**0,68**
SY11	Kendall's tau–c	0,14	0,12	0,15	0,07	0,18	0,06	0,22	-0,01	0,02	**0,51**	–
	Spearman Correlation	0,20	0,18	0,24	0,11	0,26	0,08	0,32	-0,02	0,02	**0,68**	

Zdroj: vlastné spracovanie

Podľa Spearmanovho korelačného koeficientu, škála praktizovanie ISMS v podniku (SY05) koreluje stredne silno so škálou podiel nákladov na IB z celkových nákladov (SY06), r = 0,42, a škálou dostatok finančných zdrojov na IB (SY07), r = 0,41. Kendallovo tau–c strednú silu vzájomnej závislosti v oboch prípadoch nepotvrdzuje. Škála SY05 so škálou SY06 (τ = 0,31) a SY07 (τ = 0,30) koreluje len slabo. Prikláňame sa k výsledkom Kendallovho tau–c z dôvodu nižších hodnôt koeficientu. Úroveň vytvárania, zavádzania, udržiavania a zdokonaľovania ISMS v podnikoch len málo súvisí s vynaloženými nákladmi

na informačnú bezpečnosť v podnikoch a tiež s vnímaným dostatkom finančných zdrojov na primeranú ochranu podnikových informácií.

Ostatné kombinácie intervalových škál, okrem vzťahu premenných spokojnosť s úrovňou IB podniku (SY10) a úroveň IB v podniku (SY11), majú slabú vzájomnú závislosť. Preto sa nimi nebudeme ďalej zaoberať. Škály SY10 a SY11 korelujú stredne silno, čo dokazuje Spearmanovo rho (r = 0,68) a aj Kendallovo tau–c (τ = 0,51). Spokojnosť s úrovňou informačnej bezpečnosti stredne silno súvisí so stanovenou úrovňou informačnej bezpečnosti v podniku.

V skupine premenných SY sa nachádzajú dve ordinálne premenné, pravidelnosť vyhodnocovania rizík IB (SY08) a pravidelnosť aktualizácie politiky IB (SY09). Na určenie veľkosti ich vzájomného vzťahu sme použili viacero neparametrických testov. Výsledky analýzy sa nachádzajú v tabuľke 25.

Tab. 25: Výsledky vzájomnej závislosti ordinálnych premenných SY08 a SY09

	Category	Statistic	Type	Value	Asymp. Std. Error	Approx. T	Approx. Sig.
Symmetric measures	Ordinal by Ordinal	Kendall's tau–c	–	0,55	0,06	9,18	–
		Gamma	–	0,74	0,07	9,18	–
		Spearman Correlation	–	0,70	0,06	9,24	–
	N of Valid Cases	–	–	91	–	–	–
Directional measures	Ordinal by Ordinal	Somers' d	Symmetric	0,63	–	9,18	0,000
			SY08 Dependent	0,65	0,07	9,18	0,000
			SY09 Dependent	0,61	0,07	9,18	0,000

Zdroj: vlastné spracovanie

Výsledky všetkých štatistických nástrojov potvrdzujú stredne silnú vzájomnú závislosť ordinálnych premenných. Ako reprezentanta vyberáme Kendallovo tau–c, ktorého výsledok bol najnižší (τ = 0,55). Pravidelnosť vyhodnocovania rizík IB súvisí s pravidelnosťou aktualizácie politiky IB podniku. Sila tejto priamej lineárnej závislosti je stredná až veľká. Preto môžeme tvrdiť, že podniky, ktoré pravidelne identifikujú a vyhodnocujú riziká, zároveň pravidelne aktualizujú politiku IB. Obe činnosti vedú ku zlepšovaniu celého systému riadenia informačnej bezpečnosti.

Všeobecne, len niektoré zo škál disponujú stredne silnou lineárnou závislosťou (SY10 a SY11, SY08 a SY09, SY01 a SY04). Vzájomná závislosť ostatných škál ISMS je len slabá, prípadne až neexistujúca (napr. SY02 a SY03).

4.3.2 Porovnanie premenných SY v závislosti od skúmaných skupín

V podkapitole overujeme rozdiel medzi podnikmi, ktoré vyhodnocujú riziká IB (N = 59) a ktoré riziká nevyhodnocujú (N = 32) a tiež medzi podnikmi, ktoré majú

vypracovanú politiku IB (N = 49) a tými, ktoré túto politiku ešte nevytvorili (N = 42). Skupiny porovnávame s hodnotami jednotlivých premenných systému riadenia informačnej bezpečnosti (SY), kde testujeme, či je odlišnosť skupín štatisticky významná.

K–S testom sme v predchádzajúcich kapitolách rozdelili premenné zo skupiny SY na tie, ktoré pochádzajú z normálneho rozdelenia (SY01, SY02, SY03, SY04), a tie, ktoré nie sú normálne rozložené (SY05, SY06, SY07, SY10, SY11). Premenné, ktoré spĺňajú podmienku normality rozloženia dát, testujeme dvojvýberovým t–testom s rovnosťou rozptylov. Neparametrickým Mann–Whitneyho U testom testujeme tie dáta premenných, ktoré podmienku normálneho rozdelenia nespĺňajú.

V nasledujúcich tabuľkách uvádzame prehľad len tých premenných, pri ktorých bola dokázaná štatistická významnosť skúmaných rozdielov. V tabuľke 26 sa nachádzajú výsledky testovania, ktoré na základe Levenovho testu indikujú štatisticky významnú nerovnosť rozptylov skupín (F = 4,97; p = 0,028) a následne t–testom potvrdzujú štatisticky významný rozdiel v hodnotení premennej potreba ISMS v e–business respondenta (SY04), t(49,70) = 2,23; p = 0,030, medzi tými, ktorí vyhodnocujú riziká (M = 66,64; SD = 25,13) a ktorí nevyhodnocujú riziká IB (M = 51,06; SD = 34,05).

Tab. 26: Testovanie rozdielov premennej SY04 v závislosti od vyhodnocovania rizík

		Levene's Test for Equality of Variances		t–test for Equality of Means						
									95% Confidence Interval of the Difference	
	Equal variances	F	Sig.	t	df	Sig. (2–tailed)	Mean Difference	Std. Error Difference	Lower	Upper
SY04	Assumed	4,97	0,028	2,44	89,00	0,017	15,30	6,27	2,84	27,76
	Not assumed	–	–	2,23	49,70	0,030	15,30	6,85	1,54	29,06

Zdroj: vlastné spracovanie

Výsledky neparametrického testu v tabuľke 27 dokazujú, že podniky, ktoré sa zaoberajú rizikami IB, sa štatisticky významne odlišujú v premenných SY05, SY06 a SY07 (p < 0,05) od podnikov, ktoré sa rizikami nezaoberajú. Odlišnosti ostatných skúmaných premenných sú náhodné (p > 0,05).

Tab. 27: Testovanie rozdielov premenných SY v závislosti od vyhodnocovania rizík

Premenná		Mann–Whitney U	Z	Asymp. Sig. (2–tailed)
SY05	Praktizovanie ISMS v podniku	328,00	-5,13	0,000
SY06	Podiel nákladov na IB z celkových nákladov	536,50	-3,40	0,001
SY07	Dostatok finančných zdrojov na IB	415,50	-4,40	0,000

Zdroj: vlastné spracovanie

Z pohľadu vytvárania politiky IB v podnikoch s elektronickým obchodom sa výsledky testovania odlišností v skúmaných skupinách nachádzajú v tabuľke 28. Dvojvýberové t–testy premenných s normálne rozloženými dátami nepreukázali štatistickú

významnosť rozdielov. Avšak, neparametrické testovanie potvrdilo systematické rozdiely v premenných SY05, SY06 a SY07 medzi podnikmi s vytvorenou politikou IB a podnikmi bez politiky IB na hladine významnosti $\alpha = 0,05$.

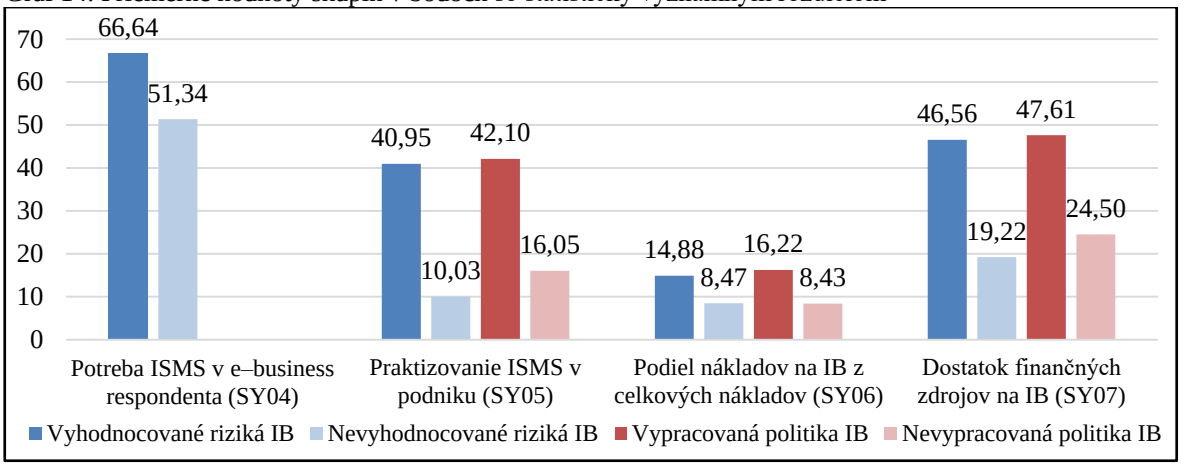
Tab. 28: Testovanie rozdielov premenných SY v závislosti od bezpečnostnej politiky

Premenná		Mann–Whitney U	Z	Asymp. Sig. (2–tailed)
SY05	Praktizovanie ISMS v podniku	462,50	-4,52	0,000
SY06	Podiel nákladov na IB z celkových nákladov	577,50	-3,61	0,000
SY07	Dostatok finančných zdrojov na IB	527,00	-4,00	0,000

Zdroj: vlastné spracovanie

Výsledky potvrdzujú, že to, či podniky majú alebo nemajú vytvorenú politiku IB, sa prejavuje pri praktizovaní ISMS, výške nákladov na IB a pri dostatku finančných zdrojov na IB. Pri ostatných premenných skupiny SY rozdiely nie sú dostatočne veľké, aby boli štatisticky významné ($p > 0,05$).

Graf 14: Priemerné hodnoty skupín v bodoch so štatisticky významným rozdielom



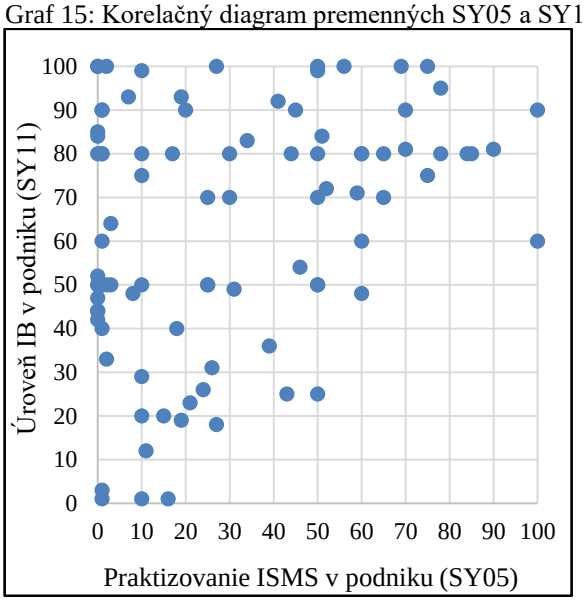
Zdroj: vlastné spracovanie

V grafe 14 uvádzame súhrnný prehľad skúmaných premenných s priemernými hodnotami jednotlivých skupín so štatisticky významným rozdielom. Vyššie priemerné hodnoty premenných sú dosahované v podnikoch, ktoré vyhodnocujú riziká a majú vypracovanú politiku IB. Rozdiely medzi skupinami sú zjavné.

4.3.3 Vplyv praktizovania ISMS na úroveň informačnej bezpečnosti

Lineárnou regresnou analýzou skúmame, či hodnoty premennej praktizovanie ISMS v podniku (SY05) štatisticky významne ovplyvňujú respondentmi stanovenú úroveň IB v podniku (SY11). Vzájomný vzťah premenných sledujeme na grafe 15, kde systematická lineárna závislosť nie je evidentná, ale ani vylúčená.

Graf 15: Korelačný diagram premenných SY05 a SY11



Zdroj: vlastné spracovanie

Výsledky analýzy sa nachádzajú v tabuľke 29. Koeficient korelácie R = 0,33 predstavuje slabý vzájomný vzťah premenných. Koeficient determinácie R^2 = 0,11 vysvetľuje 11 % variability závislej premennej SY11 ovplyvnenej nezávislou premennou SY05. Zvyšných 89 % ovplyvňujú ostatné faktory, napríklad investície do ISMS a bezpečnostných opatrení, bezpečnostné školenia, zakomponovanie požiadaviek IB do podnikových procesov, dodávateľských zmlúv, atď.

Tab. 29: Regresný model závislej premennej SY11 a nezávislej premennej SY05

Model Summary (SY11)			
R	***R Square***	***Adjusted R Square***	***Std. Error of the Estimate***
0,33	0,11	0,10	26,30

ANOVA (SY11)					
	Sum of Squares	***df***	***Mean Square***	***F***	***Sig.***
Regression	7397,66	1	7397,66	10,70	0,002
Residual	61543,95	89	691,51	–	–
Total	68941,60	90	–	–	–

Coefficients (SY11)							
	Unstandardized Coefficients		***Standardized Coefficients***	***t***	***Sig.***	***95% Confidence Interval for B***	
	B	***Std. Error***	***Beta***			***Lower Bound***	***Upper Bound***
(Constant)	53,40	4,01	0,00	13,31	0,000	45,42	61,37
SY11	0,32	0,10	0,33	3,27	0,002	0,12	0,51

Zdroj: vlastné spracovanie

Analýza rozptylu (ANOVA) potvrdzuje štatisticky významný lineárny regresný model s dobrým opisom dát, F(1, 89) = 10,70; p = 0,002. Regresný koeficient b_1 = 0,32 štatisticky významne prispieva k predikcii závislej premennej SY11 (p = 0,002).

Z výsledkov vyvodzujeme, že praktizovanie ISMS v podniku štatisticky významne vplýva na úroveň IB podniku s elektronickým obchodom na hladine významnosti $\alpha = 0,05$.

4.4 Vyhodnotenie významu informačných aktív

Vyhodnotenie významu informačných aktív by malo byť základnou činnosťou analýzy rizík každého podniku. Podniky si uvedomujú hodnotu svojich aktív, pretože práve aktíva im umožňujú podnikať. Z pohľadu podnikov s elektronickým obchodom sme identifikovali 7 podskupín informačných aktív, ktoré sú predmetom skúmania a vstupom do celkovej analýzy rizík IB. Ide o primárne aktíva (obchodné činnosti, zmluvy, know–how, dobré meno, znalosti, osobné údaje, atď.), dáta, hardvér, softvér, sieť, personál a lokalitu. Každá z podskupín obsahuje viacero informačných aktív. Samozrejme, rôzne podniky disponujú rôznymi informačnými aktívami a každému z nich priraďujú iný význam.

Pre získanie uceleného prehľadu reprezentanti podnikov hodnotili význam jednotlivých informačných aktív pre podnik na stupnici od 0 (žiadny význam aktíva) po 100 bodov (maximálny, kritický význam aktíva). Získané dáta z prieskumu ďalej vstupujú do analýzy rizík IB. Najskôr však každý respondentom určený význam informačného aktíva je pretransformovaný na stupnicu analýzy rizík pre hodnotu aktíva z tabuľky 13. Jednotlivé hodnoty informačných aktív na stupnici od 1 (nízka) po 4 (kritická) sa nachádzajú v prílohe 1. V matici môžeme jasne pozorovať, že respondenti využívajú celú šírku stanovenej škály a väčšine informačných aktív priradili dokonca vysokú až kritickú hodnotu.

Vyhodnotenie ukazovateľov, ktoré reprezentujú podskupiny informačných aktív a tiež celú skupinu IA na pôvodnej škále v bodoch, sa nachádza v tabuľke 30. Čiastkové ukazovatele predstavujú priemer a smerodajnú odchýlku všetkých hodnôt premenných, ktoré sa v konkrétnej podskupine nachádzajú. Súhrnný ukazovateľ sme získali vypočítaním aritmetického priemeru a smerodajnej odchýlky z hodnôt čiastkových ukazovateľov.

Tab. 30: Vyhodnotenie ukazovateľov skupiny IA

Súhrnný ukazovateľ		**M**	**SD**
IA	Význam informačných aktív podniku	63,84	9,55
Čiastkový ukazovateľ		**M**	**SD**
IASI	Sieť	72,24	33,16
IAPA	Primárne aktíva	71,72	30,42
IADA	Dáta	68,37	31,20
IAPE	Personál	67,12	36,22
IASO	Softvér	62,01	35,00
IAHA	Hardvér	60,83	34,29
IALO	Lokalita	44,59	36,47

Zdroj: vlastné spracovanie

Celkový význam informačných aktív podnikov s elektronickým obchodom je na úrovni 63,84 % (IA; M = 63,84; SD = 9,55). Pretože hodnota súhrnného ukazovateľa IA presiahla 50 bodov, považujeme ju za vysokú. Podniky si uvedomujú význam a kritickosť svojich informačných aktív. Pretože ukazovateľ v sebe zahŕňa všetky dôležité, aj menej dôležité informačné aktíva, táto úroveň je na slovenské podmienky akceptovateľná.

Spomedzi čiastkových ukazovateľov je podľa priemerného počtu bodov najdôležitejším informačným aktívom sieť podniku (IASI; M = 72,24; SD = 33,16). Sieť je aktívum, ktoré obsahuje internetové pripojenie, prvky počítačovej siete, telekomunikačnú sieť, atď. Podnik prevádzkujúci elektronický obchod nie je bez siete schopný realizovať svoju podnikateľskú činnosť. Vysoká hodnota čiastkového ukazovateľa je preto zmysluplná.

Za sieťou nasledujú primárne aktíva (IAPA; M = 71,72; SD = 30,42), ktorých hodnota je tiež vysoká. Síce po ich strate je možné v podnikateľskej činnosti pokračovať, ale pravdepodobne s veľkými až existenčnými problémami (napr. finančné straty, žaloby, strata konkurencieschopnosti). Ďalej nasledujú dáta (IADA), personál (IAPE), softvér (IASO), hardvér (IAHA) a nakoniec najmenej hodnotná lokalita (IALO). Skúmané podniky neprisudzujú lokalite veľký význam, hodnota čiastkového ukazovateľa je len na strednej úrovni 44,59 % (M = 44,59; SD = 36,47). V rámci podskupiny lokalita sú totiž viaceré relatívne ľahko nahraditeľné informačné aktíva (napr. EZS, CCTV, klimatizácia).

Výsledky deskriptívnej štatistiky skúmaných informačných aktív sa nachádzajú v tabuľke 31. Ako hlavný štatistický nástroj pre určenie poradia významu informačných aktív v skúmaných podnikoch sme vybrali aritmetický priemer (M).

Tab. 31: Deskriptívna štatistika premenných skupiny IA

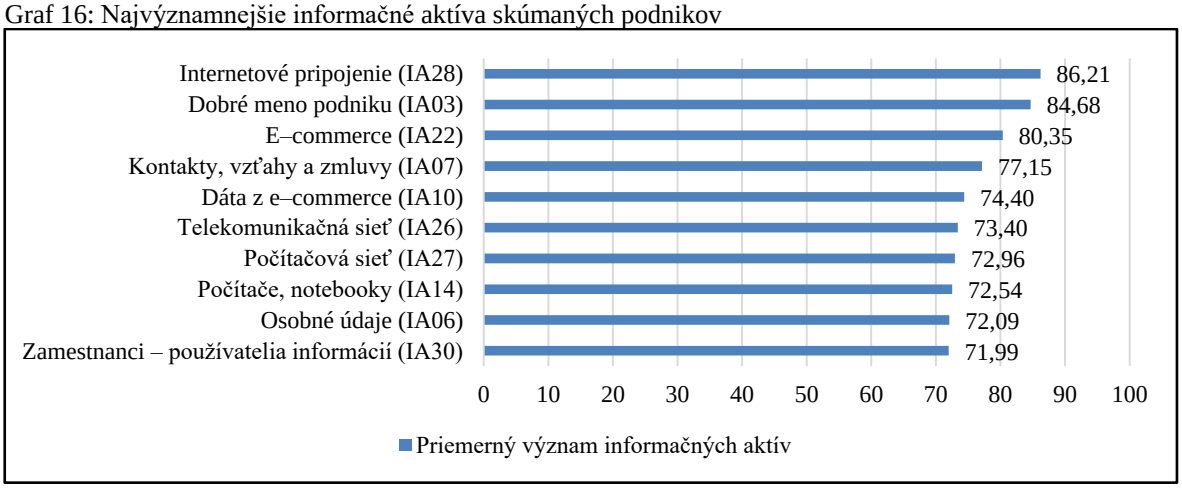
Premenná	N	Min	Max	Variačné rozpätie	Špicatosť	Šikmosť	Modus	Medián	M	SD	Poradie podľa M
IA01	91	0	100	100	-0,40	-0,98	100	80	**70,55**	**31,11**	**13**
IA02	91	2	100	98	-0,89	-0,76	100	80	**70,07**	**32,04**	**14**
IA03	91	3	100	97	3,28	-2,05	100	98	**84,68**	**24,99**	**2**
IA04	91	0	100	100	-0,58	-0,88	100	80	**67,74**	**32,74**	**17**
IA05	91	3	100	97	-0,42	-0,74	100	77	**69,37**	**27,44**	**15**
IA06	91	5	100	95	-0,62	-0,76	100	78	**72,09**	**29,12**	**9**
IA07	91	5	100	96	0,09	-1,05	100	89	**77,15**	**26,71**	**4**
IA08	91	1	100	99	-1,09	-0,49	100	66	**62,12**	**33,96**	**23**
IA09	91	2	100	98	-0,48	-0,85	100	80	**71,16**	**30,28**	**11**
IA10	91	1	100	99	0,14	-1,02	100	81	**74,40**	**28,65**	**5**
IA11	91	0	100	100	-1,25	-0,30	100	60	**59,11**	**33,07**	**26**
IA12	91	0	100	100	-1,06	-0,57	100	80	**68,79**	**31,04**	**16**
IA13	91	0	100	100	-0,86	-0,67	100	80	**67,42**	**34,09**	**18**
IA14	91	2	100	98	-0,22	-0,89	100	80	**72,54**	**29,02**	**8**
IA15	91	0	100	100	-1,10	-0,35	100	62	**60,95**	**31,56**	**24**
IA16	91	0	100	100	-1,32	-0,11	100	55	**53,96**	**34,09**	**30**
IA17	91	0	100	100	-1,51	0,09	100	50	**49,31**	**37,46**	**32**
IA18	91	0	100	100	-1,32	-0,34	100	60	**57,36**	**36,60**	**27**

Premenná	N	Min	Max	Variačné rozpätie	Špicatosť	Šikmosť	Modus	Medián	M	SD	Poradie podľa M
IA19	91	0	100	100	-0,92	-0,49	100	66	**62,65**	**31,87**	**22**
IA20	91	0	100	100	-1,09	-0,46	100	64	**59,70**	**34,73**	**25**
IA21	91	0	100	100	-1,50	-0,29	100	60	**55,51**	**38,96**	**29**
IA22	91	1	100	99	0,76	-1,34	100	95	**80,35**	**27,46**	**3**
IA23	91	0	100	100	-0,41	-0,93	100	84	**70,89**	**33,29**	**12**
IA24	91	0	100	100	-0,98	-0,45	100	69	**62,87**	**31,75**	**20**
IA25	91	0	100	100	-1,37	0,13	100	50	**46,77**	**34,91**	**35**
IA26	91	0	100	100	-0,14	-1,04	100	88	**73,40**	**31,56**	**6**
IA27	91	0	100	100	-0,13	-0,99	100	84	**72,96**	**31,07**	**7**
IA28	91	10	100	90	2,48	-1,77	100	99	**86,21**	**21,71**	**1**
IA29	91	0	100	100	-1,57	-0,29	100	70	**56,42**	**39,38**	**28**
IA30	91	0	100	100	-0,13	-1,11	100	86	**71,99**	**34,05**	**10**
IA31	91	0	100	100	-0,93	-0,78	100	82	**66,68**	**37,40**	**19**
IA32	91	0	100	100	-1,14	-0,63	100	79	**62,68**	**36,93**	**21**
IA33	91	0	100	100	-1,45	-0,01	0	50	**47,98**	**35,97**	**33**
IA34	91	0	100	100	-1,35	0,26	0	38	**43,99**	**34,87**	**37**
IA35	91	0	100	100	-1,56	0,08	100	50	**47,42**	**38,27**	**34**
IA36	91	0	100	100	-1,43	0,23	100	46	**44,53**	**36,66**	**36**
IA37	91	0	100	100	-0,93	0,67	0	20	**33,58**	**34,15**	**38**
IA38	91	0	100	100	-1,54	0,08	100	50	**50,04**	**37,34**	**31**

Zdroj: vlastné spracovanie

Poradie desiatich najvýznamnejších informačných aktív podnikov s elektronickým obchodom sa nachádza na grafe 16. S priemerom M = 86,21 bodov a SD = 21,71 bodov je najvýznamnejším aktívom elektronického podnikania internetové pripojenie (IA28). Ide o vpravo zošikmené rozdelenie (-1,77), ktoré je špicaté s väčšinou hodnôt blízko priemeru (2,48). Bez internetového pripojenia chod elektronického obchodu skutočne nie je možný. Podľa stupnice pre analýzu rizík je toto informačné aktívum priemerne až na kritickej úrovni. Respondenti najčastejšie uvádzali hodnotu 100 bodov, medián predstavuje 99 bodov. Až 75 % respondentov ohodnotilo internetové pripojenie viac ako 78,50 bodmi. Menej ako 51 bodov vrátane uviedlo len 10 % respondentov.

Graf 16: Najvýznamnejšie informačné aktíva skúmaných podnikov



Zdroj: vlastné spracovanie

Druhé v poradí je dobré meno podniku (IA03), čiže reputácia alebo hodnota značky (M = 84,68; SD = 24,99). Akonáhle podnik príde o svoje dobré meno, napríklad v dôsledku úniku osobných údajov, v momente ich zverejnenia zákazníci okamžite prestanú tento elektronický obchod využívať, čo môže viesť až k existenčným následkom pre podnik. Dáta sú špicaté (3,28), vpravo zošikmené (-2,05). Najčastejšou hodnotou je 100 bodov s mediánom 98 bodov. Význam tohto informačného aktíva je kritický. 75 % respondentov hodnotí význam aktíva viac ako 80,50 bodmi.

Dobré meno podniku prekvapivo predbehlo tretie najvýznamnejšie aktívum, samotný systém elektronického obchodu (IA22), napr. webové stránky, aplikácia, CMS, CRM (M = 80,35; SD = 27,46), ktorý je nevyhnutný, čiže kritický pre elektronické podnikanie. Dáta sú skôr špicatejšie (0,76), zošikmené k vysokým hodnotám (-1,34), s modusom 100 bodov a mediánom 95 bodov. 90 % všetkých hodnotení je viac ako 44 bodov. 25% hodnôt sa nachádza v intervale od 0 po 63 bodov.

Kritickú úroveň, v priemere nad 75 bodov, uzatvára aktívum kľúčových kontaktov, vzťahov a zmlúv (IA07), ktoré respondenti ohodnotili v priemere na 77,15 % (M = 77,15; SD = 26,71), čím sa umiestnilo na štvrtom mieste v poradí. Bez dobrých a stabilných partnerských a dodávateľsko–odberateľských vzťahov, zmlúv a kontaktov je podnikanie problematické v každom odvetví. Preto si toto informačné aktívum podniky s elektronickým obchodom obzvlášť cenia. 50 % hodnôt premennej je viac alebo menej ako 89 bodov, zatiaľ čo najčastejšia hodnota predstavuje 100 bodov. 25% všetkých hodnôt sa nachádza v intervale od 0 po 63,50 bodov. Dáta sú veľmi mierne špicaté (0,09) a skôr vpravo zošikmené (-1,05).

Ostatné skúmané informačné aktíva dosiahli v priemere menšiu ako kritickú úroveň. Prvých desať najvýznamnejších informačných aktív uzatvárajú dáta z elektronického obchodu (IA10; M = 74,40; SD = 28,65), telekomunikačná sieť (IA26; M = 73,40; SD = 31,56), počítačová sieť, čiže kabeláž a aktívne prvky (IA27; M = 72,96; SD = 31,07), pracovné stanice, tzn. počítače a notebooky (IA14; M = 72,54; SD = 29,02), osobné údaje (IA06; M = 72,09; SD = 29,12) a zamestnanci, ktorí pracujú s informáciami (IA30; M = 71,99; SD = 34,05).

Na druhej strane, najmenej významnými aktívami sú UPS záložné zdroje (IA17; M = 49,31; SD = 37,46), okolie podniku, tzn. mestská alebo obecná oblasť (IA33; M = 47,98; SD = 35,97), bezpečnostné zóny, napr. archív, serverovňa (IA35; M = 47,42; SD = 38,27), aplikácie mobilných zariadení (IA25; M = 46,77; SD = 34,91), zabezpečovací systém, tzn. EZS, EPS, CCTV a iné (IA36; M = 44,53; SD = 36,66), areály a budovy podniku (IA34;

M = 43,99; SD = 34,87) a klimatizácia (IA37; M = 33,58; SD = 34,15). Tieto informačné aktíva nemajú priamy vplyv na elektronické podnikanie, prípadne sú ľahko nahraditeľné. Z týchto dôvodov majú v prieskume najnižšie priemerné hodnoty. Zaujímavosťou sú nízke hodnoty aplikácií mobilných zariadení, ktoré sú v dnešnej dobe často využívané na podporu podnikania. Podniky si uvedomujú, že tieto aplikácie nie sú významné, v prípade straty je možné ich ľahko nahradiť a v prípade nedostupnosti sú k dispozícii funkčnosťou podobné, konkurenčné aplikácie. Aplikácie mobilných zariadení nemajú kritický vplyv na elektronické podnikanie.

Podniky s elektronickým obchodom sú schopné vyhodnotiť a identifikovať kritické informačné aktíva, ktorých strata, narušenie, poškodenie, či pozastavenie funkčnosti môže viesť k prerušeniu podnikateľskej činnosti a tým k poklesu počtu objednávok, zvýšeným nákladom, strate zákazníkov a i. Celkovo, 4 aktíva majú v priemere kritickú hodnotu, až 27 aktív vysokú a 7 aktív strednú hodnotu. Ani jedno informačné aktívum nemá v priemere nízku hodnotu. To znamená, že skúmané podniky si uvedomujú hodnotu svojich informačných aktív.

4.5 Vyhodnotenie hrozieb informačnej bezpečnosti

Ďalším krokom rizikovej analýzy v rámci dizertačnej práce je vyhodnotenie pravdepodobnosti výskytu hrozieb informačnej bezpečnosti v skúmaných podnikoch. Hrozby pôsobia na informačné aktíva podniku z vonkajšieho alebo vnútorného prostredia. Realizácia hrozby sa stáva bezpečnostným incidentom, ktorý zanecháva na aktívach rôzne následky v závislosti od existujúcich opatrení. Vyplývajúc z normy ISO/IEC 27005 sme prispôsobením na podniky, ktoré podnikajú na elektronickom trhu, identifikovali 9 podskupín hrozieb v rámci skupiny premenných HR. Sú to hrozby fyzického poškodenia zariadení alebo médií, straty základných služieb, úniku informácií, technického zlyhania, neautorizovaných činností, poškodenia funkcií, počítačovej kriminality, priemyselnej špionáže a interné hrozby.

Každá z týchto podskupín obsahuje niekoľko konkrétnych hrozieb IB, ktoré sú realizovateľné v podnikoch s elektronickým obchodom a ktorým skúmané podniky určovali pravdepodobnosť výskytu v ich podniku na škále od 0 bodov (nepravdepodobný výskyt hrozby) po 100 bodov (istý výskyt hrozby). Štatistickú analýzu uskutočňujeme s využitím tejto škály, avšak pre účely rizikovej analýzy boli získané dáta prispôsobené stupnici pre hodnotu hrozby z tabuľky 13. Hodnoty hrozieb IB v jednotlivých podnikoch sa nachádzajú v prílohe 2. Ako môžeme vidieť, väčšina hrozieb bola hodnotená ako nepravdepodobná. Iba

veľmi malá časť hrozieb je iná než nepravdepodobná. Môžeme teda tvrdiť, že väčšina podnikov sa hrozieb IB neobáva.

Celkové výsledky skupiny HR sú uvedené v tabuľke 32. Súhrnný ukazovateľ pozostáva z aritmetického priemeru a smerodajnej odchýlky z hodnôt čiastkových ukazovateľov. Čiastkové ukazovatele sú priemerom a smerodajnou odchýlkou hodnôt všetkých premenných v konkrétnej podskupine hrozieb IB.

Tab. 32: Vyhodnotenie ukazovateľov skupiny HR

Súhrnný ukazovateľ		**M**	**SD**
HR	Pravdepodobnosť výskytu hrozieb IB	16,10	5,88
Čiastkový ukazovateľ		**M**	**SD**
HRTZ	Technické zlyhanie	25,21	24,52
HRSZ	Strata základných služieb	23,79	25,26
HRPF	Poškodenie funkcií	20,48	22,79
HRUI	Únik informácií	16,00	21,91
HRPK	Počítačová kriminalita	15,57	21,27
HRFP	Fyzické poškodenie zariadení alebo médií	12,78	17,07
HRNC	Neautorizované činnosti	12,16	17,36
HRPS	Priemyselná špionáž	9,80	15,91
HRIH	Interné hrozby	9,09	16,63

Zdroj: vlastné spracovanie

Pravdepodobnosti výskytu hrozieb IB sú podľa súhrnného ukazovateľa HR hodnotené na úrovni M = 16,10 bodov; SD = 5,88 bodov. Ako sme uviedli vyššie, výsledky potvrdzujú, že podniky s elektronickým obchodom celkovo vnímajú hrozby IB ako skôr nepravdepodobné, čo v konečnom dôsledku môže spôsobiť podcenenie hrozieb IB.

Hrozby technického zlyhania (HRTZ), napr. porucha zariadenia, softvérová porucha, saturácia IS, sú hodnotené na úrovni M = 25,21 bodov; SD = 24,52 bodov. Podniky tieto hrozby vnímajú ako málo pravdepodobné. Všetky ostatné čiastkové ukazovatele reprezentujú nepravdepodobné hrozby pre podniky. Po technických zlyhaniach nasledujú hrozby straty základných služieb (HRSZ), ďalej hrozby poškodenia funkcií systémov a softvérov (HRPF), úniku informácií (HRUI), počítačovej kriminality (HRPK), fyzického poškodenia zariadení alebo médií (HRFP), neautorizovaných činností (HRNC) a priemyselnej špionáže (HRPS). Najmenej pravdepodobnou podskupinou sú interné hrozby (HRIH; M = 9,09; SD = 16,63). Podniky svojim súčasným alebo bývalým zamestnancom dôverujú. To znamená, že útok na informačné aktíva z interného prostredia podniku skoro vôbec neočakávajú.

V nasledujúcej tabuľke uvádzame výsledky opisnej štatistiky hodnôt premenných, ktoré merali pravdepodobnosti výskytu jednotlivých hrozieb v podnikoch s aktívnym

podnikaním na slovenskom elektronickom trhu. Štatistickým nástrojom pre určenie poradia premenných je opäť aritmetický priemer (M).

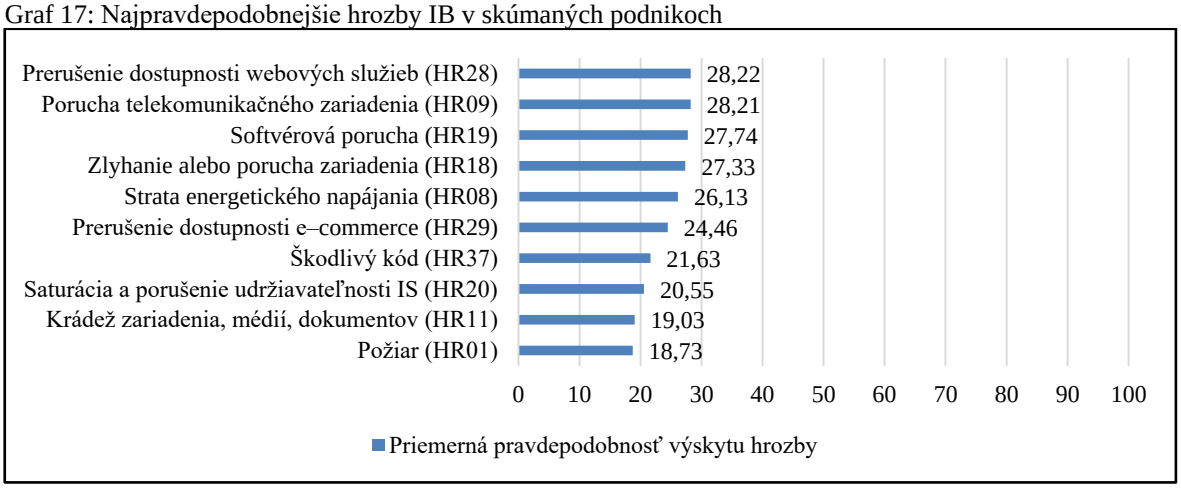
Tab. 33: Deskriptívna štatistika premenných skupiny HR

Premenná	N	Min	Max	Variačné rozpätie	Špicatosť	Šikmosť	Modus	Medián	M	SD	Poradie podľa M
HR01	91	0	69	69	-0,44	0,93	10	11	**18,73**	**18,55**	**10**
HR02	91	0	67	67	1,46	1,59	2	5	**13,07**	**16,92**	**29**
HR03	91	0	87	87	2,34	1,63	1	7	**14,64**	**17,98**	**22**
HR04	91	0	82	82	2,84	1,88	1	5	**12,22**	**17,81**	**31**
HR05	91	0	50	50	2,03	1,79	0	5	**10,31**	**14,75**	**39**
HR06	91	0	71	71	6,25	2,59	0	2	**7,74**	**14,28**	**45**
HR07	91	0	100	100	2,14	1,54	0	10	**17,02**	**20,71**	**14**
HR08	91	0	99	99	0,16	1,00	2	17	**26,13**	**25,99**	**5**
HR09	91	0	100	100	0,22	0,99	50	20	**28,21**	**27,56**	**2**
HR10	91	0	100	100	5,12	2,18	0	5	**13,34**	**19,40**	**26**
HR11	91	0	100	100	1,05	1,17	0	10	**19,03**	**20,95**	**9**
HR12	91	0	59	59	2,48	1,84	0	3	**9,90**	**14,55**	**41**
HR13	91	0	100	100	2,39	1,70	0	7	**18,71**	**25,09**	**11**
HR14	91	0	100	100	3,85	1,96	0	6	**16,68**	**23,18**	**16**
HR15	91	0	100	100	5,20	2,17	0	6	**15,11**	**21,06**	**21**
HR16	91	0	100	100	3,95	2,02	0	7	**16,98**	**23,59**	**15**
HR17	91	0	100	100	2,48	1,71	0	6	**18,27**	**24,87**	**12**
HR18	91	0	100	100	0,15	0,99	20	20	**27,33**	**25,57**	**4**
HR19	91	0	100	100	0,51	1,05	5	21	**27,74**	**25,11**	**3**
HR20	91	0	100	100	1,66	1,36	0	11	**20,55**	**22,36**	**8**
HR21	91	0	68	68	2,58	1,82	0	3	**11,45**	**16,39**	**36**
HR22	91	0	63	63	2,81	1,85	0	3	**10,74**	**15,14**	**38**
HR23	91	0	71	71	2,50	1,84	0	3	**11,23**	**17,05**	**37**
HR24	91	0	71	71	0,83	1,35	0	8	**15,36**	**18,17**	**19**
HR25	91	0	100	100	5,51	2,34	0	3	**12,04**	**19,69**	**33**
HR26	91	0	83	83	1,32	1,35	0	10	**15,97**	**17,90**	**17**
HR27	91	0	67	67	1,16	1,47	0	7	**13,26**	**16,54**	**27**
HR28	91	0	100	100	0,40	1,10	5	20	**28,22**	**26,13**	**1**
HR29	91	0	99	99	0,84	1,25	10	13	**24,46**	**25,84**	**6**
HR30	91	0	100	100	3,77	1,95	0	5	**14,56**	**20,47**	**23**
HR31	91	0	100	100	3,72	2,01	0	6	**17,14**	**24,24**	**13**
HR32	91	0	100	100	3,05	1,71	0	6	**15,43**	**19,84**	**18**
HR33	91	0	100	100	4,55	2,02	0	4	**13,13**	**19,08**	**28**
HR34	91	0	100	100	3,92	2,00	0	5	**13,62**	**20,11**	**25**
HR35	91	0	100	100	4,27	2,09	0	5	**13,81**	**20,41**	**24**
HR36	91	0	100	100	2,55	1,63	0	6	**15,26**	**20,32**	**20**
HR37	91	0	100	100	0,83	1,24	0	10	**21,63**	**24,51**	**7**
HR38	91	0	73	73	1,84	1,69	0	4	**12,21**	**17,79**	**32**
HR39	91	0	51	51	0,76	1,43	0	4	**11,58**	**15,62**	**35**
HR40	91	0	90	90	5,88	2,32	0	2	**10,08**	**16,84**	**40**
HR41	91	0	67	67	9,28	3,11	0	1	**6,05**	**12,99**	**49**
HR42	91	0	71	71	4,31	2,25	0	2	**9,09**	**15,51**	**43**
HR43	91	0	90	90	5,52	2,41	0	2	**9,78**	**18,28**	**42**
HR44	91	0	62	62	7,26	2,75	0	1	**6,46**	**12,70**	**48**
HR45	91	0	100	100	3,32	2,00	0	2	**12,71**	**21,79**	**30**
HR46	91	0	100	100	5,07	2,21	0	2	**11,80**	**19,63**	**34**
HR47	91	0	61	61	4,18	2,19	0	2	**7,54**	**13,07**	**46**
HR48	91	0	63	63	4,88	2,34	0	1	**7,26**	**13,56**	**47**
HR49	91	0	57	57	3,27	2,12	0	2	**8,04**	**14,46**	**44**

Zdroj: vlastné spracovanie

Najviac pravdepodobnou hrozbou IB je prerušenie dostupnosti webových služieb (HR28), konkrétne internet, e–mail, cloud, webové stránky a iné služby (M = 28,22; SD = 26,13). Skúmané podniky jej výskyt považujú za málo pravdepodobný. Zároveň, táto hrozba môže mať pre podniky vážne až existenčné následky, pretože jej uskutočnenie zabraňuje hlavnej činnosti elektronického podnikania. Najčastejšou hodnotou je 5 bodov a 50 % respondentov odhadlo úroveň výskytu hrozby na viac alebo menej ako 20 bodov. Ide skôr o špicatejšie (0,40), vľavo zošikmené (1,10) rozdelenie dát. Iba 25 % zo všetkých hodnôt je väčších ako 44 bodov. 90 % hodnôt sa zmestí do 69 bodov. Poradie desiatich najpravdepodobnejších hrozieb IB elektronického podnikania sledujeme v grafe 17.

Graf 17: Najpravdepodobnejšie hrozby IB v skúmaných podnikoch



Zdroj: vlastné spracovanie

Druhou najpravdepodobnejšou hrozbou IB je porucha telekomunikačného zariadenia (HR09) s priemerom M = 28,21 bodov a smerodajnou odchýlkou SD = 27,56 bodov. Jej výskyt je v podnikoch málo pravdepodobný. Najčastejšie vyskytujúcou sa hodnotou je 50 bodov, medián predstavuje 20 bodov. Rozdelenie dát je skôr špicaté (0,22) a má viac menších hodnôt podľa šikmosti (0,99). 90 % hodnôt je v intervale do 65 bodov. Poruchy telekomunikačných zariadení môžu viesť k nepriaznivým dopadom na podnikanie, pretože úzko súvisia s internetovým pripojením.

Medzi málo pravdepodobné hrozby môžeme zaradiť aj softvérové poruchy (HR19; M = 27,74; SD = 25,11), zlyhania a poruchy zariadení (HR18; M = 27,33; SD = 25,57) a stratu energetického napájania (HR08; M = 26,13; SD = 25,99). Podľa výsledkov opisnej štatistiky považujeme ostatné hrozby za skôr nepravdepodobné v elektronickom podnikaní. Prvých desať hrozieb podľa pravdepodobnosti výskytu uzatvárajú prerušenie dostupnosti elektronického obchodu (HR29; M = 24,46; SD = 25,84), škodlivý kód (HR37; M = 21,63; SD = 24,51), saturácia a porušenie udržiavateľnosti

informačného systému (HR20; M = 20,55; SD = 22,36), krádež zariadení, médií, dokumentov (HR11; M = 19,03; SD = 20,95) a požiar (HR01; M = 18,73; SD = 18,55). Všetky uvedené hrozby sú v elektronickom podnikaní uskutočniteľné a záleží na podniku, ako sa vysporiada s rizikom, ktoré vznikne pôsobením jednotlivých hrozieb na informačné aktíva. Pretože podnikmi identifikované najpravdepodobnejšie hrozby priamo súvisia s elektronickým podnikaním, tvrdíme, že sú zároveň tie, ktorých sa podniky najviac obávajú a teda môžu spôsobiť najväčšie následky na podnikoch s elektronickým obchodom.

Na druhej strane, medzi najmenej pravdepodobné hrozby v elektronickom podnikaní radíme elektromagnetickú radiáciu a impulzy (HR05; M = 7,74; SD = 14,28), podplácanie (HR47; M = 7,54; SD = 13,07), predaj dôverných a osobných údajov (HR48; M = 7,26; SD = 13,56), útok na zamestnanca (HR44; M = 6,46; SD = 12,70) a politické vydieranie (HR41; M = 6,05; SD = 12,99). Zaujímavosťou je, že skúmané podniky nevnímajú súčasné, moderné hrozby IB ako pravdepodobné. Ide najmä o útoky na dostupnosť systému (DoS, DDoS) na 20. pozícii (HR36; M = 15,26; SD = 20,32), sociálne inžinierstvo (napr. phishing, pharming) na 23. pozícii (HR30; M = 14,56; SD = 20,47), botnety na 24. pozícii (HR35; M = 13,81; SD = 20,41) a cielené a pretrvávajúce hekerské útoky na konkrétny cieľ (APT) na 43. pozícii (HR42; M = 9,09;SD = 15,51). Odôvodňujeme to tým, že podniky daným hrozbám dostatočne nerozumejú, chýba im základný prehľad.

Podľa výsledkov ohodnotenia pravdepodobnosti výskytu hrozieb IB v podnikoch s elektronickým obchodom vyplýva, že podniky buď nedostatočne doceňujú závažnosť skúmaných hrozieb alebo hrozby skutočne nie sú reálne a pravdepodobné v skúmaných podnikoch. Avšak, ak berieme v úvahu výsledky z podkapitoly, ktorá analyzovala ISMS, najmä úroveň IB len na dostačujúcej úrovni, veľkú časť podnikov, ktorá nevykonáva žiadnu činnosť ISMS (13 %) alebo len začína vytvárať ISMS (41 %), nemá vytvorenú politiku IB (46,15 %) a nevyhodnocuje riziká IB (35,16 %), prikláňame sa k tvrdeniu, že podniky nevedia náležite oceniť výskyt hrozieb a teda nie sú si vedomé ich závažnosti a skúmané hrozby poznajú na nedostatočnej úrovni.

4.6 Vyhodnotenie hrozieb smerujúcich na zraniteľnosti personálu

Zamestnancov podnikov s elektronickým obchodom považujeme za najkritickejšiu súčasť manažmentu informačnej bezpečnosti. Mnohí zamestnanci v rámci výkonu povolania pracujú s dôvernými a citlivými informáciami a inými informačnými aktívami, za ktoré nesú určitú zodpovednosť. Túto zodpovednosť si častokrát nedostatočne uvedomujú, prípadne ju neberú dostatočne vážne. V krajnom prípade im chýba vedomosť, že informačné aktíva,

s ktorými pracujú, sú dôverné a z tohto dôvodu musia byť chránené. Takýto personál je ľahkou korisťou útočníka prostredníctvom hrozieb, ktoré zneužívajú jeho zraniteľnosti, napríklad nepozornosť, nevedomosť, neskúsenosť, charakter, nestabilitu, dôverčivosť, vzťahy, nespokojnosť, únavu, atď. Úlohou každého podniku je, aby poskytol svojim zamestnancom adekvátne vzdelanie k ochrane informačných aktív, pridelil prístupy len k tým aktívam, ktoré skutočne k pracovnému výkonu potrebujú, vytvoril primerané pracovné zmluvy, napríklad s dodatkom o mlčanlivosti, a vysvetlil význam informačných aktív podniku.

V tabuľke 34 sa nachádza vyhodnotenie pravdepodobností výskytu hrozieb IB, ktoré smerujú na zraniteľnosti personálu. Tieto hrozby môžu pochádzať z interného alebo externého prostredia podniku a zdrojom môže byť samotný zamestnanec alebo iný útočník.

Tab. 34: Vyhodnotenie hrozieb smerujúcich na zraniteľnosti personálu

Hrozba	Popis	Skupina	Celkové poradie	Modus	Medián	90. percentil	M	SD
HR11	Krádež zariadenia, médií, dokumentov	HRUI	9	0	10	50	**19,03**	**20,95**
HR13	Prezradenie dôvern. dát, obch. tajomstva	HRUI	11	0	7	51	**18,71**	**25,09**
HR17	Manipulácia so zdrojovými kódmi	HRUI	12	0	6	35	**18,27**	**24,87**
HR31	Nežiadúci obsah (defacement, spam)	HRPK	13	0	6	49	**17,14**	**24,24**
HR16	Manipulácia s hardvérom	HRUI	15	0	7	49	**16,98**	**23,59**
HR14	Prezradenie osobných dát	HRUI	16	0	6	50	**16,68**	**23,18**
HR24	Poškodenie dát	HRNC	19	0	8	47	**15,36**	**18,17**
HR15	Údaje z nedôveryhodných zdrojov	HRUI	21	0	6	45	**15,11**	**21,06**
HR30	Sociálne inžinierstvo (phishing a i.)	HRPK	23	0	5	47	**14,56**	**20,47**
HR34	Nelegálne konanie (zmena osob. údajov)	HRPK	25	0	5	46	**13,62**	**20,11**
HR10	Vzdialené špehovanie, odpočúvanie	HRUI	26	0	5	39	**13,34**	**19,40**
HR45	Prezeranie dôverných informácií	HRIH	30	0	2	48	**12,71**	**21,79**
HR38	Krádež informácií a dát	HRPS	32	0	4	45	**12,21**	**17,79**
HR25	Falšovanie a nelegálne spracovanie dát	HRNC	33	0	3	38	**12,04**	**19,69**
HR46	Podvod	HRIH	34	0	2	44	**11,80**	**19,63**
HR39	Zásah do súkromia	HRPS	35	0	4	41	**11,58**	**15,62**
HR21	Neautoriz. použitie zariadenia a softvéru	HRNC	36	0	3	41	**11,45**	**16,39**
HR23	Použitie falošného, kopírov. softvéru	HRNC	37	0	3	48	**11,23**	**17,05**
HR22	Nelegálne kopírovanie systému, softvéru	HRNC	38	0	3	31	**10,74**	**15,14**
HR12	Vyhľadávanie vyradených, recykl. médií	HRUI	41	0	3	35	**9,90**	**14,55**
HR43	Vydieranie bývalým zamestnancom	HRIH	42	0	2	39	**9,78**	**18,28**
HR42	Cielené hekerské útoky (APT)	HRPS	43	0	2	40	**9,09**	**15,51**
HR49	Sabotáž systému alebo zariadení	HRIH	44	0	2	36	**8,04**	**14,46**
HR47	Podplácanie	HRIH	46	0	2	30	**7,54**	**13,07**
HR48	Predaj dôverných a osobných údajov	HRIH	47	0	1	27	**7,26**	**13,56**
HR44	Útok na zamestnanca	HRIH	48	0	1	20	**6,46**	**12,70**

Zdroj: vlastné spracovanie

Podľa priemerného počtu bodov môžeme usúdiť, že v elektronickom podnikaní sú všetky uvedené hrozby skôr nepravdepodobné. Respondenti pridelili v priemere najvyššie pravdepodobnosti úniku informácií, konkrétne krádeži zariadení, médií alebo dokumentov (HR11; M = 19,03; SD = 20,95), prezradeniu dôverných dát a obchodného tajomstva (HR13;

M = 18,71; SD = 25,09) a manipulácii so zdrojovými kódmi (HR17; M = 18,27; SD = 24,87). Na druhej strane hrozby, ktoré podniky vnímajú ako najmenej pravdepodobné, sú interné hrozby, predovšetkým sabotáž systému alebo zariadení (HR49; M = 8,04; SD = 14,46), podplácanie (HR47; M = 7,54; SD = 13,07), predaj dôverných a osobných údajov (HR48; M = 7,25; SD = 13,56) a útok na zamestnanca (HR44; M = 6,46; SD = 12,70).

To, že podniky s elektronickým obchodom vnímajú hrozby personálu ako nepravdepodobné znamená, že podniky nepredpokladajú ich realizáciu. Údaje ale nevysvetľujú, či podniky sú alebo nie sú pripravené na realizáciu daných hrozieb, čo je skôr doménou implementovaných bezpečnostných opatrení. S nárastom využívania IKT v rôznych oblastiach elektronického podnikania spolu s novými, sofistikovanými hrozbami IB predpokladáme aj nárast hrozieb smerujúcich na zamestnancov, ktorí patria medzi najzraniteľnejšie informačné aktíva podniku.

4.7 Vyhodnotenie úrovne rizík informačnej bezpečnosti

Pre účely dosiahnutia čiastkového cieľa dizertačnej práce, sme jednotlivé úrovne (miery) rizík informačnej bezpečnosti v elektronickom podnikaní vyhodnotili na základe stanovenej metódy vynásobením významov informačných aktív a pravdepodobností výskytu hrozieb IB prispôsobených na škálu od 1 po 4. Metóda je v súlade s vnímaním rizika v rámci výskumu dizertačnej práce ako kombinácia pravdepodobnosti výskytu hrozby s hodnotou aktíva, na ktoré daná hrozba pôsobí. Na vytvorenie analýzy rizík IB v skúmaných podnikoch sme v matici miery rizika vypočítali aritmetické priemery získaných mier rizík jednotlivých respondentov, ktoré sme následne kvalitatívne ohodnotili podľa intervalov v tabuľke 13. Identifikovaným rizikám sme určili poradie podľa ich závažnosti. Výslednú maticu priemerných mier rizík IB v elektronickom podnikaní uvádzame v prílohe 3.

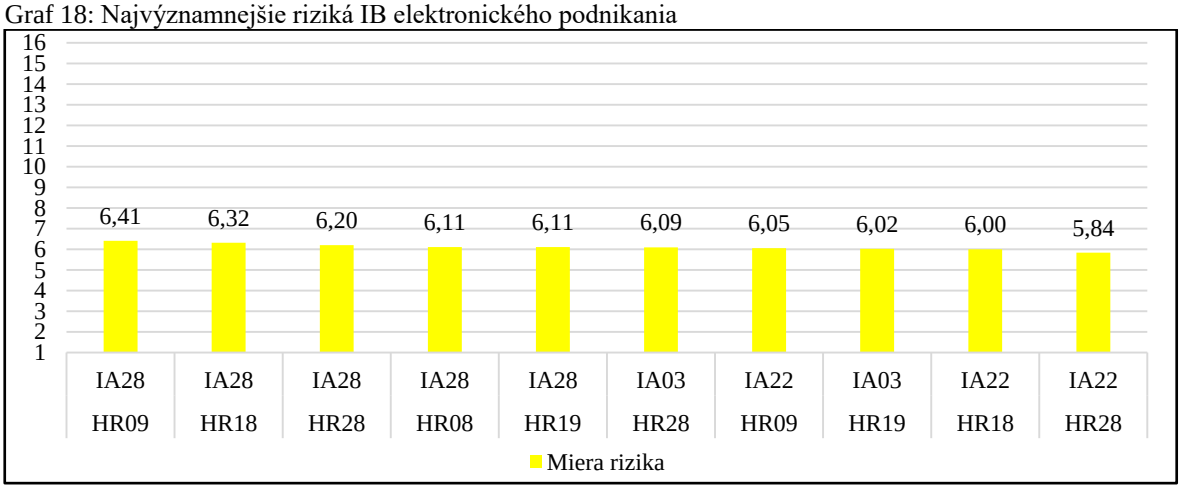
Z maximálneho počtu 1862 rizík sme identifikovali 1180 možných rizík IB v podnikoch s elektronickým obchodom. Zvyšných 682 kombinácií hrozieb IB a informačných aktív sme vylúčili z dôvodu neexistencie vplyvu konkrétnej hrozby na dané informačné aktívum. Zo všetkých identifikovaných rizík až 696 (59 %) je na nízkej úrovni s priemerom M = 3,45 bodov; SD = 0,37 bodov. 484 mier rizík (41 %) sa nachádza na strednej úrovni závažnosti s priemerom M = 4,53 bodov; SD = 0,50 bodov. Ani jedno riziko s vysokou alebo kritickou mierou nebolo identifikované. Tento stav je predovšetkým spôsobený nízkymi hodnoteniami pravdepodobností výskytu hrozieb IB respondentmi, ktoré značne znižujú priemerné miery rizík IB. Opäť môžeme konštatovať, že podnikom chýbajú skúsenosti a znalosti o hrozbách IB na to, aby kritickejšie hodnotili pravdepodobnosti ich

výskytu v elektronickom podnikaní. Podľa nášho názoru je celková závažnosť hrozieb IB a tým aj rizík IB v skutočnosti na vyššej úrovni ako v priemere uvádzajú respondenti. Na druhej strane potvrdzujeme a rešpektujeme, že respondenti citlivo reflektujú aktuálny stav ISMS v elektronickom podnikaní so všetkými svojimi limitmi.

Matica priemerných mier rizík ukazuje, že riziká IB v elektronickom podnikaní na slovenskom elektronickom trhu sa nachádzajú minimálne na nízkej a maximálne na strednej úrovni. Ak by boli identifikované kritické alebo vysoké riziká, mohli by sme pre tieto riziká nastaviť plán ošetrenia rizík a zároveň ho aplikovať na celé odvetvie elektronického podnikania. Pretože nízke a stredné úrovne priemerných rizík nie sú svojou závažnosťou a následkami významné pre elektronické podnikanie, plán ošetrenia rizík pre celé odvetvie nie je nutný. Každý podnik, ktorý prevádzkuje elektronický obchod, by si mal nastaviť individuálny plán podľa vlastnej analýzy rizík.

Skúmané riziká IB priorizujeme usporiadaním podľa získaných mier rizík. Vzhľadom na veľké množstvo identifikovaných rizík, z ktorých žiadne nie sú kritické ani vysoké, pozornosť venujeme desiatim najvýznamnejším rizikám elektronického podnikania, teda kombináciám informačných aktív a hrozieb IB (pozri graf 18). Všetky uvedené riziká sa nachádzajú na strednej úrovni podľa stupnice miery rizika.

Graf 18: Najvýznamnejšie riziká IB elektronického podnikania



Zdroj: vlastné spracovanie

Riziko, ktoré najviac ohrozuje informačnú bezpečnosť elektronického podnikania, kombinuje hrozbu poruchy telekomunikačného zariadenia (HR09) s internetovým pripojením (IA28) na úrovni 6,41 bodov z maximálnych 16 bodov. Akýkoľvek spôsob elektronického podnikania skutočne závisí od internetového pripojenia. Jeho výpadok môže mať pre podnik až existenčné následky. Existuje niekoľko spôsobov ako toto riziko minimalizovať, napríklad zabezpečením záložného internetového pripojenia iným poskytovateľom internetových služieb, nákup náhradného telekomunikačného zariadenia,

prípadne dohoda o úrovni služieb (SLA) uzatvorená s poskytovateľom internetu. V krajnom prípade môžu podniky riziko akceptovať, avšak s plným vedomím možných následkov.

To, že internetové pripojenie (IA28) je kritické aktívum elektronického podnikania, vidíme podľa prvých piatich rizík IB. Riziká ďalej v poradí ohrozujú internetové pripojenie zlyhaním alebo poruchou zariadenia (HR18), prerušením dostupnosti služieb ako sú e–mail, internet, web a cloud (HR28), stratou energetického napájania (HR08) alebo softvérovou poruchou (HR19). Prvé dve hrozby možno ošetriť rovnakým spôsobom ako pri najväčšom riziku. Stratu energetického napájania možno vyriešiť alternatívnymi zdrojmi energie, prípadne vhodným použitím záložných zdrojov UPS. Softvérovej poruche možno predísť pravidelnou aktualizáciou a kontrolou nastavení.

Šieste riziko v poradí vzniká vplyvom prerušenia dostupnosti webových služieb (HR28) na reputáciu podniku (IA03). Ak elektronický obchod nie je v prevádzke, zákazníci jednoducho začnú nakupovať u konkurencie. Zákazníci v prípade dlhšieho výpadku považujú elektronický obchod za nespoľahlivý a nedôveryhodný. Dostupnosť webových služieb je pre elektronické podnikanie kľúčová, preto je zásadné zabezpečiť adekvátne dohody o úrovni služieb s jednotlivými poskytovateľmi, či už internetového pripojenia, systému elektronického obchodu alebo iných webových služieb.

Ďalej nasleduje riziko ohrozenia samotného systému elektronického obchodu, napr. webových stránok, aplikácie, CMS alebo CRM (IA22) poruchou telekomunikačného zariadenia (HR09), riziko straty dobrého mena podniku (IA03) softvérovou poruchou (HR19) a opäť riziko ohrozenia elektronického obchodu (IA22) zlyhaním, prípadne poruchou zariadenia (HR18) alebo prerušením dostupnosti webových služieb (HR28). Miery rizík IB možno pre príslušné riziká znížiť vhodným využitím všetkých vyššie uvedených opatrení. Skúmané riziká sú skutočne realizovateľné v prostredí podnikov s elektronickým obchodom. Najvýznamnejšie riziká smerujú hlavne na tri informačné aktíva, internetové pripojenie, reputáciu podniku a systém elektronického obchodu.

4.8 Vyhodnotenie bezpečnostných opatrení

Po vyhodnotení mier rizík informačnej bezpečnosti a identifikovaní najvýznamnejších rizík informačnej bezpečnosti v elektronickom podnikaní môžeme prejsť k analýze a vyhodnoteniu bezpečnostných opatrení v skúmaných podnikoch. Podľa výsledkov mier rizík IB, významných informačných aktív, pravdepodobných hrozieb a existujúcich opatrení IB navrhujeme skupiny primeraných opatrení pre podniky s elektronickým obchodom podľa ich veľkosti.

4.8.1 Analýza existujúcich bezpečnostných opatrení

Bezpečnostné opatrenia sme pre účely prehľadného prieskumu a z dôvodu jednoznačnosti a spoločných znakov kategorizovali na organizačné a technické opatrenia. Organizačné opatrenia majú skôr strategickú a taktickú povahu, zvyšujú úroveň IB z dlhodobého hľadiska a zavádzajú, udržiavajú, monitorujú a zdokonaľujú ISMS. Technické opatrenia zabezpečujú operatívne činnosti IB, čiže priamo zmenšujú a eliminujú konkrétne riziká IB, bezpečnostné incidenty a udalosti. Pre elektronické podnikanie sme v organizačných opatreniach identifikovali 17 opatrení a v technických až 38 rôznych opatrení IB. V prieskume respondenti uvádzali úroveň využívania opatrenia na stupnici od 0 (opatrenie nie je zavedené) po 100 bodov (opatrenie je zavedené a maximálne využívané). Vyhodnotenie súhrnných ukazovateľov sa nachádza v tabuľke 35.

Tab. 35: Vyhodnotenie ukazovateľov skupiny OP

Súhrnný ukazovateľ		**M**	**SD**
OP	Opatrenia IB v podniku	37,42	2,40
Čiastkový ukazovateľ		**M**	**SD**
OPTO	Technické opatrenia	39,11	39,57
OPOO	Organizačné opatrenia	35,72	36,05

Zdroj: vlastné spracovanie

Podľa výsledku súhrnného ukazovateľa OP, ktorý predstavuje aritmetický priemer a smerodajnú odchýlku z hodnôt čiastkových ukazovateľov technických a organizačných opatrení, podniky v priemere využívajú opatrenia IB na 37,42 % (M = 37,42; SD = 2,40). Čiastkové ukazovatele sú priemerom a smerodajnou odchýlkou hodnôt všetkých premenných v danej podskupine bezpečnostných opatrení. Technické opatrenia sú pri elektronickom podnikaní využívané viac (OPTO; M = 39,11; SD = 39,57) ako organizačné opatrenia (OPOO; M = 35,72; SD = 36,05). Výsledky ukazovateľov naznačujú, že v skúmaných podnikoch sú opatrenia IB skôr nevyužívané, respektíve využívané, ale na nedostatočnej úrovni.

Tabuľka 36 ukazuje hodnoty opisnej štatistiky využívania jednotlivých bezpečnostných opatrení skúmanými podnikmi. Prvých 17 premenných patrí do podskupiny organizačných opatrení, ostatné sú technické. Poradie opatrení IB určujeme podľa aritmetického priemeru (M).

Tab. 36: Deskriptívna štatistika premenných skupiny OP

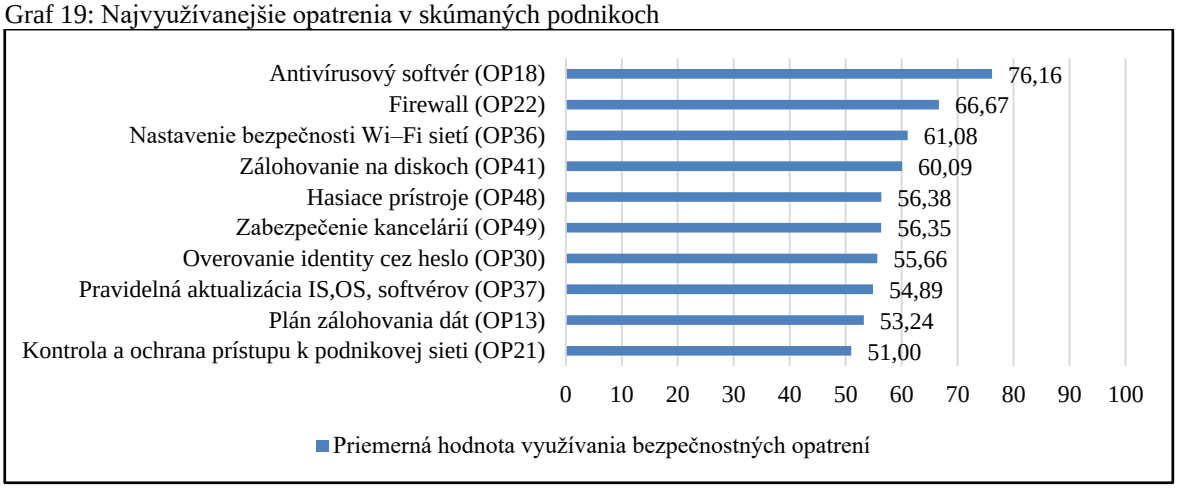
Premenná	**N**	**Min**	**Max**	**Variačné rozpätie**	**Špicatosť**	**Šikmosť**	**Modus**	**Medián**	**M**	**SD**	**Poradie podľa M**
OP01	91	0	100	100	-0,48	0,94	1	14	**29,13**	**33,19**	**44**
OP02	91	0	100	100	-0,06	1,11	0	5	**24,77**	**31,67**	**50**
OP03	91	0	100	100	-0,88	0,75	0	15	**32,41**	**34,86**	**34**

Premenná	N	Min	Max	Variačné rozpätie	Špicatosť	Šikmosť	Modus	Medián	M	SD	Poradie podľa M
OP04	91	0	100	100	-0,77	0,82	0	14	**30,68**	**34,54**	**38**
OP05	91	0	100	100	-0,69	0,89	0	8	**29,20**	**35,04**	**42**
OP06	91	0	100	100	-0,53	0,89	0	18	**29,97**	**32,81**	**41**
OP07	91	0	100	100	-1,46	0,19	100	47	**45,27**	**37,11**	**15**
OP08	91	0	100	100	-0,63	0,84	0	18	**30,23**	**33,11**	**39**
OP09	91	0	100	100	-1,22	0,41	0	36	**38,42**	**34,72**	**22**
OP10	91	0	100	100	-0,96	0,67	0	21	**34,14**	**35,42**	**31**
OP11	91	0	100	100	-1,68	0,02	0	50	**48,37**	**40,57**	**11**
OP12	91	0	100	100	-1,15	0,52	0	21	**34,52**	**34,77**	**30**
OP13	91	0	100	100	-1,47	-0,24	0	60	**53,24**	**37,63**	**9**
OP14	91	0	100	100	-1,42	0,32	0	32	**39,82**	**36,41**	**21**
OP15	91	0	100	100	-1,54	0,23	0	40	**42,58**	**38,36**	**18**
OP16	91	0	100	100	-1,20	0,61	0	24	**35,36**	**37,39**	**28**
OP17	91	0	100	100	-0,80	0,82	0	10	**29,16**	**33,38**	**43**
OP18	91	0	100	100	0,07	-1,23	100	98	**76,16**	**33,62**	**1**
OP19	91	0	100	100	-1,06	0,75	0	10	**32,21**	**37,66**	**35**
OP20	91	0	100	100	-1,47	0,50	0	15	**36,99**	**40,38**	**24**
OP21	91	0	100	100	-1,65	-0,06	100	50	**51,00**	**40,56**	**10**
OP22	91	0	100	100	-0,87	-0,75	100	79	**66,67**	**36,10**	**2**
OP23	91	0	100	100	-1,37	0,49	0	22	**37,51**	**37,55**	**23**
OP24	91	0	100	100	-0,62	0,90	0	8	**29,02**	**34,35**	**45**
OP25	91	0	100	100	-0,82	0,78	0	15	**30,88**	**34,64**	**37**
OP26	91	0	100	100	-0,76	0,80	0	15	**30,00**	**33,53**	**40**
OP27	91	0	100	100	-1,19	0,53	0	30	**36,41**	**36,09**	**26**
OP28	91	0	100	100	-0,08	1,15	0	6	**25,53**	**33,16**	**49**
OP29	91	0	100	100	0,39	1,31	0	4	**22,32**	**31,02**	**51**
OP30	91	0	100	100	-1,65	-0,23	100	60	**55,66**	**41,01**	**7**
OP31	91	0	100	100	0,99	1,61	0	1	**18,86**	**32,87**	**53**
OP32	91	0	100	100	0,43	1,37	0	2	**19,69**	**29,85**	**52**
OP33	91	0	100	100	-0,84	0,92	0	3	**28,67**	**37,60**	**46**
OP34	91	0	95	95	2,47	1,93	0	1	**14,77**	**26,62**	**55**
OP35	91	0	100	100	1,96	1,73	0	2	**16,73**	**26,79**	**54**
OP36	91	0	100	100	-1,34	-0,44	100	69	**61,08**	**38,26**	**3**
OP37	91	0	100	100	-1,58	-0,19	100	55	**54,89**	**39,31**	**8**
OP38	91	0	100	100	-1,19	0,50	0	20	**34,77**	**35,04**	**29**
OP39	91	0	100	100	-0,29	1,07	0	6	**26,25**	**34,14**	**48**
OP40	91	0	100	100	-1,49	0,19	0	45	**45,03**	**38,19**	**16**
OP41	91	0	100	100	-1,30	-0,41	100	64	**60,09**	**37,21**	**4**
OP42	91	0	100	100	-1,63	0,13	0	47	**46,62**	**40,70**	**12**
OP43	91	0	100	100	-1,54	0,25	0	43	**43,82**	**39,11**	**17**
OP44	91	0	100	100	-1,14	0,70	0	10	**33,26**	**38,42**	**32**
OP45	91	0	100	100	-1,59	0,40	0	22	**40,51**	**41,41**	**20**
OP46	91	0	100	100	-1,20	0,68	0	7	**33,09**	**38,83**	**33**
OP47	91	0	100	100	-1,73	0,31	0	21	**41,53**	**43,19**	**19**
OP48	91	0	100	100	-1,67	-0,27	100	70	**56,38**	**42,22**	**5**
OP49	91	0	100	100	-1,49	-0,28	100	54	**56,35**	**39,06**	**6**
OP50	91	0	100	100	-1,49	0,09	0	50	**45,77**	**38,05**	**13**
OP51	91	0	100	100	-0,73	0,97	0	3	**27,84**	**37,49**	**47**
OP52	91	0	100	100	-1,70	0,18	0	35	**45,68**	**41,44**	**14**
OP53	91	0	100	100	-1,02	0,83	0	6	**31,76**	**39,21**	**36**
OP54	91	0	100	100	-1,34	0,54	0	20	**36,67**	**38,99**	**25**
OP55	91	0	100	100	-1,29	0,56	0	19	**35,77**	**38,49**	**27**

Zdroj: vlastné spracovanie

Prehľad desiatich najvyužívanejších opatrení IB v podnikoch s elektronickým obchodom sa nachádza v grafe 19. Bezpečnostné opatrenie, ktoré sa v elektronickom podnikaní najviac využíva, je antivírusový softvér (OP18) s priemerom M = 76,16 bodov; SD = 33,62 bodov. Až 50 % hodnôt premennej je väčších ako 98 bodov. 75 % hodnôt prevyšuje 56 bodov. Respondenti v prieskume najčastejšie uvádzali 100 bodov, čo predstavuje až 38,46 % podnikov.

Graf 19: Najvyužívanejšie opatrenia v skúmaných podnikoch



Zdroj: vlastné spracovanie

Rozloženie dát opatrenia OP18 je veľmi málo špicaté (0,07) a výrazne vpravo zošikmené (-1,23). Podľa štatistík tvrdíme, že niekoľko nízkych hodnôt zmenšuje priemer na aktuálnu úroveň. Výsledky ukazujú, že využívanie antivírusového softvéru je v podnikoch bežné a považuje sa za základný a štandardný nástroj IB.

Opatrením IB s druhou najväčšou mierou využívania podnikmi na zabezpečenie informačných aktív pred rizikami je firewall (OP22) s priemerom M = 66,67 bodov; SD = 36,10 bodov. Najčastejšie je toto softvérové alebo hardvérové zariadenie využívané na 100 % až v 23,08 % skúmaných podnikov. Údaje premennej sú skôr ploché s viac extrémnejšími hodnotami (-0,87) a vpravo zošikmené s väčším množstvom vyšších hodnôt (-0,75). Medián predstavuje 79 bodov a iba 25 % údajov je rovných alebo menších ako 42,5 bodov. To, že skúmané podniky zaradia medzi najpoužívanejšie opatrenie práve firewall sme očakávali, pretože firewall je všeobecne vnímaný ako základný a bežný prostriedok bezpečnosti počítačových sietí. Jeho funkcie však nedokážu pokryť a eliminovať všetky bezpečnostné incidenty v počítačových sieťach. Preto je firewall vhodné kombinovať s inými nástrojmi na ochranu sieťovej prevádzky (napr. SIEM, VPN, DLP, atď.).

Tretím v poradí je nastavenie bezpečnosti Wi–Fi sietí (OP36). Premenná dosahuje priemer M = 61,08 bodov; SD = 38,26 bodov. Modus je opäť 100 bodov a až 28,57 %

respondentov uviedlo, že toto opatrenia maximálne využíva. 50 % hodnôt je nižších alebo vyšších ako 69 bodov a 75 % podnikov sa zaoberá nastavením Wi–Fi sietí na viac ako 25 bodov. Dáta sú výrazne ploché s viac extrémnymi hodnotami (-1,34) a mierne vpravo zošikmené (-0,44). Pretože elektronické podnikanie prebieha primárne v online prostredí, bezpečnostné nastavenia bezdrôtových sietí sú pre skúmané podniky dôležité. Interné podnikové Wi–Fi siete, ktoré majú nedostatočné bezpečnostné a prístupové nastavenia, sú pre útočníka jednoduchým prístupovým bodom ku informačným aktívam podniku.

Ďalšími najvyužívanejšími opatreniami IB sú zálohovanie na diskoch (OP41; M = 60,09; SD = 37,21), hasiace prístroje v prípade požiaru (OP48; M = 56,38; SD = 42,22), zabezpečenie kancelárií prostredníctvom uzamykateľných šuplíkov, skríň, dverí a trezorov (OP49; M = 56,36; SD = 39,06), overovanie identity osoby cez heslá (OP30; M = 55,66; SD = 41,01), pravidelná aktualizácia informačných systémov, operačných systémov a softvéru (OP37; M = 54,89; SD = 39,31), vytvorený plán zálohovania dát (OP13; M = 53,24; SD = 37,63) a kontrola s ochranou prístupu k podnikovej sieti (OP21; M = 51,00; SD = 40,56). Medzi prvých desať najpoužívanejších bezpečnostných opatrení elektronického podnikania sa dostalo iba jedno organizačné opatrenie, konkrétne plán zálohovania dát. Z toho vyplýva, že organizačné opatrenia, ktoré najviac podporujú ISMS, sú v skúmaných podnikoch málo využívané. Aby podniky s elektronickým obchodom riadili informačnú bezpečnosť procesným spôsobom, organizačné opatrenia sú nevyhnutné.

Opatrenia, ktoré sa pri elektronickom podnikaní skoro vôbec nevyužívajú sú bezpečnostné tokeny (OP32; M = 19,69; SD = 29,85), čipové karty zamestnancov (OP31; M = 18,86; SD = 32,87), systém jednotného prihlasovania (SSO) do podnikových systémov (OP35; M = 16,73; SD = 26,79) a overovanie identity cez biometrické prostriedky (OP34; M = 14,77; SD = 26,62).

Podľa výsledkov tvrdíme, že skúmané podniky najviac využívajú iba základné nástroje na ochranu informačných aktív podniku. Všetky pokročilé a moderné bezpečnostné opatrenia (napr. riadenie dodávok služieb, politika čistej obrazovky alebo čistého stola, školenia zamestnancov k IB, čipové karty zamestnancov, SMS autorizácia, klimatizovaná serverovňa, SIEM, DLP a i.) sú buď využívané veľmi málo alebo skoro vôbec. Podniky potrebujú získať prehľad o aktuálnych hrozbách IB a tiež o dostupných a účinných organizačných alebo technických opatreniach, napríklad vhodnými školeniami, kurzami, odbornými prezentáciami, prostredníctvom médií alebo účasťou zodpovedných zamestnancov na odborných konferenciách zameraných na problematiku IB a ISMS.

4.8.2 Porovnanie premenných OP v závislosti od skúmaných skupín

V rámci analýzy bezpečnostných opatrení porovnávame rozdiely vo využívaní jednotlivých opatrení medzi podnikmi, ktoré vyhodnocujú (N = 59) a nevyhodnocujú (N = 32) riziká IB a medzi podnikmi, ktoré majú (N = 49) a nemajú (N = 42) vypracovanú politiku IB. Rozdiely skupín testujeme, či sú štatisticky významné.

Podľa výsledkov K–S testu, iba dáta premennej plán zálohovania dát (OP13; Z = 1,27; p = 0,062) sú rozložené normálne. Rozdiely tejto premennej v závislosti od skúmaných skupín testujeme dvojvýberovým t–testom pre nezávislé súbory s rovnakým rozptylom. Pretože ostatné premenné skupiny opatrenia IB v podniku (OP) nie sú rozložené normálne (K–S test; p < 0,05), podrobujeme ich neparametrickému testovaniu Mann–Whitneyho U testom. V ďalšej časti uvádzame iba štatisticky významné výsledky testov, z ktorých možno vyvodiť relevantné závery.

Výsledky dvojvýberového t–testu nepreukázali štatisticky významný rozdiel opatrenia plán zálohovania dát (OP13) medzi skupinami podnikov, ktoré vyhodnocujú riziká IB a ktoré riziká nevyhodnocujú, t(89,00) = 1,37; p = 0,174. V tabuľke 37 sa nachádzajú výsledky neparametrického testovania premenných OP, ktoré indikujú štatisticky významné odlišnosti v skúmaných skupinách. Podniky, ktoré sa zaoberajú rizikami IB, sa na hladine významnosti α = 0,05 odlišujú od podnikov, ktoré riziká nevyhodnocujú, v 20 bezpečnostných opatreniach. Ako príklad uvádzame opatrenia systém tvorby a správy hesiel (OP07), riadenie a kontrola sieťových zariadení (OP14) a SIEM (OP26).

Tab. 37: Testovanie rozdielov premenných OP v závislosti od vyhodnocovania rizík

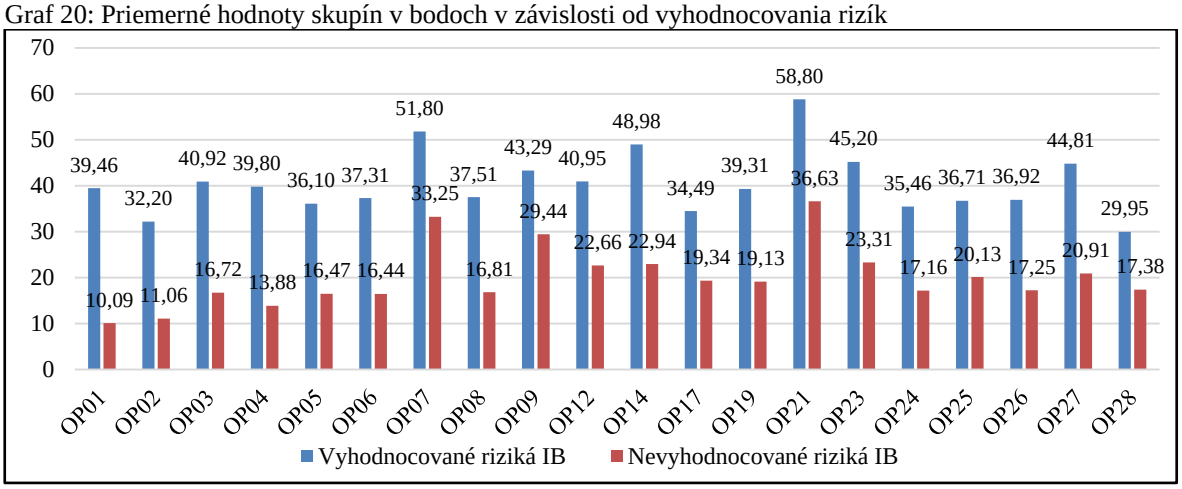
	Mann–Whitney U	Z	Asymp. Sig. (2–tailed)		Mann-Whitney U	Z	Asymp. Sig. (2–tailed)
OP01	459,00	-4,04	0,000	OP14	582,50	-3,01	0,003
OP02	629,50	-2,63	0,009	OP17	666,00	-2,32	0,020
OP03	588,00	-2,97	0,003	OP19	697,50	-2,06	0,039
OP04	569,50	-3,12	0,002	OP21	647,00	-2,48	0,013
OP05	685,00	-2,16	0,031	OP23	609,00	-2,79	0,005
OP06	615,50	-2,74	0,006	OP24	617,00	-2,73	0,006
OP07	619,00	-2,11	0,035	OP25	607,00	-2,81	0,005
OP08	590,00	-2,95	0,003	OP26	608,00	-2,81	0,005
OP09	709,00	-1,96	0,050	OP27	581,00	-3,03	0,002
OP12	658,00	-2,39	0,017	OP28	691,00	-2,12	0,034

Zdroj: vlastné spracovanie

V grafe 20 sú zobrazené priemerné hodnoty skupín pre opatrenia so štatisticky významnými odlišnosťami daných skupín. Priemerné hodnoty podnikov s vyhodnocovaním rizík sú pre každé opatrenie vyššie ako druhá skupina podnikov. Preto z pohľadu všetkých

signifikantných prípadov konštatujeme, že podniky s elektronickým obchodom, ktoré vyhodnocujú riziká IB, viac využívajú dané opatrenia.

Graf 20: Priemerné hodnoty skupín v bodoch v závislosti od vyhodnocovania rizík



Zdroj: vlastné spracovanie

V tabuľke 38 uvádzame testovanie rozdielov medzi podnikmi s vytvorenou a bez vytvorenej politiky IB pre premennú plán zálohovania dát (OP13), ktorej dáta sú normálne rozložené. Levenov test potvrdzuje štatisticky významnú rovnosť rozptylov skupín ($F = 1,52$; $p = 0,221$) a súvisiaci dvojvýberový t–test na hladine významnosti $\alpha = 0,05$ indikuje štatisticky významný rozdiel v opatrení plán zálohovania dát, $t(89,00) = 2,48$; $p = 0,015$, medzi podnikmi, ktoré majú bezpečnostnú politiku ($M = 62,06$; $SD = 35,47$) a podnikmi, ktoré túto politiku nemajú vytvorenú ($M = 42,95$; $SD = 37,86$). Podniky s politikou IB viac plánujú zálohovanie údajov.

Tab. 38: Testovanie rozdielov premennej OP13 v závislosti od bezpečnostnej politiky

		Levene's Test for Equality of Variances		t–test for Equality of Means						
									95% Confidence Interval of the Difference	
	Equal variances	F	Sig.	t	df	Sig. (2–tailed)	Mean Difference	Std. Error Difference	Lower	Upper
OP13	Assumed	1,52	0,221	2,48	89,00	0,015	19,11	7,70	3,82	34,40
	Not assumed	–	–	2,47	84,87	0,015	19,11	7,73	3,73	34,49

Zdroj: vlastné spracovanie

Výsledky testovania rozdielov medzi skúmanými skupinami pre premenné OP, ktoré nesplnili podmienky normálneho rozdelenia, sa nachádzajú v nasledujúcej tabuľke.

Tab. 39: Testovanie rozdielov premenných OP v závislosti od bezpečnostnej politiky

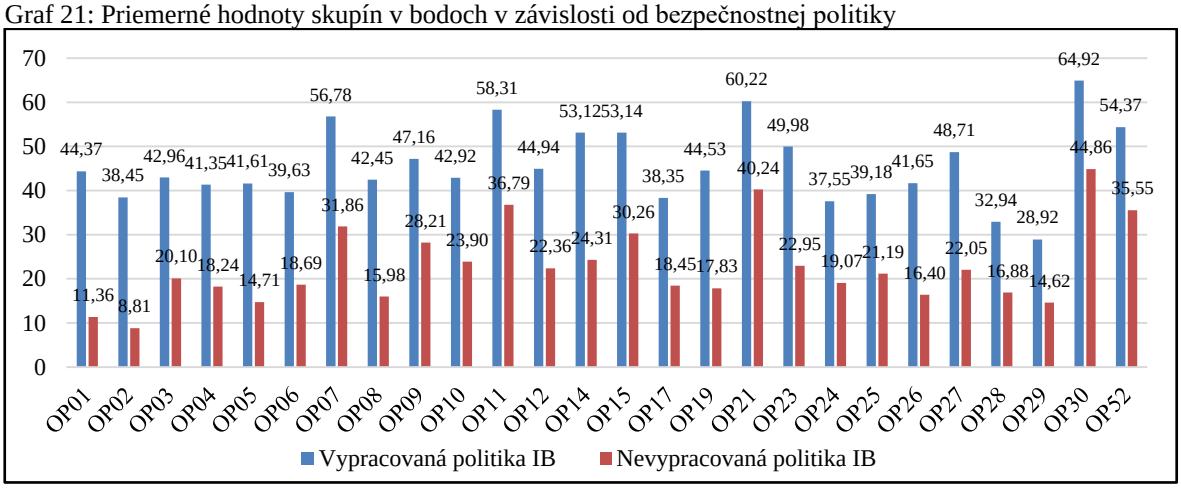
	Mann–Whitney U	Z	Asymp. Sig. (2–tailed)		Mann-Whitney U	Z	Asymp. Sig. (2–tailed)
OP01	438,50	-4,71	0,000	OP15	714,50	-2,51	0,012
OP02	536,00	-3,95	0,000	OP17	663,00	-2,93	0,003
OP03	681,00	-2,78	0,005	OP19	628,00	-3,21	0,001
OP04	653,00	-3,00	0,003	OP21	725,50	-2,43	0,015
OP05	603,00	-3,41	0,001	OP23	570,50	-3,66	0,000

	Mann–Whitney U	Z	Asymp. Sig. (2–tailed)		Mann-Whitney U	Z	Asymp. Sig. (2–tailed)
OP06	687,00	-2,73	0,006	OP24	637,50	-3,13	0,002
OP07	644,50	-3,06	0,002	OP25	619,00	-3,28	0,001
OP08	551,50	-3,82	0,000	OP26	539,00	-3,92	0,000
OP09	701,00	-2,62	0,009	OP27	562,00	-3,73	0,000
OP10	768,50	-2,08	0,037	OP28	665,00	-2,92	0,004
OP11	723,50	-2,44	0,015	OP29	723,00	-2,46	0,014
OP12	643,00	-3,09	0,002	OP30	747,50	-2,26	0,024
OP14	601,00	-3,41	0,001	OP52	726,00	-2,42	0,015

Zdroj: vlastné spracovanie

Podniky, ktoré zaviedli bezpečnostnú politiku, sa štatisticky významne odlišujú od podnikov, ktoré túto politiku nemajú až v 26 opatreniach, napríklad v opatrení stanovenie rolí IB (OP03), overovanie identity cez heslo (OP30), bezpečnostné dvere a okná (OP52), atď. Priemerné hodnoty opatrení IB pre konkrétne skupiny sú zobrazené v grafe 21.

Graf 21: Priemerné hodnoty skupín v bodoch v závislosti od bezpečnostnej politiky



Zdroj: vlastné spracovanie

Rovnako ako v prípade vyhodnocovania rizík, podniky s vypracovanou politikou IB majú všetky priemerné hodnoty skúmaných opatrení vyššie ako podniky bez politiky IB. Podniky s bezpečnostnou politikou viac využívajú dané opatrenia.

4.8.3 Výber bezpečnostných opatrení pre elektronické podnikanie

Na základe výsledkov z analýz systému riadenia informačnej bezpečnosti, informačných aktív, hrozieb IB, posúdenia úrovní rizík IB, existujúcich bezpečnostných opatrení a odborného odhadu navrhujeme výber bezpečnostných opatrení pre elektronické podnikanie podľa veľkosti podniku. Rozlíšenie podľa veľkosti podniku je nevyhnutné, pretože niektoré opatrenia sú pre mikropodniky a MSP nepotrebné (napr. z dôvodu malého rozsahu IT infraštruktúry) a v konečnom dôsledku príliš nákladné (napr. SIEM, penetračné testovanie, SSO, DLP). Ak by boli náklady na opatrenia vyššie ako je podnikom prijateľná

úroveň, primeranú IB nie je možné dosiahnuť (pozri graf 3). V takom prípade je IB podniku nadbytočne vysoká a náklady neadekvátne. Úlohou každého podniku s elektronickým obchodom je, aby podľa stanovených cieľov, požiadaviek IB a tiež výsledkov posúdenia rizík IB prispôsobil stanovené bezpečnostné opatrenia svojim procesom a zaviedol primeranú IB za akceptovateľné náklady. Návrh pridelenia bezpečnostných opatrení skúmaným podnikom podľa ich veľkosti uvádzame v tabuľke 40.

Tab. 40: Bezpečnostné opatrenia pre elektronické podnikanie

Kategória opatrení podľa ISO/IEC 27001	Cieľ opatrení podľa ISO/IEC 27002	Bezpečnostné opatrenia			Aktuálna úroveň implementácie	Príklad ošetreného rizika
		Mikro podniky	MSP	Veľké podniky		
Politiky informačnej bezpečnosti	Vytvárať a aktualizovať politiky, smernice a postupy, ktoré vymedzujú a usmerňujú podporu a manažment informačnej bezpečnosti v podniku a zabezpečujú súlad so zákonmi, podnikovými procesmi a požiadavkami	OP01	OP01	OP01	Stredná	HR38–IA09
		OP02	OP02	OP02	Nízka	HR45–IA05
		–	OP04	OP04	Stredná	HR28–IA22
		OP06	OP06	OP06	Stredná	HR32–IA19
		OP07	OP07	OP07	Stredná	HR14–IA10
		–	OP08	OP08	Stredná	HR39–IA30
		–	OP11	OP11	Stredná	HR40–IA02
		–	–	OP12	Stredná	HR35–IA13
		–	OP13	OP13	Vysoká	HR37–IA09
		–	OP14	OP14	Stredná	HR18–IA28
		–	OP15	OP15	Stredná	HR21–IA13
		OP16	OP16	OP16	Stredná	HR30–IA30
		–	–	OP17	Stredná	HR04–IA26
		–	–	OP51	Stredná	HR32–IA35
Organizácia informačnej bezpečnosti	Vytvoriť organizačné zázemie pre zriadenie, prevádzku, monitorovanie a zlepšovanie manažmentu informačnej bezpečnosti a pre informačnú bezpečnosť pri práci na diaľku	–	OP03	OP03	Stredná	HR47–IA04
		OP16	OP16	OP16	Stredná	HR45–IA02
		OP18	OP18	OP18	Veľmi vysoká	HR24–IA10
		OP20	OP20	OP20	Stredná	HR10–IA05
		–	OP21	OP21	Vysoká	HR21–IA21
		OP30	OP30	OP30	Vysoká	HR22–IA20
		OP36	OP36	OP36	Vysoká	HR32–IA23
		OP37	OP37	OP37	Vysoká	HR19–IA24
		–	–	OP38	Stredná	HR13–IA01
		OP40	OP40	OP40	Stredná	HR10–IA05
		OP41	OP41	OP41	Vysoká	HR18–IA12
		OP42	OP42	OP42	Stredná	HR18–IA13
		OP50	OP50	OP50	Stredná	HR16–IA14
Personálna bezpečnosť	Zabezpečiť, aby si zamestnanci boli vedomí svojej zodpovednosti k informačným aktívam podniku pred nástupom, počas zamestnania a po ukončení zamestnania	–	OP03	OP03	Stredná	HR43–IA02
		OP06	OP06	OP06	Stredná	HR14–IA06
		–	OP08	OP08	Stredná	HR42–IA05
		OP09	OP09	OP09	Stredná	HR45–IA04
		OP10	OP10	OP10	Stredná	HR46–IA03
		–	OP11	OP11	Stredná	HR13–IA05
		–	OP15	OP15	Stredná	HR17–IA08
Riadenie aktív	Určiť, klasifikovať a priradiť zodpovednosť za informačné aktíva a zaistiť ochranu pri zaobchádzaní s aktívami a médiami	–	OP13	OP13	Vysoká	HR18–IA16
		–	OP15	OP15	Stredná	HR32–IA13
		OP41	OP41	OP41	Vysoká	HR07–IA13
		OP42	OP42	OP42	Stredná	HR18–IA10
		OP43	OP43	OP43	Stredná	HR12–IA12
Riadenie prístupov	Zaistiť len autorizovaným používateľom prístup ku informáciám, zariadeniam spracúvajúcim informácie, službám a systémom	–	OP03	OP03	Stredná	HR17–IA08
		OP06	OP06	OP06	Stredná	HR11–IA15
		OP07	OP07	OP07	Stredná	HR21–IA14
		–	OP15	OP15	Stredná	HR32–IA21
		OP20	OP20	OP20	Stredná	HR14–IA06
		–	OP21	OP21	Vysoká	HR32–IA01
		–	–	OP27	Stredná	HR45–IA05

Kategória opatrení podľa ISO/IEC 27001	Cieľ opatrení podľa ISO/IEC 27002	Bezpečnostné opatrenia			Aktuálna úroveň implementácie	Príklad ošetreného rizika
		Mikro podniky	MSP	Veľké podniky		
		OP30	OP30	OP30	Vysoká	HR34–IA10
		–	OP31	OP31	Nízka	HR32–IA35
		OP33	OP33	OP33	Stredná	HR38–IA09
		–	–	OP35	Nízka	HR32–IA24
		OP36	OP36	OP36	Vysoká	HR10–IA04
		OP50	OP50	OP50	Stredná	HR11–IA14
Šifrovanie	Využiť kryptografické prostriedky na zabezpečenie dôverných informácií	OP38	OP38	OP38	Stredná	HR10–IA02
		OP39	OP39	OP39	Stredná	HR15–IA07
		OP40	OP40	OP40	Stredná	HR10–IA10
Fyzická bezpečnosť a bezpečnosť prostredia	Nepovoliť neautorizovaný prístup ku informačným aktívam a znemožniť zničenie, stratu alebo vyzradenie informačných aktív	OP06	OP06	OP06	Stredná	HR16–IA15
		–	OP31	OP31	Nízka	HR30–IA32
		OP45	OP45	OP45	Stredná	HR11–IA35
		–	OP46	OP46	Stredná	HR01–IA34
		–	OP47	OP47	Stredná	HR11–IA26
		OP48	OP48	OP48	Vysoká	HR01–IA16
		OP49	OP49	OP49	Vysoká	HR11–IA05
		OP50	OP50	OP50	Stredná	HR16–IA13
		–	–	OP51	Stredná	HR32–IA35
		OP52	OP52	OP52	Stredná	HR11–IA14
		–	OP53	OP53	Stredná	HR06–IA13
		–	OP54	OP54	Stredná	HR49–IA27
		–	OP55	OP55	Stredná	HR07–IA28
Bezpečnosť prevádzky	Zaistiť bezpečnú prevádzku zariadení a softvéru, ochrániť informačné aktíva pred stratou a škodlivým kódom, zaznamenávať a monitorovať dáta	–	OP13	OP13	Vysoká	HR18–IA13
		OP18	OP18	OP18	Veľmi vysoká	HR37– IA10
		–	OP23	OP23	Stredná	HR34–IA06
		–	–	OP28	Stredná	HR36–IA27
		OP37	OP37	OP37	Vysoká	HR19–IA28
		OP41	OP41	OP41	Vysoká	HR20–IA09
		OP42	OP42	OP42	Stredná	HR08–IA13
Komunikačná bezpečnosť	Chrániť informácie v sieťach, v sieťových zariadeniach a pri ich prenose	–	OP11	OP11	Stredná	HR13–IA02
		–	OP14	OP14	Stredná	HR09–IA28
		OP18	OP18	OP18	Veľmi vysoká	HR37–IA29
		–	OP19	OP19	Stredná	HR32–IA14
		OP20	OP20	OP20	Stredná	HR10–IA09
		–	OP21	OP21	Vysoká	HR32–IA27
		OP22	OP22	OP22	Vysoká	HR31–IA31
		–	OP24	OP24	Stredná	HR37–IA18
		–	OP25	OP25	Stredná	HR37–IA21
		–	–	OP27	Stredná	HR22–IA22
		OP36	OP36	OP36	Vysoká	HR42–IA02
		–	–	OP38	Stredná	HR10–IA07
		OP40	OP40	OP40	Stredná	HR27–IA22
		OP43	OP43	OP43	Stredná	HR12–IA13
Akvizícia, vývoj a údržba informačných systémov	Integrovať požiadavky informačnej bezpečnosti do vývojového cyklu informačných systémov	–	OP05	OP05	Stredná	HR09–IA22
		–	OP13	OP13	Vysoká	HR18–IA09
		–	OP15	OP15	Stredná	HR49–IA20
		OP37	OP37	OP37	Vysoká	HR19–IA03
		OP39	OP39	OP39	Stredná	HR25–IA09
Riadenie vzťahov s dodávateľmi	Zabezpečiť informačné aktíva, ktoré sú sprístupnené dodávateľom	–	OP04	OP04	Stredná	HR18–IA22
		–	OP05	OP05	Stredná	HR28–IA28
		–	OP15	OP15	Stredná	HR21–IA16
Riadenie bezpečnostných incidentov	Riadiť bezpečnostné incidenty, udalosti a zraniteľnosti	–	–	OP12	Stredná	HR36–IA18
		–	–	OP26	Stredná	HR32–IA29
		–	–	OP29	Nízka	HR34–IA06
Kontinuita informačnej bezpečnosti	Zaistiť dostupnosť zariadení, ktoré spracúvajú informácie	–	–	OP17	Stredná	HR28–IA03
		OP44	OP44	OP44	Stredná	HR08–IA28

Kategória opatrení podľa ISO/IEC 27001	Cieľ opatrení podľa ISO/IEC 27002	Bezpečnostné opatrenia			Aktuálna úroveň implementácie	Príklad ošetreného rizika
		Mikro podniky	MSP	Veľké podniky		
Súlad	Zabezpečiť súlad s právnymi a zmluvnými požiadavkami a s politikami podniku	OP02	OP02	OP02	Nízka	HR46–IA30
		–	OP04	OP04	Stredná	HR14–IA06
		–	OP13	OP13	Vysoká	HR25–IA12
		–	OP23	OP23	Stredná	HR24–IA11
		–	–	OP38	Stredná	HR33–IA05
		–	OP47	OP47	Stredná	HR39–IA32

Zdroj: vlastné spracovanie

Preskúmané a vyhodnotené bezpečnostné opatrenia sme priradili osobitne mikropodnikom, MSP a veľkým podnikom podľa aktuálnych potrieb a požiadaviek IB v elektronickom podnikaní. Kategorizáciu opatrení sme uskutočnili podľa Prílohy A normy ISO/IEC 27001[138] a cieľ opatrení sme s využitím normy ISO/IEC 27002[139] prispôsobili skúmanej problematike. V tabuľke je zároveň uvedený súčasný stav implementácie bezpečnostného opatrenia podľa výsledkov prieskumu spolu s príkladom rizika, ktorého pravdepodobnosť alebo následky dané opatrenie priamo znižuje. Navrhnutý výber opatrení IB slúži ako primeraný bezpečnostný štandard pre elektronické podnikanie.

4.9 Testovanie a verifikácia stanovených hypotéz

V rámci dizertačnej práce testujeme tri stanovené hypotézy, ktoré verifikujeme alebo falzifikujeme s využitím štatistických testov. Hypotézy vychádzajú zo súčasného stavu poznania ISMS a z predpokladov zameraných na elektronické podnikanie.

4.9.1 Hypotéza 1

Základom Hypotézy 1 je predpoklad, že množstvo finančných prostriedkov vynaložených na informačnú bezpečnosť súvisí s úrovňou IB, ktorú určujú podniky s elektronickým obchodom. V prípade, že podnik vynaloží viac, vníma vyššiu úroveň IB, alebo z druhého pohľadu, ak podniky vnímajú vysokú úroveň IB, majú aj vyššie náklady na IB. Hypotéza, ktorú overujeme korelačnou analýzou premenných podiel nákladov na IB z celkových nákladov a úroveň IB v podniku, je stanovená nasledovne:

H_0: Medzi nákladmi vynaloženými na informačnú bezpečnosť a úrovňou informačnej bezpečnosti stanovenou podnikmi neexistuje štatisticky významná stredne silná závislosť ($r > 0,3$) meraná korelačným koeficientom.

[138] STN ISO/IEC 27001: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Požiadavky.*
[139] STN ISO/IEC 27002: 2014: *Informačné technológie – Bezpečnostné metódy – Pravidlá dobrej praxe riadenia informačnej bezpečnosti.*

H_1: Medzi nákladmi vynaloženými na informačnú bezpečnosť a úrovňou informačnej bezpečnosti stanovenou podnikmi existuje štatisticky významná stredne silná závislosť (r > 0,3) meraná korelačným koeficientom.

Pretože výsledky K–S testu pre podiel nákladov na IB z celkových nákladov (SY06; Z = 2,49; p < 0,001) a pre úroveň IB v podniku (SY11; Z = 1,63; p = 0,006) dokazujú, že dáta premenných nie sú normálne rozložené, na meranie vzájomnej závislosti vyberáme Spearmanov korelačný koeficient a Kendallovo tau–c, ktorých výsledky sú zobrazené v tabuľke 41.

Tab. 41: Výsledky vzájomnej závislosti premenných SY06 a SY11

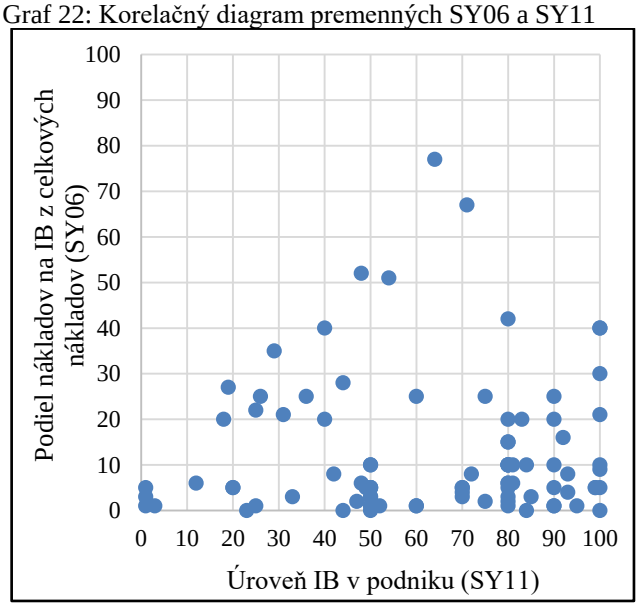
	Category	Statistic	Value	Asymp. Std. Error	Approx. T	Approx. Sig.
Symmetric measures	Ordinal by Ordinal	Kendall's tau–c	0,06	0,07	0,78	–
		Spearman Correlation	0,08	0,11	0,72	–
	N of Valid Cases	–	91	–	–	–

Zdroj: vlastné spracovanie

Spearmanov korelačný koeficient predstavuje r = 0,08 a Kendallovo tau–c je ešte nižšie, τ = 0,06. Pretože obe hodnoty sú veľmi nízke a blízke nule, čo vystihuje triviálnu silu vzájomnej lineárnej závislosti skúmaných premenných, prijímame nulovú hypotézu H_0. Vzájomná závislosť medzi nákladmi vynaloženými na informačnú bezpečnosť v podnikoch s elektronickým obchodom a úrovňou informačnej bezpečnosti stanovenou podnikmi je minimálna. Medzi premennými neexistuje štatisticky významná závislosť.

Minimálnu závislosť premenných podiel nákladov na IB z celkových nákladov a úroveň IB v podniku môžeme sledovať v grafe 22, kde nie je evidentné systematické usporiadanie bodov. Body sú v grafe rozložené náhodne.

Graf 22: Korelačný diagram premenných SY06 a SY11



Zdroj: vlastné spracovanie

Tento poznatok môžeme vysvetliť z pohľadu rozdelenia bezpečnostných opatrení na dve skupiny. Zatiaľ čo technické opatrenia sú finančne nákladné, organizačné opatrenia IB nemusia nutne znamenať dodatočné náklady, hoci rovnako prispievajú ku zvyšovaniu podnikmi vnímanej, ale aj reálnej úrovne IB. Napríklad, ak podnik vytvorí, zverejní a dodržiava politiku IB, ktorá nie je technickým opatrením, ale vo svojej podstate zdokumentovaná sada pravidiel, výrazne zvýši vnímanú úroveň IB, pričom náklady na vypracovanie tejto politiky sú len minimálne alebo žiadne. Preto výška investícií do IB neovplyvňuje úroveň IB, ktorá je stanovená respondentmi a teda vnímaná v podniku.

4.9.2 Hypotéza 2

V rámci hypotézy 2 skúmame, či existujú rozdiely v implementácii bezpečnostného opatrenia riadenie rizík informačnej bezpečnosti medzi podnikmi, ktoré disponujú vyššími rozpočtami a ktoré disponujú nižšími rozpočtami určenými na informačnú bezpečnosť. Hypotézu sme stanovili nasledovne:

H_0: Podniky, ktoré disponujú vyšším (1 smerodajná odchýlka nad priemerom) objemom finančných prostriedkov na informačnú bezpečnosť, sa štatisticky významne neodlišujú v riadení rizík informačnej bezpečnosti od tých, ktoré disponujú nižším (1 smerodajná odchýlka pod priemerom) objemom finančných prostriedkov na informačnú bezpečnosť.

H_1: Podniky, ktoré disponujú vyšším (1 smerodajná odchýlka nad priemerom) objemom finančných prostriedkov na informačnú bezpečnosť, sa štatisticky významne odlišujú v riadení rizík informačnej bezpečnosti od tých, ktoré disponujú nižším (1 smerodajná odchýlka pod priemerom) objemom finančných prostriedkov na informačnú bezpečnosť.

Metódou smerodajnej odchýlky sme rozdelili hodnoty premennej dostatok finančných zdrojov na IB (SY07) na dve skupiny s extrémnymi hodnotami. Priemer SY07 predstavuje M = 36,95 bodov; SD = 32,15 bodov. Jedna smerodajná odchýlka nad priemerom tvorí interval hodnôt od 69,10 bodov do 100 bodov. V tejto skupine sa nachádza 18 hodnôt. Na druhej strane, hodnota 4,80 bodov predstavuje jednu smerodajnú odchýlku pod priemerom. Všetky jednotky v súbore, ktoré majú túto alebo nižšiu hodnotu, sú druhou extrémnou skupinou. V skupine je 20 hodnôt. Priemer hodnôt premennej riadenie rizík IB (OP01) pri hodnotách skupiny jednej SD nad priemerom SY07 je M = 40,50 bodov; SD = 37,30 bodov. Priemer hodnôt OP01 pri hodnotách skupiny jednej SD pod priemerom SY07 predstavuje M = 9,95 bodov; SD = 18,36 bodov. Už pri týchto hodnotách pozorujeme

značný rozdiel, avšak prostredníctvom štatistického testovania zistíme, či sú rozdiely systematické alebo náhodné.

Pred zvolením vhodného testu podrobujeme premennú riadenie rizík IB (OP01) K–S testu, ktorý určuje, či hodnoty pochádzajú z normálneho rozdelenia. Výsledky ukazujú, že dáta nie sú normálne rozložené (Z = 1,94; p = 0,001), preto vyberáme neparametrický Mann–Whitneyho U test. Výsledok testu, ktorý je uvedený v tabuľke 42, je pre riadenie rizík informačnej bezpečnosti vysoko štatisticky významný (U = 22,50; p < 0,001). Hypotézu H_0 zamietame a prijímame alternatívnu hypotézu H_1. Podniky, ktoré disponujú vyšším objemom finančných prostriedkov na informačnú bezpečnosť, sa štatisticky významne odlišujú v riadení rizík informačnej bezpečnosti od tých, ktoré disponujú nižším objemom finančných prostriedkov na informačnú bezpečnosť.

Tab. 42: Mann–Whitneyho U test aplikovaný na OP01

Ranks	***N***			***Mean Rank***		***Sum of Ranks***	
	1 SD pod M	*1 SD nad M*	*Total*	*1 SD pod M*	*1 SD nad M*	*1 SD pod M*	*1 SD nad M*
OP01	20,00	18,00	38,00	27,38	55,44	547,50	998,00

Test Statistics	***Mann-Whitney U***	***Wilcoxon W***	***Z***	***Asymp. Sig. (2–tailed)***
OP01	22,50	998,00	-4,77	0,000

Zdroj: vlastné spracovanie

Veľkosť účinku určíme ako r = -4,77/√38 = -0,77, čo pre dáta premennej riadenie rizík IB predstavuje silný efekt. Pri výslednej štatistickej významnosti p < 0,001, silnom efekte r = -0,77 a na základe zistených systematických rozdielov medzi priemermi skupín konštatujeme, že podniky, ktoré disponujú vyšším objemom finančných prostriedkov určených na IB, viac využívajú riadenie rizík IB.

4.9.3 Hypotéza 3

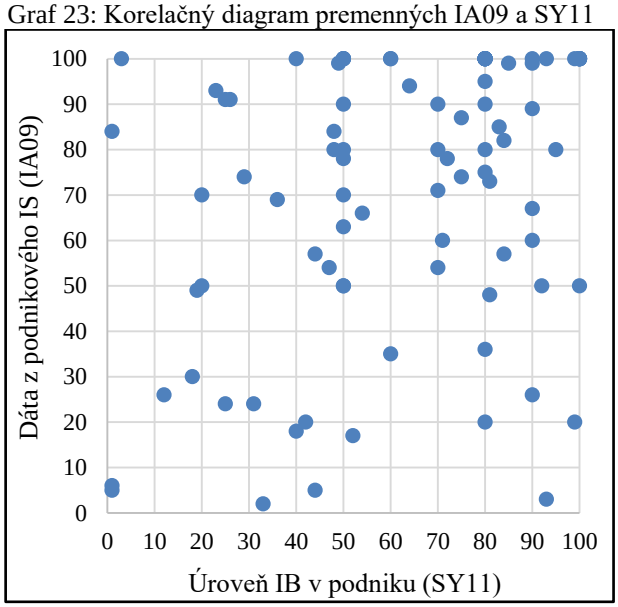
Hypotézou 3 overujeme, či podnikmi vnímaná úroveň informačnej bezpečnosti v ich prostredí ovplyvňuje hodnotenie významu dát z podnikového informačného systému. Na meranie vzťahu premenných využívame lineárnu regresnú analýzu. Hypotézu sme stanovili nasledovne:

H_0: Úroveň informačnej bezpečnosti vnímaná podnikmi s elektronickým obchodom nie je štatisticky signifikantným prediktorom významu dát z podnikového informačného systému.

H_1: Úroveň informačnej bezpečnosti vnímaná podnikmi s elektronickým obchodom je štatisticky signifikantným prediktorom významu dát z podnikového informačného systému.

Podľa korelačného diagramu premenných dáta z informačného systému podniku (IA09) a úroveň informačnej bezpečnosti v podniku (SY11) nie je možné pozorovať jednoznačnú lineárnu závislosť (pozri graf 23), čo však túto závislosť nevylučuje.

Graf 23: Korelačný diagram premenných IA09 a SY11



Zdroj: vlastné spracovanie

Z analýzy významu informačných aktív vyplýva, že dáta z podnikového IS (M = 71,16; SD = 30,28) sú síce vysoko hodnotené, ale nie sú najvýznamnejším aktívom elektronického podnikania. Nachádzajú sa až na 11. pozícii v poradí významnosti. Avšak, vplyv vnímanej úrovne IB v elektronickom podnikaní na veľkosť ich významu je možná a predpokladaná. Tvrdenie argumentujeme tým, že ak podniky s elektronickým obchodom dosahujú vyššiu úroveň IB, viac si uvedomujú závažnosť dát z IS. Hypotézu verifikujeme lineárnou regresnou analýzou v tabuľke 43.

Tab. 43: Regresný model závislej premennej IA09 a nezávislej premennej SY11

Model Summary (IA09)			
R	***R Square***	***Adjusted R Square***	***Std. Error of the Estimate***
0,34	0,11	0,11	28,65

ANOVA (IA09)					
	Sum of Squares	***df***	***Mean Square***	***F***	***Sig.***
Regression	9488,93	1	9488,93	11,56	0,001
Residual	73035,59	89	820,62	–	–
Total	82524,53	90	–	–	–

Coefficients (IA09)							
	Unstandardized Coefficients		***Standardized Coefficients***	***t***	***Sig.***	***95% Confidence Interval for B***	
	B	***Std. Error***	***Beta***			***Lower Bound***	***Upper Bound***
(Constant)	47,82	7,49	0,00	6,38	0,000	32,93	62,71
SY11	0,37	0,11	0,34	3,40	0,001	0,15	0,59

Zdroj: vlastné spracovanie

Koeficient korelácie R = 0,34 ukazuje slabý až stredne silný vzájomný vzťah skúmaných premenných. Podľa koeficientu determinácie R^2 = 0,11, regresný model vysvetľuje, že 11 % variability závislej premennej IA09 je ovplyvnených nezávislou premennou SY11. To, aká je podnikmi vnímaná úroveň IB (SY11), ovplyvnilo 11 % z hodnotenia dát z podnikového IS (IA09). Väčšinu, čiže 89 % ovplyvňujú všetky ostatné faktory, napríklad druh dát zachytávaných IS podniku, citlivosť alebo dôvernosť dát v IS, umiestnenie dát v lokálnej sieti alebo v cloude a iné.

Výsledok analýzy rozptylu (ANOVA) potvrdzuje, že model ako celok je štatisticky významný, F(1, 89) = 11,56; p = 0,001, pretože p–hodnota je oveľa nižšia ako hladina významnosti α = 0,05. Z toho vyplýva, že model dobre opisuje vzájomný vzťah medzi skúmanými premennými.

Lineárny regresný model pozostáva z lokujúcej konštanty b_0 = 47,82 s 95 % intervalom spoľahlivosti od 32,93 do 62,71 a z regresného koeficientu b_1 = 0,37 s 95 % intervalom spoľahlivosti od 0,15 do 0,59. Regresný koeficient b_1 štatisticky významne prispieva k predikcii závislej premennej IA09 (p = 0,001). Výslednú regresnú rovnicu podľa vzoru všeobecnej lineárnej rovnice $Y_i = b_0 + b_1 * X_i + \varepsilon_i$ pre i = 1, 2, ..., n, kde Y je závislá premenná, X nezávislá premenná a ε je chyba merania, môžeme zostaviť nasledovne:

$$IA09_i = 47,82 + 0,37 * SY11_i, \text{ teda:}$$

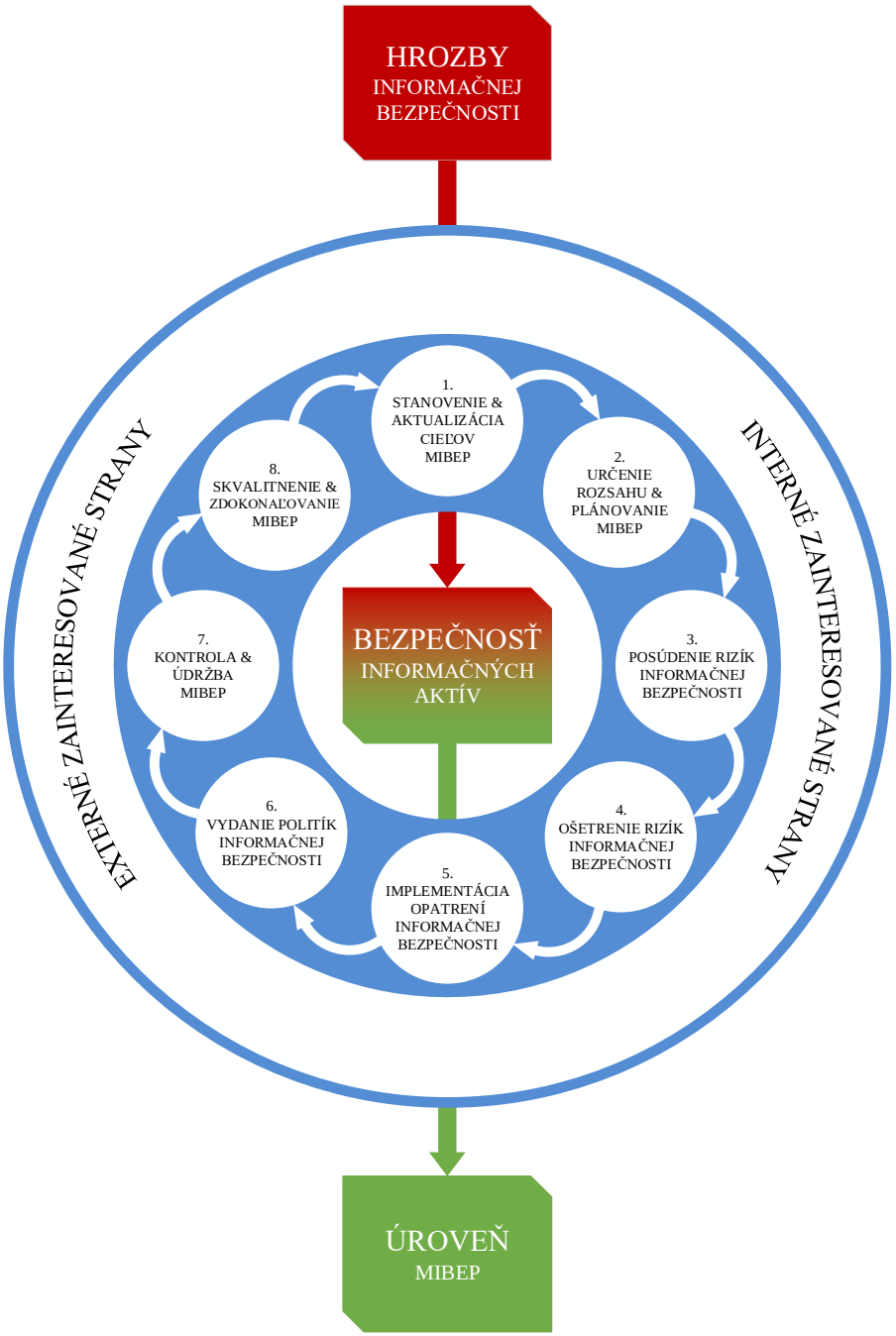
$$\text{Význam dát z IS podniku}_i = 47,82 + 0,37 * \text{Úroveň IB v podniku}_i$$

Na základe štatisticky významných výsledkov regresného modelu zamietame nulovú hypotézu H_0 a prijímame alternatívnu hypotézu H_1. Úroveň informačnej bezpečnosti vnímaná podnikmi s elektronickým obchodom štatisticky signifikantne ovplyvňuje význam dát z podnikového informačného systému.

4.10 Model manažmentu informačnej bezpečnosti elektronického podnikania

Po preskúmaní systému riadenia informačnej bezpečnosti, uskutočnení analýzy rizík informačnej bezpečnosti v podnikoch s elektronickým obchodom, preskúmaní a selekcii bezpečnostných opatrení pre elektronické podnikanie a verifikácii stanovených hypotéz pristupujeme k návrhu modelu manažmentu informačnej bezpečnosti elektronického podnikania (v skratke MIBEP), ktorý spája poznatky získané z dosahovania čiastkových cieľov dizertačnej práce.

Navrhovaný kvalitatívny model MIBEP, ktorý je zobrazený na obrázku 13, vychádza z aktuálneho stavu poznania skúmanej problematiky a výsledkov vlastného výskumu. Ide o dynamický, procesný model, čím zabezpečuje kontinuitu riadenia informačnej bezpečnosti a neustále zvyšuje bezpečnosť informačných aktív podniku. Model MIBEP je zameraný na prostredie elektronického podnikania a je univerzálne aplikovateľný v podnikoch rôznych veľkostí.



Obr. 13: Model MIBEP
Zdroj: vlastné spracovanie

Pri návrhu modelu založeného na báze systému, ktorý pozostáva zo vstupov (hrozby informačnej bezpečnosti), prvkov (interné alebo externé zainteresované strany, procesy MIBEP zamerané na bezpečnosť informačných aktív), výstupov (úroveň MIBEP) a vzájomných väzieb, bol aplikovaný systémový prístup, ktorým sme na určenie riešenia skúmali vnútorné aj vonkajšie súvislosti problematiky.

Hlavným cieľom implementácie modelu MIBEP je systematická a zároveň primeraná ochrana informačných aktív elektronického podnikania. Inými slovami, podniky v rámci akceptovateľných nákladov vyžadujú čo najvyššiu bezpečnosť svojich informačných aktív, pretože narušenie dôvernosti, dostupnosti alebo bezúhonnosti aktív môže viesť až k úplnému zastaveniu základnej podnikateľskej činnosti skúmaných podnikov, ktorou je elektronický predaj tovarov alebo služieb. Podniky dosahujú bezpečnosť informačných aktív a tým aj adekvátnu úroveň celého systému MIBEP práve kontinuálnym uskutočňovaním ôsmych identifikovaných procesov, čím zároveň spĺňajú požiadavky interných a externých zainteresovaných strán. Model MIBEP podrobne vysvetľujeme v nasledujúcich bodoch:

- *Hrozby informačnej bezpečnosti* – sú organizovanými, prípadne i náhodnými vstupmi do systému MIBEP s cieľom zneužiť zraniteľné miesta informačných aktív elektronického podnikania a tým podnik oslabiť. Medzi najpravdepodobnejšie hrozby v elektronickom podnikaní radíme prerušenie dostupnosti webových služieb, poruchy telekomunikačných zariadení a softvérové poruchy. Hrozby informačnej bezpečnosti sú v podnikovom prostredí realizované vo forme bezpečnostných incidentov,
- *Bezpečnosť informačných aktív* – je hlavným prvkom systému MIBEP a jednou z kľúčových potrieb elektronického podnikania a požiadaviek zainteresovaných strán. Bezpečnosť informačných aktív závisí od schopnosti procesov MIBEP eliminovať hrozby informačnej bezpečnosti, čo znamená, že akonáhle procesy nie sú schopné udržať primeranú úroveň celého systému, zraniteľné informačné aktíva podniku s elektronickým obchodom sú ohrozené a teda náchylnejšie na bezpečnostné incidenty. Z druhého pohľadu, kontinuálne a kvalitné vykonávanie procesov v stanovenom poradí prináša bezpečnosť informačných aktív elektronického podnikania a zároveň vysokú úroveň systému MIBEP. Informačné aktíva s najväčšou hodnotou v elektronickom podnikaní sú internetové pripojenie, dobré meno podniku a systém elektronického obchodu,

- *Úroveň MIBEP* – reprezentuje finálny výstup, ktorým je identifikácia celkovej úrovne systému MIBEP, čo odráža kvalitu bezpečnosti informačných aktív podniku s elektronickým obchodom. Úroveň systému môže byť merateľná, napríklad certifikácia od príslušnej autority, alebo nemerateľná, čiže nepretržitá schopnosť úspešne eliminovať hrozby informačnej bezpečnosti a čeliť bezpečnostným incidentom,
- *Zainteresované strany* – sú prvkom systému, ktorý pozitívne alebo negatívne ovplyvňuje chod procesov MIBEP. Rozdeľujeme ich nasledovne:
  - *Interné zainteresované strany* – nesú zodpovednosť za chod elektronického podnikania a zároveň predstavujú zainteresované strany z vnútorného prostredia podniku, predovšetkým zamestnancov a manažment podniku. Interné zainteresované strany vytvárajú požiadavky na informačnú bezpečnosť podniku, o procesoch MIBEP rozhodujú a schvaľujú ich. Procesy im poskytujú dokumentáciu, oznamy a dôveryhodnosť plynúcu z ochrany informačných aktív a kvality celého systému,
  - *Externé zainteresované strany* – nemajú zodpovednosť za chod elektronického podnikania. Ide o najrôznejšie fyzické a právnické osoby, napríklad odberatelia, dodávatelia, logistické spoločnosti, poskytovatelia služieb (napríklad webový hosting, cloudové služby, platobné brány), organizácie a inštitúcie aktívne v oblasti elektronického podnikania a informačnej bezpečnosti, ktoré tiež kladú požiadavky na informačnú bezpečnosť podniku s elektronickým obchodom. Z pohľadu verejnej správy ide o reguláciu procesov MIBEP. Procesy dodávajú externým zainteresovaným stranám oznamy, prehľady, vyhlásenia a zároveň sú zdrojom reputácie podniku,
- *Procesy MIBEP* – pozostávajú z ôsmych skupín rôznych činností, ktorých postupné a neustále vykonávanie chráni informačné aktíva pred hrozbami informačnej bezpečnosti a tým zvyšuje celkovú úroveň systému. Po ukončení cyklu všetkých ôsmych procesov MIBEP kontinuálne začína nový cyklus realizáciou prvého procesu. Implementácia modelu MIBEP je uskutočňovaná v poradí podľa nasledujúcich bodov:
  1. *Stanovenie a aktualizácia cieľov MIBEP* – určuje špecifické, realistické, merateľné, termínované a manažmentom podniku akceptovateľné a schválené ciele MIBEP, ktoré integrujú požiadavky interných a externých zainteresovaných strán. Podniky, ktoré prevádzkujú elektronický obchod,

stanovujú ciele s prihliadnutím na svoju veľkosť. Ciele, ktoré nie sú prispôsobené veľkosti podniku, sa môžu stať nerealistickými a tým aj nedosiahnuteľnými. Ak začína nový cyklus procesov, ciele je potrebné aktualizovať, prípadne stanoviť nové ciele,

2. *Určenie rozsahu a plánovanie MIBEP* – vymedzuje rozsah a určuje metriky činností procesov, aby zodpovedali každému podniku. Proces vytvára plány na realizáciu nasledujúcich procesov a definuje role zodpovedné za konkrétne činnosti procesov,
3. *Posúdenie rizík informačnej bezpečnosti* – pozostáva z identifikácie informačných aktív podniku, hrozieb, existujúcich opatrení, ďalej z analýzy rizík, určenia jednotlivých mier rizík, priorizovania rizík a vytvorenia zoznamu rizík informačnej bezpečnosti,
4. *Ošetrenie rizík informačnej bezpečnosti* – rozhoduje o primeranom spôsobe ošetrenia rizík, určuje opatrenia informačnej bezpečnosti vhodné pre podniky s elektronickým obchodom, formuluje vyhlásenie o aplikovateľnosti opatrení a vytvára plán ošetrenia rizík elektronického podnikania,
5. *Implementácia opatrení informačnej bezpečnosti* – zavádza a uskutočňuje vybrané technické a organizačné opatrenia na základe plánu ošetrenia rizík. V rámci organizačných opatrení sú formulované konkrétne politiky informačnej bezpečnosti,
6. *Vydanie politík informačnej bezpečnosti* – uvádza politiky informačnej bezpečnosti do podnikovej praxe, prispôsobuje dotknuté procesy elektronického podnikania a oboznamuje zainteresované strany,
7. *Kontrola a údržba MIBEP* – udržiava dosiahnutú úroveň procesov, celého systému MIBEP a kontroluje plnenie stanovených cieľov, vytvorených plánov a určených metrík,
8. *Skvalitnenie a zdokonaľovanie MIBEP* – napráva nedostatky, skvalitňuje činnosti procesov a určuje postup a kroky na kontinuálne zdokonaľovanie systému MIBEP. Ak podnik nevidí priestor na zdokonaľovanie, čiže nedokáže nájsť potenciál zdokonalenia systému a nemá dodatočné možnosti na skvalitnenie činností procesov, ukončí cyklus a pokračuje prvým procesom, stanovaním a aktualizáciou cieľov MIBEP.

Implementácia modelu MIBEP v prostredí podniku, ktorý prevádzkuje elektronické podnikanie, začína definovaním a predložením požiadaviek na informačnú bezpečnosť podniku zo strany interných zainteresovaných strán určeným zamestnancom. Interné zainteresované strany zvyknú byť prvé, ktoré si uvedomujú možné ohrozenie informačných aktív podniku. Prvotná identifikácia hrozieb informačnej bezpečnosti nie je nutná, pretože predpokladáme, že hrozby existujú aj v prípade, že ich manažment podniku alebo zamestnanci nezaznamenajú. Dôležité je skôr porozumenie významu informačných aktív podniku a rozhodnutie interných zainteresovaných strán o zavedení modelu MIBEP. Externé zainteresované strany požiadavky na IB dopĺňajú. Môže však nastať prípad, že implementáciu modelu iniciuje externá zainteresovaná strana, napríklad orgány štátnej správy prostredníctvom príslušného zákona.

Po rozhodnutí o implementácii modelu v podniku s elektronickým obchodom a predložení požiadaviek nasleduje postupná realizácia procesov v jednotlivých cykloch od stanovenia cieľov až po skvalitnenie a zdokonaľovanie procesov MIBEP. Po ukončení prvého cyklu nasleduje proces stanovenia a aktualizácie cieľov MIBEP. Doba trvania jedného cyklu je pre každý podnik individuálna v závislosti napríklad od dostupných zdrojov, znalostí zamestnancov a veľkosti podniku.

Model MIBEP radíme medzi procesné modely manažmentu informačnej bezpečnosti, ktorého cieľom je, podobne ako modelu PDCA, kontinuálne zlepšovanie procesov na dosiahnutie primeranej bezpečnosti informačných aktív. Spolu s modelmi BMIS a Všeobecným modelom faktorov vplyvu sa zameriava na podniky, avšak predovšetkým na tie, ktoré obchodujú na elektronickom trhu. Z pohľadu siedmych dimenzií požiadaviek ISMS podľa normy ISO/IEC 27001 je navrhnutý model na úrovni PDCA modelu, pretože sa zaoberá všetkými danými požiadavkami. Na rozdiel od obsahovo blízkych procesných modelov, konkrétne Mapy procesov SRIB a TQISM, zahŕňa riešenie problematiky kontextu v organizácii, postavenia vrcholového manažmentu v podniku a podpory ISMS.

Model MIBEP je uplatniteľný vo všetkých procesoch elektronického podnikania, čím sa zhoduje len s modelmi PDCA a Všeobecným modelom faktorov vplyvu. Avšak, tieto modely sú pre podniky s elektronickým obchodom príliš všeobecné, sú určené pre procesy všetkých organizácií alebo podnikov a nestanovujú niektoré významné procesy pre elektronické podnikanie (napr. posúdenie alebo ošetrenie rizík informačnej bezpečnosti, vydanie politík informačnej bezpečnosti).

5 Diskusia

Ak podniky chcú dosiahnuť primeranú úroveň bezpečnosti svojich informačných aktív, potrebujú praktizovať jednotlivé procesy manažmentu informačnej bezpečnosti. Pre oblasť elektronického podnikania navrhujeme implementáciu procesného modelu MIBEP v podnikovom prostredí, pretože vytvára, udržiava, kontroluje a zároveň skvalitňuje systém riadenia informačnej bezpečnosti. V kapitole uvádzame odporúčania k zavedeniu modelu MIBEP v skúmaných podnikoch, vyhodnocujeme výsledky výskumu, stanovené ciele a určujeme prínosy výsledkov výskumu dizertačnej práce pre teoretickú, pedagogickú a podnikovú oblasť.

5.1 Návrh odporúčaní k implementácii modelu v elektronickom podnikaní

Hrozby informačnej bezpečnosti je veľmi náročné predvídať najmä v podnikovom prostredí, v ktorom chýba adekvátne bezpečnostné povedomie. Mnoho interných zainteresovaných strán si ani neuvedomuje význam informačných aktív, s ktorými denne prichádzajú do kontaktu. Navyše, mnohí správcovia IT infraštruktúry sa mylne domnievajú, že keď majú zavedené len základné technické opatrenia, obyčajne antivírusový softvér, firewall, prípadne IDS/IPS, ich informačná bezpečnosť automaticky dosahuje vysokú úroveň. Hrozby informačnej bezpečnosti vychádzajú rovnako z externého ako interného prostredia podniku a iba technické bezpečnostné opatrenia nedokážu pokryť všetky reálne hrozby a bezpečnostné incidenty. Z pohľadu elektronického podnikania, internet nie je jediným zdrojom hrozieb IB, ale aj dodávatelia, konkurencia, vlastní zamestnanci, technológie, prírodné javy, atď. Na zachovanie bezpečnosti informačných aktív je nutné vytvoriť a zaviesť komplexný systém, ktorý požiadavkami IB pokryje všetky činnosti podniku, ktoré využívajú informačné aktíva. Ucelený systém na ochranu informačných aktív možno v elektronickom podnikaní vytvoriť podľa modelu MIBEP, ktorý umožňuje aktívne reagovať na hrozby IB, znižovať ich pravdepodobnosť alebo následky a v mnohých prípadoch aj hrozby predvídať.

V nasledujúcej tabuľke uvádzame návrh odporúčaní v podobe činností potrebných k zavedeniu modelu MIBEP v elektronickom podnikaní triedené podľa procesov modelu. Zároveň navrhujeme dokumentáciu k jednotlivým procesom, ktorá slúži na overenie správnej prevádzky celého systému riadenia informačnej bezpečnosti v elektronickom podnikaní.

Tab. 44: Odporúčania k zavedeniu modelu MIBEP v elektronickom podnikaní

Proces	Odporúčané činnosti k zavedeniu modelu MIBEP	Dokumenty
1. Stanovenie a aktualizácia cieľov MIBEP	• Reflektovať požiadavky na IB z pohľadu zainteresovaných strán • Stanoviť špecifické, realistické, merateľné a termínované ciele • Ciele dať schváliť manažmentu podniku • Aktualizovať ciele v prípade ďalšieho cyklu procesov	• Správa o cieľoch MIBEP
2. Určenie rozsahu a plánovanie MIBEP	• Definovať činnosti procesov, ich rozsah a metriky • Vytvoriť časový harmonogram realizácie procesov • Pripraviť návrh rozpočtu • *Určiť zamestnanca zodpovedného za systém (mikropodniky)* • *Určiť role a zamestnancov zodpovedných za procesy (MSP)* • *Vytvoriť oddelenie IB, určiť role a zamestnancov zodpovedných za procesy (veľké podniky)*	• Rozsah a metriky procesov MIBEP • Plán realizácie procesov MIBEP • Organizačná štruktúra MIBEP
3. Posúdenie rizík informačnej bezpečnosti	• Vyhodnotiť význam informačných aktív • Vyhodnotiť pravdepodobnosť hrozieb IB • Vyhodnotiť existujúce opatrenia IB • Analyzovať, určiť miery a priorizovať riziká IB	• Analýza a zoznam rizík IB
4. Ošetrenie rizík informačnej bezpečnosti	• Vybrať spôsoby ošetrenia rizík podľa výsledkov analýzy rizík IB • *Vybrať akceptovateľné opatrenia IB (pozri tabuľku 40)* • Aktualizovať rozpočet • Rozpočet dať schváliť manažmentu podniku	• Plán ošetrenia rizík IB • Vyhlásenie o aplikovateľnosti opatrení IB
5. Implementácia opatrení informačnej bezpečnosti	• Vytvoriť časový harmonogram implementácie opatrení IB • Zaviesť a nastaviť technické opatrenia IB • Zaviesť organizačné opatrenia IB • Vytvoriť zvolené politiky IB v rámci organizačných opatrení • Definovať sankcie za nedodržiavanie a odmeny za vylepšovanie politík IB • Vybrať a zrealizovať školenia IB pre rôzne skupiny zamestnancov	• Plán realizácie opatrení IB
6. Vydanie politík informačnej bezpečnosti	• Oboznámiť interné zainteresované strany s politikami IB • Oboznámiť externé zainteresované strany s politikami IB, ktorými sú priamo dotknuté • Dodržiavať politiky IB • Upraviť prevádzkové procesy, ak je to potrebné	• Politiky IB
7. Kontrola a údržba MIBEP	• Pravidelne vyhodnocovať stanovené ciele, plány a metriky • Pravidelne kontrolovať činnosti procesov • Sledovať hrozby IB a kontrolovať riziká IB • Pravidelne kontrolovať opatrenia IB • Pravidelne kontrolovať dodržiavanie politík IB • *Vykonať interný audit v rámci možností (MSP a veľké podniky)*	• Plán revízie procesov MIBEP • Plán revízie analýzy rizík IB • Plán revízie opatrení a politík IB
8. Skvalitnenie a zdokonaľovanie MIBEP	• Náprava neefektívnych činností procesov • Navrhnúť a uskutočniť návrhy na zdokonalenie procesov • Navrhnúť vhodný formát spätnej väzby a získať spätnú väzbu od interných zainteresovaných strán • *Vykonať externý audit v rámci možností podniku (veľké podniky)* • Informovať manažment podniku o úrovni systému MIBEP	• Vyhodnotenie kvality systému MIBEP • Vyhodnotenie cieľov MIBEP • Správa o úrovni MIBEP

Zdroj: vlastné spracovanie

Obsah procesov modelu MIBEP môže byť rôzny v závislosti od veľkosti podniku. Napríklad, mikropodniky so svojimi obmedzenými rozpočtami nedokážu a častokrát ani nepotrebujú implementovať pokročilé technické opatrenia (DLP, SIEM, biometrické prostriedky, atď.) a vykonávať mnohé personálne a finančne náročné činnosti (napr. externý audit). Na druhej strane, takéto opatrenia nemusia byť pre veľké podniky problematické. Odporúčané činnosti z predchádzajúcej tabuľky, okrem vyznačených kurzívou, sú

aplikovateľné v každom podniku a považujeme ich za nevyhnutné minimum pre implementáciu modelu MIBEP. Vyznačené činnosti možno aplikovať podľa veľkosti podniku uvedenej v zátvorke a výber bezpečnostných opatrení sme uskutočnili v tabuľke 40. Pri každej činnosti môžeme rátať s istou formou prispôsobenia. Avšak, prispôsobenie je možné do tej miery, aby bola udržaná kvalita systému na primeranej úrovni. Podniky samozrejme môžu realizovať oveľa viac činností v porovnaní s tými, ktoré sme uviedli v odporúčaniach, a dodatočne zvýšiť bezpečnosť informačných aktív a úroveň systému MIBEP. Na druhej strane, je potrebné vyhnúť sa duplicite dokumentovaných údajov a upraviť činnosti procesov a opatrenia, ktoré by mohli navzájom kolidovať.

Systém podľa modelu MIBEP v prostredí elektronického podnikania môže okrem mnohých výhod, napríklad v podobe neustálej schopnosti úspešne čeliť hrozbám IB a bezpečnostným incidentom, vyššej dôveryhodnosti zo strany zákazníka alebo jasne definovaného a prehľadného systému pre zodpovedných zamestnancov, priniesť začiatočné problémy s už existujúcimi procesmi podniku. Cieľom aplikovaného modelu nie je existujúce procesy, ktoré generujú tržby a pridanú hodnotu podniku, narušiť alebo zastaviť. Model prináša osem nových procesov, ktoré je nutné prispôsobiť podniku do takej miery, aby prevádzka podniku nebola narušená a aby bol vytvorený konsenzus medzi existujúcimi procesmi a procesmi MIBEP. Z tohto dôvodu je počas implementácie a pri uskutočňovaní procesov MIBEP dôležitá komunikácia zodpovedných zamestnancov s vedením podniku a ostatnými zamestnancami. Určitá miera ovplyvnenia či pozmenenia podnikových procesov je však akceptovateľná v tom prípade, ak systém podľa modelu MIBEP skutočne zvýši bezpečnosť informačných aktív konkrétneho podniku a začne úspešne eliminovať hrozby informačnej bezpečnosti.

Zamestnanci zodpovední za procesy MIBEP v podniku okrem prediskutovania požiadaviek a rozpočtu na pravidelných stretnutiach s vedením podniku potrebujú sledovať, zaznamenávať a v primeranej miere plniť požiadavky externých zainteresovaných strán, ktorých nesplnenie môže viesť až k strate zákazníkov, kľúčových dodávateľov alebo v krajnom prípade k pokutám a žalobám. Kontakt s externými zainteresovanými stranami je dôležitý aj z pohľadu získavania nových poznatkov a sledovania trendov IB, prípadne pri oznámení a poskytnutí informácií o závažnom bezpečnostnom incidente uskutočnenom v podniku dotknutým stranám. Vyvážený a vhodne nastavený vzťah medzi zodpovednými zamestnancami, internými a externými zainteresovanými stranami je pre implementáciu modelu MIBEP zásadný a vyžadovaný.

Využitie navrhovaného modelu MIBEP v elektronickom podnikaní je univerzálne, pretože nie je závislé na veľkosti podniku, právnej forme, ekonomickej činnosti podniku, množstve investovaných finančných prostriedkov alebo konkrétnom technickom riešení. Každý podnik s elektronickým obchodom môže jednotlivé činnosti procesov prispôsobiť svojmu prostrediu tak, aby boli adekvátne, realizovateľné a finančne akceptovateľné. Avšak, musí byť dodržaná podmienka, že dané činnosti prispievajú ku zvyšovaniu úrovne celého systému MIBEP a tým aj ku bezpečnosti informačných aktív podniku.

5.2 Vyhodnotenie predpokladov a výskumných cieľov

Výskum uskutočnený v rámci dizertačnej práce prináša viacero hodnotných poznatkov a záverov pre oblasť manažmentu informačnej bezpečnosti so zameraním na elektronické podnikanie. Vychádzajúc zo súčasného stavu poznania problematiky sme identifikovali štyri predpoklady, ktoré sa stali základom pre stanovenie hypotéz a vedeckých cieľov práce. V nasledujúcich častiach skúmame, či dosiahnuté výsledky výskumu potvrdzujú predpoklady a vyhodnocujeme hypotézy a ciele dizertačnej práce.

V Predpoklade A sa nachádza tvrdenie, že podnikom na slovenskom elektronickom trhu chýba ucelený systém riadenia informačnej bezpečnosti.[140] [141] Tento predpoklad sme skúmali premennou praktizovanie ISMS v podniku (SY05). Výsledky naznačujú (M = 30,08; SD = 28,59), že predpoklad platí aj na našej vzorke dát. Až 25 % podnikov sa ISMS nevenuje vôbec. 75 % podnikov uskutočňuje ISMS len na úrovni do 50 bodov zo 100 bodov. Z údajov je zrejmé, že podniky ISMS skôr nezavádzajú. Už z prvej kapitoly vyplýva, že správnou cestou pre podniky je práve aplikácia procesného prístupu prostredníctvom ISMS, ktorý zaručí primeranú IB elektronického podnikania. Iba 8 % skúmaných podnikov sa systémovému riadeniu IB venuje na tejto pokročilej úrovni. Zvyšným podnikom ucelený systém riadenia informačnej bezpečnosti chýba. Avšak, podľa hodnôt premennej SY01 si podniky dôležitosť ISMS v elektronickom podnikaní uvedomujú a na úrovni 64,89 % sa prikláňajú k tvrdeniu, že ISMS by mal byť riešený v rámci elektronického podnikania (M = 64,89; SD = 30,02). Navyše, výsledky analýzy dát premennej SY04 ukazujú, že podniky sa v priemere prikláňajú k potrebe zdokonaľovania ISMS v ich podniku (M = 61,26;

[140] NETOLICKÁ, B. 2012 (b). *5 zásad pre riadenie a presadzovanie informačnej bezpečnosti v organizácii.* [online]. 2012 [cit. 2015-12-05]. Dostupné na internete: <http://www.eset.com/sk/firmy/services/clanky/5-zasad-informacnej-bezpecnosti/>.
[141] KRÁL, D. 2011. Information Security in Small and Medium-Sized Companies. In *ACTA VŠFS*. ISSN 1802-792X, 2011, roč. 5, č. 1, s. 61.

SD = 29,33). Až 15,38 % podnikov si je maximálne istých, že systém riadenia informačnej bezpečnosti potrebuje.

Ďalšie poznatky vychádzajúce z aktuálneho stavu poznania manažmentu informačnej bezpečnosti v oblasti elektronického podnikania zhrňuje Predpoklad B s tvrdením, že podniky s elektronickým obchodom nedisponujú dostatkom finančných zdrojov na primerané zabezpečenie informačných aktív.[142] [143] [144] Vytvorený predpoklad overujeme v premenných SY06, v ktorej skúmame podiel nákladov na IB z celkových nákladov podniku, a SY07, v ktorej priamo zisťujeme, či podniky disponujú dostatkom finančných zdrojov na IB. Výsledkom analýzy dát premennej SY06 je, že skúmané podniky v priemere využívajú 12,63 % z celkových nákladov na IB (M = 12,63; SD = 15,11). Tento údaj je ale skreslený niekoľkými veľmi vysokými hodnotami. Modus (5 %) a medián (6 %) ukazujú lepší obraz o rozložení dát. Vysvetľujú, že väčšina podnikov investuje do IB okolo 5 % z celkových nákladov. Iba 10 % podnikov investuje do IB viac ako 30 %. Malé a stredné podniky využívajú na IB v priemere najviac, až 18,86 % z celkových nákladov. Nasledujú mikropodniky (10,81 %) a veľké podniky (9,67 %). Hoci sa výsledky analýzy dát premennej SY06 k Predpokladu B neviažu priamo, ukazujú, že podniky, ktoré obchodujú na slovenskom elektronickom trhu, skutočne využívajú určitú časť nákladov na IB a tým sa bezpečnosťou informačných aktív minimálne pasívne zaoberajú. Na základe výsledkov ostatných premenných skupiny systém riadenia informačnej bezpečnosti (SY) tvrdíme, že tieto náklady podniky využívajú primárne len na základné bezpečnostné opatrenia (napr. antivírusový systém, aplikačný firewall, protokol TLS, zálohovanie a i.). Výsledkom premennej SY07 je, že podniky dostatkom voľných finančných prostriedkov na IB disponujú len na úrovni 36,95 bodov zo 100 bodov (M = 36,95; SD = 32,15). Najviac týchto zdrojov majú veľké podniky (až 51,33 bodov), potom mikropodniky (37,33 bodov) a MSP (33,67 bodov). 50 % hodnôt predstavovalo menej ako 29 bodov. Až 10 % podnikov určilo hodnotu 0 alebo 1 bod, čo znamená, že tieto podniky vôbec nemajú dostatočné prostriedky na bezpečnosť podnikových informačných aktív. Výsledky výskumu z veľkej časti

[142] ČERNÝ, M. 2014. *Prístup k informačnej bezpečnosti v malých a stredných podnikoch* [online]. 2014 [cit. 2015-12-05]. Dostupné na internete: <http://www.itnews.sk/2014-06-24/c163829-pristup-k-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch>.

[143] SINGH, A. N. et al. 2013. Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. In *Global Journal of Flexible Systems Management*. ISSN 0972-2696, 2013, vol. 14, no. 4, p. 225.

[144] STEHLÍKOVÁ, B. – HOROVČÁK, P. 2012. Manažment informačnej bezpečnosti v malých a stredných podnikoch. In *Security Revue* [online]. 2012 [cit. 2015-12-01]. Dostupné na internete: <http://www.securityrevue.com/article/2012/06/manazment-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch/>.

odzrkadľujú Predpoklad B. Väčšina podnikov, ktoré obchodujú na slovenskom elektronickom trhu, dostatočné finančné zdroje na ochranu informačných aktív skôr nemajú.

Na základe Predpokladu B sme stanovili dve hypotézy, Hypotézu 1 a Hypotézu 2. V rámci Hypotézy 1 sme korelačným koeficientom skúmali, či podiel nákladov na IB z celkových nákladov (SY06) a podnikmi stanovená úroveň IB (SY11) navzájom závisia minimálne na stredne silnej úrovni ($r > 0,3$). Pretože hodnoty Spearmanovho korelačného koeficientu ($r = 0,08$) a Kendallovo tau–c ($\tau = 0,06$) sú blízke nule, prijali sme nulovú hypotézu. Vzájomná lineárna závislosť skúmaných premenných je triviálna. Medzi nákladmi vynaloženými na IB a úrovňou IB stanovenou podnikmi neexistuje štatisticky významná stredne silná, ani väčšia závislosť. Na rozdiel od tvrdení Singha a kol.[145], Černého[146], Stehlíkovej a Horovčáka[147], sme závislosť medzi nákladmi na IB a úrovňou IB v podniku pre oblasť elektronického podnikania nepotvrdili.

Hypotéza 2 skúma, či existuje štatisticky významný rozdiel v opatrení riadenie rizík IB (OP01) medzi podnikmi (SY07), ktoré disponujú vyšším objemom finančných prostriedkov na IB (jedna SD nad M) a ktoré disponujú nižším objemom finančných prostriedkov určených na IB (jedna SD pod M). Výsledok testovania neparametrickým Mann–Whitneyho U testom je pre riadenie rizík IB vysoko štatisticky významný ($U = 22,50$; $p < 0,001$; $r = -0,77$). Z tohto dôvodu sme zamietli hypotézu H_0 a prijali hypotézu H_1. Skúmané skupiny podnikov sa štatisticky významne odlišujú v opatrení riadenie rizík IB. Pri štatistickej významnosti $p < 0,001$ a silnom efekte $r = -0,77$ môžeme tvrdiť, že tie podniky, ktoré majú vyššie rozpočty určené na ochranu informácií, viac využívajú riadenie rizík IB. Podľa štúdie spoločnosti PwC konštatujeme, že 24 % podnikov, ktoré v roku 2015 zvýšili svoje rozpočty na IB[148], budú aj viac riadiť riziká IB.

Štúdie viacerých autorov (napr. Netolická[149], Černý a Romanová[150], EY[151]) podmienili vytvorenie Predpokladu C pre náš výskum. Predpokladáme, že hrozby smerujúce

---

[145] SINGH, A. N. et al. 2013. Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. In *Global Journal of Flexible Systems Management*. ISSN 0972-2696, 2013, vol. 14, no. 4, p. 225.

[146] ČERNÝ, M. 2014. *Prístup k informačnej bezpečnosti v malých a stredných podnikoch* [online]. 2014 [cit. 2015-12-05]. Dostupné na internete: <http://www.itnews.sk/2014-06-24/c163829-pristup-k-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch>.

[147] STEHLÍKOVÁ, B. – HOROVČÁK, P. 2012. Manažment informačnej bezpečnosti v malých a stredných podnikoch. In *Security Revue* [online]. 2012 [cit. 2015-12-01]. Dostupné na internete: <http://www.securityrevue.com/article/2012/06/manazment-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch/>.

[148] PWC. 2015. *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016.* [online]. 2015 [cit. 2015-12-03]. Dostupné na internete: <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html>.

[149] NETOLICKÁ, B. 2012 (a). *Sociálne inžinierstvo v kontexte informačnej bezpečnosti v organizácii.* [online]. 2012 [cit. 2015-12-03]. Dostupné na internete: <http://www.eset.com/sk/firmy/services/clanky/socialne-inzinierstvo-ib/>.

[150] ČERNÝ, M. – ROMANOVÁ, A. 2012. Interní zamestnanci ako hrozba bezpečnosti dát. In *Ekonomika a manažment podniku: vedecký časopis pre ekonomiku, riadenie a manažment slovenských podnikov.* ISSN 1336-4130, 2012, roč.10, č. 1-2, s. 7.

[151] EY. 2015. *Creating trust in the digital world: EY´s Global Information Security Survey 2015.* [online]. 2015 [cit. 2015-12-03]. Dostupné na internete: <http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf>.

na zraniteľnosti personálu sú významnou príčinou rizík IB. Hrozby, ktoré smerujú na zamestnancov, sme preskúmali a analyzovali v samostatnej podkapitole, kde sme identifikovali celkovo 26 možných hrozieb. Avšak, všetky z týchto hrozieb sú v elektronickom podnikaní hodnotené ako nepravdepodobné. Prvé riziko, ktoré spôsobuje jedna zo skúmaných hrozieb, sa nachádza až na 48. pozícii v poradí rizík a dosahuje strednú mieru s 5,33 bodmi. Ide o hrozbu prezradenia dôverných dát, prípadne obchodného tajomstva. Navyše, prvých 100 rizík v poradí obsahuje iba 6 rizík spôsobených danými hrozbami. Na našej vzorke dát sa predpoklad nepotvrdil, pretože riziká zapríčinené hrozbami smerujúcimi na zamestnancov sme síce v elektronickom podnikaní identifikovali, ale nie sú tak významnou príčinou, ako napríklad zlyhanie alebo porucha zariadenia, či prerušenie dostupnosti webových služieb.

Podľa posledného Predpokladu D vychádzajúceho zo štúdií viacerých spoločností, najmä Kaspersky Lab[152] a Entrust[153], sme na dátovom súbore zisťovali, či sú dáta z podnikového IS najvýznamnejším informačným aktívom pre podniky. Výsledky analýzy významu informačných aktív predpoklad nedosvedčujú. Dáta z IS sa nachádzajú až na 11. pozícii v poradí podľa významu informačných aktív. Majú síce priradenú vysokú hodnotu (M = 71,16; SD = 30,28), ale rozhodne nie sú najvýznamnejším aktívom elektronického podnikania. Podľa výsledkov výskumu je najvyššie hodnoteným aktívom internetové pripojenie (M = 86,21; SD = 21,71). V elektronickom podnikaní je významnejší iný druh dát, konkrétne dáta z elektronického obchodu (M = 74,40; SD = 28,65).

K Predpokladu D sa viaže Hypotéza 3, v ktorej s využitím lineárnej regresnej analýzy overujeme, či vnímaná úroveň IB v podniku s elektronickým obchodom (SY11) štatisticky signifikantne ovplyvňuje význam dát z podnikového IS (IA09). Tvrdíme, že ak podniky dosahujú vyššiu úroveň IB, viac si uvedomujú závažnosť dát z podnikového IS. Výsledok regresnej analýzy potvrdzuje štatisticky významný model, $F(1, 89) = 11,56$; $p = 0,001$. 11 % variability závislej premennej IA09 je vysvetlených nezávislou premennou SY11 ($R^2 = 0,11$). Regresný koeficient $b_1 = 0,37$ štatisticky významne prispieva k predikcii závislej premennej IA09 ($p = 0,001$). Zápis výslednej regresnej rovnice je nasledovný:

$$IA09_i = 47,82 + 0,37 * SY11_i, \text{ teda:}$$

$$\text{Význam dát z IS podniku}_i = 47,82 + 0,37 * \text{Úroveň IB v podniku}_i$$

[152] KASPERSKY. 2015. *Damage control: The cost of security breaches, IT security risks special report series* [online]. 2015. [cit. 2014-10-17]. Dostupné na internete: <http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf>.

[153] ENTRUST. 2004. *Protecting Your Most Important Asset: Information – How Data Security Mitigates Risk and Enables Compliance.* [online]. 2004 [cit. 2015-12-03]. Dostupné na internete: <https://www.entrust.com/wp-content/uploads/2013/05/secure_data_wp.pdf>.

Na základe štatisticky významného regresného modelu zamietame hypotézu H_0 a prijímame hypotézu H_1. Úroveň informačnej bezpečnosti stanovená v podniku štatisticky významne ovplyvňuje význam dát z podnikového informačného systému.

Návrhom kvalitatívneho a procesného modelu MIBEP spolu s odporúčaniami bol splnený hlavný cieľ dizertačnej práce. Model vychádza z analýzy, komparácie a syntézy informácií súčasného stavu poznania ISMS, dostupných modelov manažmentu informačnej bezpečnosti a z generalizácie výsledkov analýz dát z dotazníkového prieskumu. Vytvorením a zdokonaľovaním systému podľa navrhovaného modelu podniky udržiavajú bezpečnosť svojich informačných aktív pred hrozbami IB na adekvátnej úrovni. Hlavným výstupom systému je identifikácia celkovej úrovne MIBEP, čo predstavuje úroveň kvality IB podniku. Na rozdiel od ostatných modelov ISMS je zameraný výhradne na podniky, ktoré obchodujú na elektronickom trhu, a počíta s hrozbami IB ako s nežiaducim vstupom do systému. Model MIBEP prináša chýbajúce riešenie pre elektronické podnikanie v teórii a podnikovej praxi.

Splnenie hlavného cieľa je podmienené úspešným splnením všetkých čiastkových cieľov dizertačnej práce, ktoré spolu s najvýznamnejšími dosiahnutými výsledkami uvádzame v nasledujúcich bodoch:

- Analyzovať, porovnať a vytvoriť syntézu teoretických východísk manažmentu informačnej bezpečnosti so zameraním na elektronické podnikanie v domácom a zahraničnom prostredí,
    - Podkapitola Zhrnutie východísk manažmentu informačnej bezpečnosti,
    - Podkapitola Zhrnutie východísk elektronického podnikania,
- Analyzovať a porovnať vybrané modely manažmentu informačnej bezpečnosti,
    - Porovnanie vybraných modelov ISMS v tabuľke 7,
- Identifikovať a vyhodnotiť súčasný stav úrovne manažmentu informačnej bezpečnosti podnikov s elektronickým obchodom na základe dostupných poznatkov, výskumných štúdií a vlastného prieskumu,
    - Podniky s elektronickým obchodom si dôležitosť ISMS uvedomujú (SY01; M = 64,89; SD = 30,02) a prikláňajú sa k potrebe zdokonaľovania ISMS v ich podniku (SY04; M = 61,26; SD = 29,33), ale ISMS skôr nezavádzajú (SY05; M = 30,08; SD = 28,59),
    - Najväčší počet podnikov využíva 5 % z celkových nákladov na IB a 50 % podnikov využíva menej ako 6 % z celkových nákladov na IB,

- Skúmané podniky dostatkom finančných zdrojov skôr nedisponujú (SY07; M = 36,95; SD = 32,15) a až 10 % podnikov nemá vôbec dostatok prostriedkov, ktoré by mohli investovať do IB,
- 35,16 % zo všetkých podnikov vôbec nevyhodnocuje riziká a 54,95 % podnikov vyhodnocuje riziká IB minimálne aspoň raz ročne,
- 46,15 % skúmaných podnikov nemá vypracovanú politiku IB,
- Podniky s elektronickým obchodom sú skôr spokojné so svojou úrovňou IB (SY10; M = 66,63; SD = 27,09),
- Podnikmi vnímaná úroveň IB je dostačujúca (SY11; M = 62,93; SD = 27,68) a veľké podniky si oproti podnikom ostatných veľkostí najviac uvedomujú potrebu chrániť informácie,
- Nutnosť riešenia ISMS v elektronickom podnikaní a potreba ISMS v konkrétnom podniku majú stredne silný vzájomný vzťah (SY01 a SY04; $r = 0,42$; $p < 0,001$),
- Spokojnosť s úrovňou IB stredne silno súvisí so stanovenou úrovňou IB v podniku (SY10 a SY11; $\tau = 0,51$),
- Existuje štatisticky významný rozdiel v hodnotení nutnosti zavádzania ISMS v elektronickom podnikaní medzi tými, ktorí vyhodnocujú riziká IB a ktorí riziká IB nevyhodnocujú,
- Rozdiel medzi tým, či podniky majú alebo nemajú vytvorenú politiku IB alebo či sa zaoberajú rizikami IB alebo nezaoberajú, sa štatisticky významne prejavuje pri praktizovaní ISMS, výške nákladov na IB a pri vnímanom dostatku finančných zdrojov na IB,
- Praktizovanie ISMS štatisticky významne vplýva na úroveň IB podniku s elektronickým obchodom na hladine významnosti $\alpha = 0,05$,
- Podniky majú len základný prehľad o IB a sú pripravené na hrozby IB na základnej, dostačujúcej úrovni,

- Preskúmať vplyv nákladov vynaložených na informačnú bezpečnosť na podnikmi vnímanú úroveň informačnej bezpečnosti,
  - Podľa výsledku overenia Hypotézy 1, medzi nákladmi vynaloženými na IB a úrovňou IB stanovenou podnikmi neexistuje štatisticky významná závislosť,
- Vyhodnotiť význam informačných aktív podnikov obchodujúcich na slovenskom elektronickom trhu,

- Celkový význam informačných aktív je na úrovni 63,84 % (M = 63,84; SD = 9,55),
- Spomedzi čiastkových ukazovateľov je najdôležitejším informačným aktívom sieť (M = 72,24; SD = 33,16) pred primárnymi aktívami (M = 71,72; SD = 30,42) a dátami (M = 68,37; SD = 31,20),
- Najvýznamnejšími informačnými aktívami v elektronickom podnikaní sú internetové pripojenie (M = 86,21; SD = 21,71), dobré meno podniku (M = 84,68; SD = 24,99) a elektronický obchod (M = 80,35; SD = 27,46),
- Vyhodnotenie významu aktív jednotlivých podnikov na stupnici od nízkej po kritickú hodnotu v prílohe 1,
- Podniky s elektronickým obchodom sú schopné adekvátne vyhodnotiť a identifikovať kritické informačné aktíva a uvedomujú si ich hodnotu,

- Preskúmať a vyhodnotiť pravdepodobnosti výskytu hrozieb informačnej bezpečnosti v podnikoch s elektronickým obchodom,
  - Celkovo, podniky s elektronickým obchodom hodnotia hrozby IB ako nepravdepodobné (M = 16,10; SD = 5,88) a pretože je súhrnný ukazovateľ príliš nízky, skúmané podniky hrozby IB skôr podceňujú,
  - Spomedzi čiastkových ukazovateľov sú najviac pravdepodobné hrozby technického zlyhania (M = 25,21; SD = 24,52), ktoré podniky vnímajú ako málo pravdepodobné na rozdiel od ostatných skupín hrozieb, ktoré podniky vnímajú ako nepravdepodobné,
  - Najviac pravdepodobnými hrozbami IB sú prerušenie dostupnosti webových služieb (M = 28,22; SD = 26,13), porucha telekomunikačného zariadenia (M = 28,21; SD = 27,56) a softvérová porucha (M = 27,74; SD = 25,11),
  - Vyhodnotenie pravdepodobnosti výskytu hrozieb jednotlivých podnikov na stupnici od nepravdepodobnej po viac–menej istú hrozbu v prílohe 2,
  - Pretože podniky sú skôr spokojné so svojou úrovňou IB, ktorú vnímajú ako dostačujúcu, ale zároveň hrozby IB podceňujú, konštatujeme, že reálna úroveň IB v podniku je nižšia ako podnikmi vnímaná úroveň IB,
- Preskúmať a vyhodnotiť pravdepodobnosti výskytu hrozieb informačnej bezpečnosti smerujúcich na zraniteľnosti personálu,
  - 26 možných hrozieb na zraniteľnosti zamestnancov v elektronickom podnikaní a všetky sú hodnotené ako nepravdepodobné,
  - Prvých 100 rizík obsahuje iba 6 rizík spôsobených danými hrozbami,

- Najvyššie pravdepodobnosti boli pridelené úniku informácií (M = 19,03; SD = 20,95), prezradeniu dôverných dát a obchodného tajomstva (M = 18,71; SD = 25,09) a manipulácii so zdrojovými kódmi (M = 18,27; SD = 24,87),
- Najmenej pravdepodobné hrozby sú podplácanie (M = 7,54; SD = 13,07), predaj dôverných a osobných údajov (M = 7,25; SD = 13,56) a útok na zamestnanca (M = 6,46; SD = 12,70),

- Analyzovať, stanoviť miery a priorizovať riziká informačnej bezpečnosti,
  - 1180 možných rizík IB v podnikoch s elektronickým obchodom,
  - 59 % rizík má nízku mieru (M = 3,45; SD = 0,37),
  - 41 % rizík má strednú mieru (M = 4,53; SD = 0,50),
  - Ani jedno riziko nemá vysokú alebo kritickú mieru, čo je spôsobené nízkymi hodnoteniami pravdepodobností výskytu hrozieb IB,
  - Riziko, ktoré najviac ohrozuje IB elektronického podnikania, kombinuje hrozbu poruchy telekomunikačného zariadenia (HR09) s internetovým pripojením (IA28) na úrovni 6,41 bodov zo 16 bodov,
  - Matica priemerných mier rizík IB v prílohe 3,
- Preskúmať existujúce bezpečnostné opatrenia skúmaných podnikov a vybrať primerané opatrenia na zníženie rizík informačnej bezpečnosti,
  - V elektronickom podnikaní sa opatrenia IB využívajú v priemere na 37,42 % (M = 37,42; SD = 2,40), čo považujeme za nedostatočnú úroveň,
  - Technické opatrenia sú využívané viac (M = 39,11; SD = 39,57) ako organizačné opatrenia (M = 35,72; SD = 36,05),
  - Najvyužívanejšími opatreniami sú antivírusový softvér (M = 76,16; SD = 33,62), firewall (M = 66,67; SD = 36,10) a nastavenie bezpečnosti Wi–Fi sietí (M = 61,08; SD = 38,26),
  - Skúmané podniky najviac využívajú iba základné nástroje IB, všetky pokročilé opatrenia IB sú buď málo využívané alebo skoro vôbec,
  - Podniky, ktoré sa zaoberajú rizikami IB a ktoré sa rizikami nezaoberajú, sa štatisticky významne odlišujú v 20 bezpečnostných opatreniach,
  - Podniky, ktoré majú politiku IB, viac plánujú zálohovanie údajov,
  - Podniky, ktoré zaviedli bezpečnostnú politiku, sa štatisticky významne odlišujú až v 26 opatreniach od podnikov, ktoré túto politiku nemajú,
  - Výber primeraných bezpečnostných opatrení pre elektronické podnikanie podľa veľkosti podniku v tabuľke 40.

Pri spracovaní dizertačnej práce boli identifikované dve obmedzenia výskumu, ktoré bránia preskúmaniu problematiky z ďalších aspektov. Prvým obmedzením je absencia exaktných štatistických dát tržieb z elektronického predaja tovaru a služieb na Slovensku, kde sú k dispozícii najmä odborné odhady organizácií. Ďalším obmedzením výskumu je počet respondentov, ktorý je oproti celkovému počtu vyše 1100 oslovených podnikov zjavne nízky. Počet 91 respondentov síce považujeme za dostatočne reprezentatívny a nepredstavuje problém pri súhrnných analýzach, ale skôr pri porovnávaní kategórií premenných. Akonáhle sme štatistickými testami porovnávali rozdiely medzi viac ako dvomi kategóriami (napr. veľkosť podniku, právna forma), z dôvodu nedostatočnej veľkosti vzorky nebolo možné získať relevantné výsledky. Avšak, spomínané obmedzenia výskumu neovplyvnili priebeh dosahovania hlavného cieľa a čiastkových cieľov dizertačnej práce.

5.3 Prínosy pre oblasť teórie

Po splnení a vyhodnotení čiastkových cieľov a hlavného cieľa dizertačnej práce pristupujeme k identifikácii prínosov získaných poznatkov pre oblasť teórie, ktorými sú:

- Uskutočnená analýza, komparácia a syntéza súčasného stavu poznania ISMS a elektronického podnikania na základe teoretických východísk v prvej kapitole a zrealizovaného prieskumu v podnikoch s elektronickým obchodom,
- Analyzované a komparované existujúce modely manažmentu informačnej bezpečnosti z pohľadu dimenzií požiadaviek ISMS podľa normy ISO/IEC 27001 a možností uplatnenia modelov v elektronickom podnikaní,
- Vytvorený vysoko reliabilný dotazník so škálami od akceptovateľnej po excelentnú úroveň reliability ($\alpha = 0{,}64$ až $0{,}98$) a s možnosťou opätovného využitia,
- Uskutočnená analýza rizík IB s identifikáciou 1180 možných rizík v podnikoch s elektronickým obchodom a ich priorizovanie podľa miery rizík IB, najvýznamnejším rizikom je pôsobenie hrozby poruchy telekomunikačného zariadenia na internetové pripojenie,
- Uskutočnená analýza využitia bezpečnostných opatrení v podnikoch na slovenskom elektronickom trhu a zistenie, že najvyužívanejšími bezpečnostnými opatreniami v elektronickom podnikaní sú antivírusový softvér, firewall a nastavenie bezpečnosti Wi-Fi sietí,
- Zistenie, že medzi nákladmi vynaloženými na IB a podnikmi stanovenou úrovňou IB neexistuje štatisticky významná závislosť,

- Zistenie, že tie podniky, ktoré disponujú vyšším objemom finančných prostriedkov na IB, štatisticky významne viac využívajú riadenie rizík,
- Zistenie, že úroveň IB stanovená v podniku štatisticky signifikantne ovplyvňuje význam dát z IS podniku,
- Potvrdenie predpokladu, že podnikom na slovenskom elektronickom trhu chýba ucelený systém riadenia informačnej bezpečnosti,
- Potvrdenie predpokladu, že podniky s elektronickým obchodom nedisponujú dostatkom finančných zdrojov na primerané zabezpečenie informačných aktív,
- Vyvrátenie predpokladu, že hrozby smerujúce na zraniteľnosti personálu sú významnou príčinou rizík IB v elektronickom podnikaní,
- Vyvrátenie predpokladu, že dáta z podnikového IS sú pre podniky s elektronickým obchodom najvýznamnejším informačným aktívom,
- Návrh kvalitatívneho, procesného a systémového modelu MIBEP ako jedného z modelov ISMS, ktorý spĺňa požiadavky ISMS podľa normy ISO/IEC 27001 a ktorý je zameraný výhradne na elektronické podnikanie.

5.4 Prínosy pre podnikovú prax

Výsledky dizertačnej práce sú prínosom pre praktickú oblasť elektronického podnikania, pretože jednoznačne identifikujú, že:

- Podniky s elektronickým obchodom sú schopné adekvátne vyhodnotiť význam svojich informačných aktív,
- Význam informačných aktív podnikov je podľa súhrnného ukazovateľa na úrovni M = 63,84 bodov; SD = 9,55 bodov, najvýznamnejším aktívom elektronického podnikania je internetové pripojenie,
- Podniky si dostatočne neuvedomujú aktuálnosť hrozieb IB, preto je potrebné úroveň bezpečnostného povedomia v elektronickom podnikaní zvýšiť napríklad vytvorením vhodnej sady bezpečnostných školení,
- Pravdepodobnosť výskytu hrozieb IB sa podľa súhrnného ukazovateľa nachádza na úrovni M = 16,10 bodov; SD = 5,88 bodov, najpravdepodobnejšou hrozbou elektronického podnikania je prerušenie dostupnosti webových služieb,
- Podniky využívajú predovšetkým základné bezpečnostné opatrenia (napr. antivírusový softvér, firewall, zálohovanie, zabezpečenie kancelárií) a pokročilé opatrenia sú využívané len málo (napr. šifrovanie dát, elektronický podpis),

- Úroveň informačnej bezpečnosti, ktorá je stanovená podnikmi s elektronickým obchodom, dosahuje M = 62,93 bodov; SD = 27,68 bodov,
- Praktizovanie ISMS štatisticky významne vplýva na úroveň IB vnímanú v podnikoch s elektronickým obchodom,
- Reálna úroveň IB je nižšia ako podnikmi vnímaná úroveň IB, pretože podniky sú skôr spokojné so svojou úrovňou IB, ktorú vnímajú ako dostačujúcu, ale zároveň hrozby IB podceňujú,
- Podniky majú možnosť výberu bezpečnostných opatrení zaradených do jednotlivých kategórií s konkrétnymi cieľmi a členených podľa veľkosti podniku,
- Podniky sa môžu riadiť odporúčanými činnosťami a dokumentáciou pri zavádzaní systému podľa modelu MIBEP,
- Podniky po zavedení procesného, v elektronickom podnikaní všeobecne aplikovateľného modelu MIBEP zvýšia úroveň zabezpečenia informačných aktív.

5.5 Prínosy pre pedagogickú oblasť

Získané poznatky vyplývajúce z výskumu dizertačnej práce sú obohatením pre pedagogický proces predovšetkým v predmete Elektronické podnikanie, ako aj v ďalších tematických okruhoch zameraných na informačnú bezpečnosť a manažment informačnej bezpečnosti. Prínosy pre pedagogickú oblasť sú zhrnuté v nasledujúcich bodoch:

- Vypracovaný prehľad teoretických východísk manažmentu informačnej bezpečnosti,
- Syntéza procesu posúdenia rizík informačnej bezpečnosti z viacerých zdrojov,
- Vypracovaná analýza a prehľadná komparácia deviatich modelov manažmentu informačnej bezpečnosti,
- Prehľad súčasného stavu elektronického podnikania v SR a v zahraničí,
- Možnosť zaradenia získaného poznatku, že praktizovanie činností ISMS vedie ku zvyšovaniu úrovne informačnej bezpečnosti v podniku, do predmetov zameraných na manažment informačnej bezpečnosti,
- Začlenenie modelu MIBEP medzi ostatné modely ISMS s možnosťou ich výučby v predmetoch manažmentu informačnej bezpečnosti,
- Možnosť zaradenia informácií o modeli MIBEP spolu s navrhnutými odporúčaniami na implementáciu modelu do výučby predmetov, ktoré obsahujú témy zamerané na elektronické podnikanie.

Záver

Informácie, ktoré dosahujú vysokú úroveň kvality, majú pre podnik veľkú hodnotu. Na základe presných, úplných, dôverných a dostupných informácií dokáže podnik vykonávať rozhodnutia, ktoré ho robia stabilnejším, konkurencieschopnejším, rýchlejšie rastúcim a lepšie prispôsobiteľným trhovému prostrediu. Obzvlášť v elektronickom podnikaní, bez kvalitných informácií o zákazníkovi podnikatelia nedokážu produkt alebo službu priamo a vhodným spôsobom zacieliť. Na druhej strane, bez detailných, úplných a dôveryhodných informácií zákazník sotva nakúpi daný produkt alebo službu. Informácie a informačné aktíva, ktoré ich zachytávajú, spracúvajú, ukladajú, vytvárajú, transformujú na znalosti alebo s informáciami iným spôsobom pracujú, sú v elektronickom prostredí nevyhnutné. Bez mnohých informačných aktív s vysokým až kritickým významom podniky nedokážu pokračovať vo svojej prevádzke. Akonáhle podnik akékoľvek významné informačné aktívum stratí, poškodí, vyzradí alebo je dané aktívum nedostupné, príde z dôvodu straty dôvery o zákazníkov a následne o reputáciu, tržby, konkurenčnú výhodu, stabilitu, atď. Podnikanie na elektronickom trhu vyžaduje ochranu všetkých informačných aktív takým spôsobom, že dosiahne primeranú úroveň informačnej bezpečnosti, ideálne uskutočňovaním manažmentu informačnej bezpečnosti. ISMS definujeme ako ucelený systém v rámci riadenia organizácie, ktorý chráni informácie a informačné aktíva pred rizikami informačnej bezpečnosti.

Riziká informačnej bezpečnosti sú zapríčinené najrôznejšími hrozbami, ktoré pôsobia na zraniteľné miesta informačných aktív podnikov. Hrozby informačnej bezpečnosti zneužívajú informačné aktíva vo forme bezpečnostných incidentov, ktoré sú zdrojom následkov rôznych veľkostí na podnik a jeho prevádzku. V elektronickom podnikaní sú tieto hrozby o to pravdepodobnejšie, pretože celý transformačný proces je zabezpečovaný informačno–komunikačnými technológiami a počítačovými sieťami. Vhodný výber bezpečnostných opatrení a procesné riadenie rizík informačnej bezpečnosti umožňuje eliminovať riziká a znižovať mieru jednotlivých rizík na akceptovateľnú úroveň. ISMS integruje proces riadenia rizík a obohacuje ho o celú radu činností, ktoré vedú ku kontinuálne, systémovo a procesne dosahovanej dôvernosti, dostupnosti a bezúhonnosti informácií na akceptovateľnej úrovni z pohľadu zainteresovaných strán.

Návrhom modelu MIBEP sme splnili hlavný cieľ dizertačnej práce a zároveň priniesli konkrétne riešenie pre podniky s elektronickým obchodom. Kvalitatívny, procesný a v elektronickom podnikaní univerzálne aplikovateľný model MIBEP je založený na

aktuálnom stave poznania ISMS a výsledkoch vlastného výskumu. Model MIBEP zavádza systém, ktorý riadi bezpečnosť informačných aktív elektronického podnikania, spĺňa požiadavky interných a externých zainteresovaných strán a disponuje schopnosťou úspešne čeliť hrozbám informačnej bezpečnosti. Jeho výstupom je identifikácia úrovne manažmentu informačnej bezpečnosti v prostredí elektronického podnikania, ktorá pri kontinuálnom uskutočňovaní ôsmych procesov MIBEP dosahuje adekvátnu kvalitu. Procesná a systémová implementácia modelu MIBEP spolu s odporúčaniami v podnikoch s elektronickým obchodom prináša výhodu v podobe riadenej informačnej bezpečnosti.

Dosiahnutie hlavného cieľa vychádza z úspešného splnenia všetkých čiastkových cieľov dizertačnej práce stanovených na základe výskumných predpokladov a teoretických východísk problematiky ISMS a elektronického podnikania. Čiastkové ciele boli splnené s využitím všeobecných a špeciálnych metód vedeckej práce, usmernení podľa noriem rady ISO/IEC 27000 a odporúčaní organizácií aktívnych v oblasti informačnej bezpečnosti.

V prvej kapitole sme analyzovali, porovnávali a vytvárali syntézu súčasného stavu poznania oblastí manažmentu informačnej bezpečnosti, elektronického podnikania a existujúcich modelov ISMS z excerpcie poznatkov z prestížnych literárnych zdrojov, štatistických databáz, noriem, vedeckých štúdií a prieskumov organizácií zameraných na informačnú bezpečnosť. V rámci manažmentu informačnej bezpečnosti sme preskúmali východiská, ciele a požiadavky informačnej bezpečnosti, ďalej štruktúru, rámec, aktuálnu legislatívu a normy ISMS, súčasné bezpečnostné incidenty a ostatné primárne procesy ISMS. Posúdenie rizík považujeme za najvýznamnejší proces ISMS z dôvodu vytvorenia kompletnej rizikovej analýzy. Následne možno určiť spôsoby ošetrenia rizík a vybrať vhodné opatrenia informačnej bezpečnosti za akceptovateľné náklady, čím podniky dosiahnu primeranú bezpečnosť informačných aktív.

Ďalšou časťou v rámci preskúmania súčasného stavu poznania problematiky je komparácia dostupných modelov ISMS, ktoré podporujú implementáciu, riadenie a zlepšovanie procesov ISMS. Väčšina modelov je procesne orientovaná a v organizáciách všeobecne aplikovateľná. Avšak, každý model vychádza z iného výskumu, prostredia, štandardu či rámca, preto má odlišný cieľ a spôsob dosiahnutia informačnej bezpečnosti. Ich zhoda spočíva v potrebe docieliť primeranú úroveň ISMS v organizácii.

V kapitole nasleduje excerpcia poznatkov o elektronickom podnikaní spolu s prehľadom podnikania na Slovensku, kde sú aktuálne najviac využívané živnosti, potom spoločnosti s ručením obmedzeným a akciové spoločnosti. Zároveň, v SR sú najpočetnejšie mikropodniky spolu s malými podnikmi. Ďalej nasleduje prehľad súčasného stavu podnikov

v oblasti využívania elektronických obchodov doma a v zahraničí a špecifické vlastnosti podnikov so zameraním na informačnú bezpečnosť, hrozby a opatrenia. Využívanie internetu každým rokom stúpa a s dostupnosťou internetu vznikajú nové elektronické trhy. Vzostupný trend dosvedčujú Čína a USA, popredné krajiny elektronického podnikania, ktoré každý rok znásobujú tržby z predaja produktov a služieb cez internet. Aj v SR je každoročný nárast počtu elektronických obchodov a postupná informatizácia spoločnosti znakom rozvoja elektronického podnikania. Avšak, rozvoj nemôže pokračovať, ak podniky nevytvoria bezpečné prostredie pre informačné aktíva. Zákazník je totiž citlivý na bezpečnostné incidenty smerované na elektronické obchody. Akékoľvek realizované a neošetrené riziko informačnej bezpečnosti zapríčiňuje stratu množstva zákazníkov a tým až existenčné problémy. Navrhovaným riešením je implementácia modelu MIBEP, ktorý zaručí primeranú úroveň informačnej bezpečnosti.

Hlavný cieľ a čiastkové ciele práce sú definované v druhej kapitole na základe predpokladov vytvorených skúmaním súčasného stavu problematiky. Ciele sú podložené prieskumami a tvrdeniami rôznych organizácií a autorov, ktorí sa zaoberajú problematikou ISMS. V kapitole sú sformulované tri výskumné hypotézy, ktoré boli verifikované alebo falzifikované na základe vlastného výskumu. Výsledkom korelačnej analýzy v Hypotéze 1 je, že medzi nákladmi vynaloženými na informačnú bezpečnosť a podnikmi stanovenou úrovňou informačnej bezpečnosti neexistuje štatisticky významná stredne silná závislosť. Testovaním Hypotézy 2 sme zistili, že tie podniky, ktoré disponujú vyšším objemom finančných prostriedkov na IB, viac využívajú riadenie rizík. Pomocou regresnej analýzy bola overená Hypotéza 3, ktorá potvrdzuje, že úroveň informačnej bezpečnosti vnímaná v podniku ovplyvňuje význam dát z podnikového informačného systému.

Tretia kapitola charakterizuje objekt skúmania, opisuje zvolené postupy spracovania práce, dosahovania cieľov a uskutočňovania dotazníkového prieskumu. Jednotlivé činnosti na dizertačnej práci sme uskutočňovali postupne podľa fázy iniciácia, koncepcia, plánovanie, realizácia a ukončenie. Objektom skúmania sú podniky obchodujúce na slovenskom elektronickom trhu. Hlavnou podmienkou zaradenia konkrétneho podniku do výskumu bolo uskutočňovanie predaja produktov alebo služieb prostredníctvom elektronického obchodu a využívanie IKT pri riešení dodávateľsko–odberateľských vzťahov. V prehľadných tabuľkách sú uvedené premenné prieskumu a zvolené metódy vedeckej práce rozdelené podľa jednotlivých častí dizertačnej práce. Formulácia cieľov, výber vedeckých metód a preskúmanie teoretických východísk sa stali základom pre realizáciu vlastného výskumu a návrh riešenia identifikovaného problému.

V kapitole Výsledky práce sme uskutočnili výskumné činnosti štatistickou analýzou dát z dotazníkového prieskumu a návrhom riešení v jednotlivých skúmaných oblastiach. Využitím Cronbachovej alfy bola potvrdená vysoko reliabilná vnútorná konzistencia dotazníka. V rámci kapitoly sme preskúmali ISMS v podnikoch, ktoré obchodujú na slovenskom elektronickom trhu, a vytvorili kompletnú rizikovú analýzu elektronického podnikania na Slovensku spolu s výberom adekvátnych bezpečnostných opatrení podľa veľkosti podniku. Zároveň sme zistili, že podniky s elektronickým obchodom si dôležitosť ISMS uvedomujú a prikláňajú sa k potrebe jeho zdokonaľovania, ale ISMS skôr nezavádzajú. Podniky s elektronickým obchodom sú skôr spokojné so svojou úrovňou informačnej bezpečnosti, ktorú vnímajú ako dostačujúcu. Tiež sme identifikovali, že podniky majú len základný prehľad o informačnej bezpečnosti a sú pripravené na hrozby informačnej bezpečnosti len na minimálnej úrovni. Navyše, podniky nedostatočne doceňujú závažnosť hrozieb. Podniky predovšetkým využívajú iba elementárne nástroje informačnej bezpečnosti, všetky pokročilé bezpečnostné opatrenia sú málo využívané. Na druhej strane, skúmané podniky sú schopné náležite vyhodnotiť a identifikovať informačné aktíva. Kapitola bola ukončená verifikáciou hypotéz a návrhom modelu MIBEP.

V Diskusii sme stanovili odporúčania pre implementáciu navrhovaného modelu, vyhodnotili predpoklady, dosiahnuté výskumné ciele a identifikovali prínosy dizertačnej práce pre teoretickú, pedagogickú a podnikovú oblasť. Ako najväčší prínos dizertačnej práce pre teóriu, vzdelávanie a rovnako aj pre podnikovú prax považujeme model MIBEP, ktorý prináša doposiaľ chýbajúce riešenie skúmanej problematiky.

Dosiahnuté výsledky a formulované závery dizertačnej práce nepredstavujú ukončenie výskumnej činnosti v manažmente informačnej bezpečnosti elektronického podnikania. Oblasti, v ktorých môžu výskumné, ale aj vzdelávacie a podnikateľské činnosti na základoch výsledkov dizertačnej práce pokračovať, sú napríklad rozšírenie výskumu na ďalšie krajiny a porovnanie problematiky v týchto krajinách (napr. krajiny EÚ, USA, Čína, Japonsko), vytvorenie spolupráce s organizáciami pôsobiacimi v oblasti informačnej bezpečnosti s cieľom vzdelávať zamestnancov a študentov v skúmanej problematike, zvýšenie úrovne bezpečnostného povedomia v skúmaných podnikoch napríklad vytvorením a uskutočnením vhodnej sady bezpečnostných školení, vytvorenie metodiky na zavedenie, udržiavanie a zdokonaľovanie systému podľa modelu MIBEP v podnikoch s elektronickým obchodom, vytvorenie metodiky interného a externého auditu systému podľa modelu MIBEP a overenie efektívnosti zavedenia modelu MIBEP v podnikateľskej praxi.

Zoznam použitej literatúry

1. ABBASS, W. – BAINA, A. – BELLAFKIH, M. 2016. Improvement of Information System Security Risk Management. In *4th IEEE International Colloquium on Information Science and Technology (CiSt)*. Tangier–Assilah: IEEE, 2016. ISBN 978-1-5090-0751-6, p. 182 – 187.
2. AL RAWABDEH, W. – ZEGLAT, D. – ALZAWAHREH, A. 2012. The Importance of Trust and Security Issues in E-Commerce Adoption in the Arab World. In *European Journal of Economics, Finance and Administrative Sciences*. ISSN 1450-2275, 2012, vol. 52, p. 172 – 178.
3. ALCADE, B. et al. 2009. Towards a Decision Model Based on Trust and Security Risk Management. In *AISC '09 Proceedings of the Seventh Australasian Conference on Information Security. Vol. 98.* Wellington: Australian Computer Society, 2009. ISBN 978-1-920682-79-8, p. 61 – 70.
4. ALTUHHOVA, O. – MATULEVIČIUS, R. – AHMED, N. 2012. Towards Definition of Secure Business Processes. In *Advanced Information Systems Engineering Workshops (CaiSE 2012), Lecture notes in Business Information Processing. Vol. 112*. Berlin: Springer, 2012. ISBN 978-3-642-31069-0, p. 1 – 15.
5. ARLINE, K. 2015. *What is C2B?* [online]. 2015 [cit. 2015-12-10]. Dostupné na internete: <http://www.businessnewsdaily.com/5001-what-is-c2b.html>.
6. BOJANC, R. – JERMAN-BLAŽIČ, B. 2008. An economic modelling approach to information security risk management. In *International Journal of Information Management*, ISSN 0268-4012, 2008, vol. 28, no. 5, p. 413 – 422.
7. BOLEK, V. – KORČEK, F. – BEŇOVÁ, M. 2015. Information security risk management in Slovak enterprises. In *CER Comparative European Research 2015: proceedings of the 4th biannual CER conference*. [online]. London: Sciemcee publishing, 2015, 240 p. [cit. 2015-12-01]. Dostupné na internete: <http://www.sciemcee.org/library/proceedings/cer/cer2015_proceedings02.pdf>. ISBN 978-0-9928772-8-6.
8. CICHONSKI, P. et al. 2012. *Computer Security Incident Handling Guide.* [online]. Gaithersburg: NIST, 2012, 70 p. [cit. 2015-12-03]. Dostupné na internete: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>.
9. CSIRT.SK. 2014. *Analýza aktuálneho stavu a vývoja incidentov v prvom polroku 2014.* [online]. 2014 [cit. 2015-03-01]. Dostupné na internete: <https://www.csirt.gov.sk/doc/Analyza_CSIRT.SK.pdf>.
10. CSIRT.SK. 2017 (a). *Organizácie*. [online]. 2017 [cit. 2017-02-26]. Dostupné na internete: <https://www.csirt.gov.sk/informacna-bezpecnost/zahranicne-zdroje/organizacie-85e.html>.
11. CSIRT.SK. 2017 (b). *Štandardy informačnej bezpečnosti*. [online]. 2017 [cit. 2017-02-26]. Dostupné na internete: <https://www.csirt.gov.sk/bezpecnostna-studovna/sulad/standardy-informacnej-bezpecnosti-877.html>.
12. CSIRT.SK. 2017 (c). *Incidenty za obdobie od 1.1.2016 do 31.12.2016.* [online]. 2017 [cit. 2017-02-26]. Dostupné na internete: <https://www.csirt.gov.sk/graf-2016-8a0.html>.
13. CSIRT.SK. 2017 (d). *Incidenty za obdobie od 1.1.2015 do 31.12.2015.* [online]. 2017 [cit. 2017-02-26]. Dostupné na internete: <https://www.csirt.gov.sk/graf-2015-893.html>.

14. CYBERSECURITY. 2016. *Cyber Security (Kybernetická bezpečnost)*. [online]. 2016 [cit. 2017-02-27]. Dostupné na internete: <http://www.cybersecurity.cz/basic.html>.
15. ČERMÁK, M. 2009. *Řízení informačních rizik v praxi.* Brno: Tribun EU, 2009. 134 s. ISBN 978-80-7399-731-1.
16. ČERNÝ, M. 2014. *Prístup k informačnej bezpečnosti v malých a stredných podnikoch* [online]. 2014 [cit. 2015-12-05]. Dostupné na internete: <http://www.itnews.sk/2014-06-24/c163829-pristup-k-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch>.
17. ČERNÝ, M. – ROMANOVÁ, A. 2012. Interní zamestnanci ako hrozba bezpečnosti dát. In *Ekonomika a manažment podniku: vedecký časopis pre ekonomiku, riadenie a manažment slovenských podnikov.* ISSN 1336-4130, 2012, roč. 10, č. 1-2, s. 5 – 25.
18. ČSN ISO/IEC 27001: 2006: *Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky.*
19. DEKÝŠ, P. 2010. *Správa informačnej bezpečnosti v malej a stredne veľkej spoločnosti.* [online]. 2010 [cit. 2015-12-05]. Dostupné na internete: <http://www.eset.com/sk/firmy/services/clanky/sprava-informacnej-bezpecnosti/>.
20. DOUCEK, P. a kol. 2011. *Řízení bezpečnosti informací.* 2. vyd. Praha: Professional Publishing, 2011. 286 s. ISBN 978-80-7431-050-8.
21. DVORSKÝ, J. 2016. *Internetový predaj na Slovensku.* [online]. 2016 [cit. 2017-03-06]. Dostupné na internete: <http://www.bezpecnynakup.sk/storage/file/ts_19_10_16.doc>.
22. EFOCUS. 2014. Až 90 % slovenských podnikov registruje zneužívanie pracovného webu zamestnancami. In *eFocus*. [online]. 2014 [cit. 2015-12-03]. Dostupné na internete: <http://www.efocus.sk/kategoria/bezpecnost/clanok/az-90-slovenskych-podnikov-registruje-zneuzivanie-pracovneho-webu-zamestnan/>. ISSN 1337-9801.
23. ENISA. 2015 (a). *The ISMS Framework.* [online]. 2015 [cit. 2015-12-01]. Dostupné na internete: <https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/framework>.
24. ENISA. 2015 (b). *The Need for ISMS.* [online]. 2015 [cit. 2015-12-01]. Dostupné na internete: <https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-isms/need>.
25. ENTRUST. 2004. *Protecting Your Most Important Asset: Information – How Data Security Mitigates Risk and Enables Compliance.* [online]. 2004 [cit. 2015-12-03]. Dostupné na internete: <https://www.entrust.com/wp-content/uploads/2013/05/secure_data_wp.pdf>.
26. ESET. 2014. *Systém riadenia informačnej bezpečnosti.* [online]. 2014 [cit. 2015-12-01]. Dostupné na internete: <http://static1.esetstatic.com/uploads/media/System_riadenia_informacnej_bezpecnosti.pdf>.
27. EUROSTAT. 2016. *Share of enterprises´ turnover on e-commerce.* [online]. 2016 [cit. 2017-03-09]. Dostupné na internete: <http://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&plugin=1&language=en&pcode=tin00110>.
28. EUROSTAT. 2017 (a). *Digital single market - promoting e-commerce for businesses.* [online]. 2017 [cit. 2017-03-10]. Dostupné na internete: <http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bdek_sme&lang=e>
29. EUROSTAT. 2017 (b). *E-commerce sales.* [online]. 2017 [cit. 2017-03-09]. Dostupné na internete: <http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_ec_eseln2&lang=e>

30. EUR-LEX. 2014. *Nariadenie komisie (EÚ) č. 651/2014.* [online]. 2014. [cit. 2015-12-10]. Dostupné na internete: <http://eur-lex.europa.eu/legal-content/SK/TXT/?uri=CELEX%3A32014R0651>.
31. EUR-LEX. 2016. *Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.* [online]. 2016. [cit. 2017-02-27]. Dostupné na internete: <http://eur-lex.europa.eu/legal-content/SK/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.SLK>.
32. EY. 2014 (a). *Cyber Threat Intelligence – how to get ahead of cybercrime*. [online]. 2014 [cit. 2015-12-01]. Dostupné na internete: <http://www.ey.com/Publication/vwLUAssets/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime/$FILE/EY-cyber-threat-intelligence-how-to-get-ahead-of-cybercrime.pdf>.
33. EY. 2014 (b). *Get Ahaed of Cybercrime: EY´s Global Information Security Survey – 2014.* [online]. 2014 [cit. 2015-12-04]. Dostupné na internete: <http://www.ey.com/Publication/vwLUAssets/EY-global-information-security-survey-2014/$FILE/EY-global-information-security-survey-2014.pdf>.
34. EY. 2015. *Creating trust in the digital world: EY´s Global Information Security Survey 2015.* [online]. 2015 [cit. 2015-12-03]. Dostupné na internete: <http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf>.
35. ECOMMERCEFOUNDATION. 2015. *Global B2C E-commerce Report 2015.* [online]. 2015 [cit. 2015-12-10]. Dostupné na internete: <https://www.ecommercefoundation.org/report-info/45/Global-B2C-E-commerce-Report-2015-Light-Version>.
36. GOGELA, R. 2011. *Standardy a definice pojmů ISMS.* [online]. 2011 [cit. 2015-12-04]. Dostupné na internete: <http://www.cybersecurity.cz/data/Gogela.pdf>.
37. HARTONO, E., et al. 2014. Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. In *Decision Support Systems.* [online]. 2014, vol. 62, p. 11-21 [cit. 2014-11-16]. Dostupné na internete: <http://www.sciencedirect.com/science/article/pii/S0167923614000396>. ISSN 0167-9236.
38. HASAN, J. – PÓYA, A. – KITA, P. 2016. E-commerce Impacts on Selected Economic Area in Slovakia. In *International Journal of Innovative Research in Computer and Communication Engineering.* ISSN 2320-9798, 2016, vol. 4, no. 8, p. 14952 – 14959.
39. HEUREKA. 2015 (a). *Obrat e-commerce 2015.* [online]. 2015 [cit. 2017-03-10]. Dostupné na internete: <https://www.heurekashopping.sk/resources/attachments/p0/20/heureka-obrat-2015-sk.jpg>.
40. HEUREKA. 2015 (b). *Obrat e-commerce 2015.* [online]. 2015 [cit. 2017-03-10]. Dostupné na internete: <https://www.heurekashopping.cz/resources/attachments/p0/3/heureka-obrat-2015.pdf>.
41. HUDEC, L. 2014. *Manažment informačnej bezpečnosti.* [online]. 2014 [cit. 2015-12-01]. Dostupné na internete: <http://www.informatizacia.sk/ext_dok-prezgr_manazment_ib/17907c>.
42. HUO, C. – MENG, L. – CHEN, K. 2015. Research on the University Network Information Security Risk Management Model Based on the Fuzzy Sets. In *International Conference on Automation, Mechanical Control and Computational*

Engineering AMCEE. Ji´nan: Atlantis Press, 2015. ISBN 978-94-62520-64-6, p. 89 – 93.

43. CHEN, S. 2005. *Strategic Management of E-business*. 2nd ed. Chichester: John Wiley & Sons, 2005. 384 s. ISBN 0-470-87073-7.
44. CHENG, C. B. – CHAN, C. C. H. – LIN, K. C. 2006. Intelligent agents for e-marketplace: Negotiation with issue trade-offs by fuzzy inference systems. In *Decision Support Systems*. ISSN 0167-9236, 2006, vol. 40, no. 2, p. 626 – 638.
45. ISACA. 2009. *An Introduction to the Business Model for Information Security*. [online]. 2009 [cit. 2017-03-20]. Dostupné na internete: <http://www.isaca.org/Knowledge-Center/Research/Documents/Introduction-to-the-Business-Model-for-Information-Security_res_Eng_0109.pdf>.
46. ISACA. 2010. *The Business Model for Information Security*. Rolling Meadows: ISACA, 2010. 73 s. ISBN 978-1-60420-154-3.
47. ISACA. 2012 (a). *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows: ISACA, 2012. 94 s. ISBN 978-1-60420-237-3.
48. ISACA. 2012 (b). *COBIT 5 for Information Security*. Rolling Meadows: ISACA, 2012. 220 s. ISBN 978-1-60420-255-7.
49. ISACA. 2014. *Implementing the NIST Cybersecurity Framework*. Rolling Meadows: ISACA, 2014. 108 s. ISBN 978-1-60420-358-5.
50. ISACA. 2015. *CSX Cybersecurity Nexus: Cybersecurity Fundamentals – study guide*. Rolling Meadows: ISACA, 2015. 190 s. ISBN 978-1-60420-593-0.
51. ISO. 2017. The ISO Survey of Management System Standard Certifications (2006-2015). [online]. 2017 [cit. 2017-02-25]. Dostupné na internete: <http://www.iso.org/iso/iso_27001_iso_survey2015.xls>.
52. JI, H. – ZOU, S. 2016. Electronic Commerce in China Information Security Management System Strategy Research. In *2nd International Conference on Humanities and Social Research (ICHSSR 2016)*. [online]. 2016 [cit. 2017-03-28]. Dostupné na internete: <http://www.atlantis-press.com/php/download_paper.php?id=25861735>. ISBN 978-94-6252-235-0.
53. JIRÁSEK, P. – NOVÁK, L. – POŽÁR, J. 2015. *Výkladový slovník kybernetické bezpečnosti.* Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2015. 240 s. ISBN 978-80-7251-436-6.
54. KASPERSKY. 2015. *Damage control: The cost of security breaches, IT security risks special report series.* [online]. 2015. [cit. 2014-10-17]. Dostupné na internete: <http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf>.
55. KEITH, M. 2015. *Global ecommerce sales, trends and statistics 2015*. [online]. 2015 [cit. 2015-12-10]. Dostupné na internete: <http://www.remarkety.com/global-ecommerce-sales-trends-and-statistics-2015 >.
56. KOKLES, M. – BOLEK, V. 2013. Hrozby počítačovej kriminality. In *Manažment v teórii a v praxi*. [online]. 2013, roč. 9, č. 3, s. 4 – 16 [cit. 2015-12-04.] Dostupné na internete: <http://mtp.euke.sk/wp-content/uploads/2014/03/MTP-3-2013.pdf>. ISSN 1336-7137.
57. KOKLES, M. – KORČEK, F. 2015. Analýza rizík informačnej bezpečnosti v malých a stredných podnikoch. In *Ekonomika a manažment: Vedecký časopis Fakulty podnikového manažmentu Ekonomickej univerzity v Bratislave*. ISSN 1336-3301, 2015, roč. 12, č. 1, s. 38 – 55.
58. KOKLES, M. – ROMANOVÁ, A. 2014. *Informatika*. Bratislava: Sprint 2, 2014. 243 s. ISBN 978-80-89710-13-3.

59. KRÁL, D. 2011. Information Security in Small and Medium-Sized Companies. In *ACTA VŠFS*. ISSN 1802-792X, 2011, roč. 5, č. 1, s. 61 – 73.
60. LAUDON, K. C., – TRAVER, C. G. 2014. *E-commerce: business, technology, society*. 10th ed. New Jersey: Pearson, 2014. 804 s. ISBN 978-0-13-302444-9.
61. LOKHANDE, P. S. – MESHRAM, B. B. 2013. E-Commerce Applications: Vulnerabilities, Attacks and Countermeasures. In *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*. ISSN 2278-1323, 2013, vol. 2, no. 2, p. 499 – 509.
62. MANDIĆ, M. 2009. Privacy and security in e-commerce. In *Market-Tržište.* ISSN 0353-4790, 2009, vol. 21, no. 2, p. 247 – 260.
63. MARSHALL. 2008. *USC Marshall Institute Licenses New Information Security Model*. [online]. 2018 [cit. 2017-03-20]. Dostupné na internete: <https://www.marshall.usc.edu/news/releases/2008/usc-marshall-institute-licenses-new-information-security-model>.
64. MAYER, N. et al. 2008. Towards a Measurement Framework for Security Risk Management. In *Proceedings of the Workshop on Modeling Security (MODSEC08) held as part of the 2008 International Conference on Model Driven Engineering Languages and Systems (MODELS)*. Toulouse: CEUR–WS, 2008. ISSN 1613-0073.
65. MUTHAIYAH, S. – ERNEST, J. A. J. – WAI, C. K. 2004. Review Of E-commerce Issues: Consumes' Perception On Security And Privacy. In *International Business & Economics Research Journal*. ISSN 1535-0754, 2004, vol. 3, no. 9, p. 69 – 78.
66. NBÚ SR. 2016. *Strategické dokumenty*. [online]. Národný bezpečnostný úrad, 2016 [cit. 2017-02-27]. Dostupné na internete: <http://www.nbusr.sk/kyberneticka-bezpecnost/strategicke-dokumenty/index.html>.
67. NETOLICKÁ, B. 2012 (a). *Sociálne inžinierstvo v kontexte informačnej bezpečnosti v organizácii*. [online]. 2012 [cit. 2015-12-03]. Dostupné na internete: <http://www.eset.com/sk/firmy/services/clanky/socialne-inzinierstvo-ib/>.
68. NETOLICKÁ, B. 2012 (b). *5 zásad pre riadenie a presadzovanie informačnej bezpečnosti v organizácii.* [online]. 2012 [cit. 2015-12-05]. Dostupné na internete: <http://www.eset.com/sk/firmy/services/clanky/5-zasad-informacnej-bezpecnosti/>.
69. NIRANJARAMURTHY, M. – DHARMENDRA, CH. 2013. The study of E-Commerce Security Issues and Solutions. In *International Journal of Advanced Research in Computer and Communication Engineering* [online]. 2013, vol. 2, no. 3 [cit. 2017-03-27]. Dostupné na internete: <http://www.ijarcce.com/upload/2013/july/69-o-Niranjanamurthy%20-The%20study%20of%20E-Commerce%20Security%20Issues%20and%20Solutions.pdf>. ISSN 2278-1021.
70. NIST. 2014. *Framework for Improving Critical Infrastructure Cybersecurity.* [online]. National Institute of Standards and Technology, 2014. 39 s. [cit. 2017-03-14]. Dostupné na internete: <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.
71. NOVÁK, L. – POŽÁR, J. 2011. *Systém řízení informační bezpečnosti*. [online]. 2011 [cit. 2015-12-02]. Dostupné na internete: <http://www.cybersecurity.cz/data/SRIB.pdf>.
72. ONDRÁK, V. – SEDLÁK, P. – MAZÁLEK, V. 2013. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. 377 s. ISBN 978-80-7204-872-4.
73. PCI SSC. 2013. *Information Supplement: PCI DSS E-commerce Guidelines*. [online]. 2013 [cit. 2017-03-28]. Dostupné na internete:

<https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf>.

74. PCI SSC. 2017. *Information Supplement: Best Practices for Securing E-commerce*. [online]. 2017 [cit. 2017-03-28]. Dostupné na internete: <https://www.pcisecuritystandards.org/pdfs/best_practices_securing_ecommerce.pdf>.
75. PWC. 2015. *Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016.* [online]. 2015 [cit. 2015-12-03]. Dostupné na internete: <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html>.
76. RAKOVSKÁ, E. 2016. New aspects and tasks of knowledge management in the e-business era. In *11th International workshop on knowledge management: conference proceedings*. Trenčín: Vysoká škola manažmentu v Trenčíne, 2016. ISBN 978-80-89306-33-6. p. 79 – 86.
77. REVATHI, C. – SHANTHI, K. – SARANYA, A. R. 2015. A Study on E-Commerce Security Issues. In *International Journal of Innovative Research in Computer and Communication Engineering*. ISSN 2320-9798, 2015, vol. 3, no. 12, p. 12896 – 12901.
78. ROKOVANIE VLÁDY SR. 2015. *Akčný plán realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020.* [online]. 2017. [cit. 2017-02-27]. Dostupné na internete: <http://www.rokovania.sk/File.aspx/ViewDocumentHtml/Mater-Dokum-197723?prefixFile=m_>.
79. ROUSE, M. 2014. *E-business (electronic business)*. [online]. 2014 [cit. 2017-06-17]. Dostupné na internete: <http://searchcio.techtarget.com/definition/e-business>.
80. SAID, A. R. et al. 2013. Relationship between Organizational Characteristics and Information Security Knowledge Management Implementation. In *Taylor´s 6th Teaching and Learning Conference 2013: Transformative Higher Education Teaching and Learning in Practice (TTLC 2013)*, Selangor: Taylor´s University, 2013. p. 433 – 443.
81. SHARBAF, M. S. 2014. A New Perspective to Information Security: Total Quality Information Security Management. In *Proceedings of the 7th International Conference on Security of Information and Networks (SIN ˈ14)*, New York: ACM, 2014. ISBN 978-1-4503-3033-6, p. 56 – 60.
82. SHREDIT. 2017. *Security Tracker – Australia*. [online]. 2017 [cit. 2017-03-06]. Dostupné na internete: <https://www.shredit.com.au/getmedia/a4a2f8e5-6f4c-4368-bffe-4e1e557267cd/Shred-it_Security_Tracker_AUS.aspx?ext=.pdf>.
83. SCHIFF, J. L. 2015. *6 Biggest Business Security Risks and How You Can Fight Back.* [online]. 2015 [cit. 2015-11-13]. Dostupné na internete: <http://www.cio.com/article/2872517/data-breach/6-biggest-business-security-risks-and-how-you-can-fight-back.html?page=2>.
84. SINGH, A. N. et al. 2013. Information Security Management (ISM) Practices: Lessons from Select Cases from India and Germany. In *Global Journal of Flexible Systems Management*. ISSN 0972-2696, 2013, vol. 14, no. 4, p. 225 – 239.
85. SIVÁK, R. a kol. 2011. *Slovník znalostnej ekonomiky*. Bratislava: Sprint 2, 2011. 434 s. ISBN 978-80-89383-45-9.
86. SMEJKAL, V. – RAIS, K. 2013. *Řízení rizik ve firmách a jiných organizacích.* 4. vyd. Praha: Grada Publishing, 2013. 488 s. ISBN 978-80-247-4644-9.

87. STATDAT. 2017. *Ekonomické subjekty v RO podľa vybraných právnych foriem a kategórie počtu zamestnancov.* [online]. 2017 [cit. 2017-03-04]. Dostupné na internete: <https://goo.gl/TAKlhc>.
88. STEHLÍKOVÁ, B. – HOROVČÁK, P. 2012. Manažment informačnej bezpečnosti v malých a stredných podnikoch. In *Security Revue.* [online]. 2012 [cit. 2015-12-01]. Dostupné na internete: <http://www.securityrevue.com/article/2012/06/ manazment-informacnej-bezpecnosti-v-malych-a-strednych-podnikoch/>.
89. STN ISO/IEC 27000: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Prehľad a slovník.*
90. STN ISO/IEC 27001: 2014: *Informačné technológie – Bezpečnostné metódy – Systémy riadenia informačnej bezpečnosti – Požiadavky.*
91. STN ISO/IEC 27002: 2014: *Informačné technológie – Bezpečnostné metódy – Pravidlá dobrej praxe riadenia informačnej bezpečnosti.*
92. STN ISO/IEC 27005: 2012: *Informačné technológie – Bezpečnostné metódy – Riadenie rizík informačnej bezpečnosti.*
93. STRNÁD, O. 2011. *Systém riadenia informačnej bezpečnosti.* Ostrava: Amos, 2011. 241 s. ISBN 978-80-904766-6-0.
94. SUCHÁNEK, P. 2012. *E-commerce: Elektronické podnikání a koncepce elektronického obchodování.* Praha: Ekopress, 2012. 144 s. ISBN 978-80-86929-84-2.
95. SUTN.SK. 2017. *Zoznam vybraných noriem*. [online]. Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2017 [cit. 2017-02-25]. Dostupné na internete: <https://www.sutn.sk/eshop/public/search.aspx>.
96. ŠÚBERTOVÁ, E. a kol. 2014. *Podnikanie v malých a stredných podnikoch: modelové príklady.* Bratislava: KARTPRINT, 2014. 135 s. ISBN 978-80-89553-21-1.
97. ÚNMZ CZ. 2017. *Podrobné vyhledávání v normách.* [online]. Úřad pro technickou normalizáci, metrologii a státní zkušebnictví, 2017 [cit. 2017-02-25]. Dostupné na internete: <http://seznamcsn.unmz.cz/vyhledavani.aspx>.
98. ÚOOÚ SR. 2017. *Národný právny rámec.* [online]. Úrad na ochranu osobných údajov Slovenskej republiky, 2017 [cit. 2017-06-15]. Dostupné na internete: <https://dataprotection.gov.sk/uoou/sk/content/narodny-pravny-ramec>.
99. WIRADINATA, T. 2017. Nascent entrepreneurs in e-marketplace: The effect of founders' self-efficacy and personality. In *International Journal of Electronic Business*. ISSN 1470-6067, 2017, vol. 13, no. 2/3, p. 163 – 182.
100. WU, X. F. – ZHOU, J. – YUAN, X. 2012. The Research of Factors which Effect B2C E-commerce Trust – Based on the Mechanism of Process. In *Advanced Materials Research*. ISSN 1662-8985, 2012, vols. 591-593, p. 2583 – 2586.
101. YAZDANIFARD, R. – EDRES, N. A. H. – SEYEDI, A. P. 2011. In *International Proceedings of Computer Science and Information Technology*. [online]. 2011, vol. 16 [cit. 2017-03-28]. Dostupné na internete: <http://www.ipcsit.com/vol16/5-ICICM2011M008.pdf>. ISSN 2010-460X.

Prílohy

Príloha 1: Význam informačných aktív podniku podľa respondentov

Príloha 2: Pravdepodobnosti výskytu hrozieb IB podľa respondentov

Príloha 3: Matica priemerných mier rizík informačnej bezpečnosti

Príloha 1: Význam informačných aktív podniku podľa respondentov

Číslo	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
IA01	1	4	4	1	3	1	1	1	1	4	4	4	2	4	3	4	1	1	4	4	4	4	4	1	4	4	4	2	4	4	4	3	4	4	4	4	4	4	4	4	4	3	3	4	4	4
IA02	3	4	3	1	4	1	2	1	1	2	4	4	2	4	4	4	1	1	2	4	3	1	4	1	4	4	4	2	4	4	4	1	3	4	3	4	4	4	4	4	3	4	4	1	4	4
IA03	3	4	4	1	4	4	4	3	1	4	4	4	3	4	4	4	1	4	4	4	4	4	4	4	4	4	1	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
IA04	4	4	1	1	3	4	2	2	1	3	4	4	3	2	1	4	1	1	4	4	4	1	4	4	4	3	1	2	4	4	4	4	4	4	1	4	4	4	4	1	4	4	4	3	3	4
IA05	2	4	3	3	4	2	2	2	2	2	3	4	3	2	4	4	1	4	4	3	4	3	4	2	4	2	1	2	4	3	4	4	4	4	4	4	2	4	4	4	3	4	3	3	3	4
IA06	1	4	4	4	3	1	1	4	2	3	4	4	3	2	4	4	4	4	3	3	4	4	4	2	4	2	4	2	4	4	4	3	4	3	2	3	2	4	4	4	3	4	1	4	3	4
IA07	2	4	4	3	3	4	3	4	1	3	4	4	2	4	4	4	1	2	4	4	4	1	4	2	4	3	2	2	4	4	4	4	4	3	4	4	4	3	4	4	2	4	1	3	4	4
IA08	2	4	1	4	4	1	1	4	1	1	3	4	3	2	3	4	4	1	3	3	4	1	4	1	4	1	1	2	4	4	4	4	4	3	4	3	3	4	2	4	3	4	3	2	1	4
IA09	4	4	1	3	4	2	2	3	1	4	4	4	3	4	3	4	4	4	4	2	4	1	4	1	4	4	1	2	4	4	4	3	4	3	3	4	4	4	3	4	4	4	3	2	4	4
IA10	2	4	1	4	4	1	2	3	1	4	4	4	3	4	2	4	4	1	4	3	4	3	4	1	4	1	4	2	4	3	4	4	4	3	4	4	3	4	3	4	4	4	4	2	4	4
IA11	1	4	1	4	4	4	1	3	1	1	4	4	3	2	1	4	4	4	3	3	4	1	4	1	4	1	1	2	4	4	4	3	4	4	2	1	2	4	2	1	3	4	1	2	1	4
IA12	2	4	3	4	4	4	1	4	1	3	4	4	2	2	3	4	4	4	2	3	4	1	4	4	4	4	1	2	4	4	4	1	4	4	2	3	3	4	2	4	2	4	1	3	4	4
IA13	2	3	2	4	4	4	4	3	2	3	4	4	2	3	3	4	4	2	1	3	4	1	3	2	4	1	1	2	4	4	4	3	4	4	4	4	4	4	1	1	4	4	1	2	1	4
IA14	2	3	4	4	4	1	3	3	1	3	4	4	3	2	4	4	4	4	4	3	4	1	4	2	4	4	1	2	4	3	4	3	4	3	4	4	4	4	2	4	3	4	1	3	4	4
IA15	2	3	3	4	4	1	3	3	2	1	4	4	1	2	3	4	4	1	3	3	4	1	4	1	4	4	1	2	4	2	4	3	4	4	4	4	1	4	2	1	2	4	1	2	4	4
IA16	1	3	4	3	3	1	1	3	1	1	3	4	2	4	3	4	1	1	3	3	4	1	4	1	4	2	1	2	4	1	4	3	4	4	4	4	3	4	1	3	1	2	1	2	4	4
IA17	2	3	1	4	4	4	1	3	2	1	4	4	3	4	3	4	1	1	3	3	4	1	2	3	4	1	1	2	4	3	4	3	3	3	2	4	4	4	1	1	1	4	1	1	1	4
IA18	2	3	4	4	4	3	4	1	2	1	3	4	3	4	3	4	1	1	4	3	3	1	3	4	4	1	1	2	4	4	4	3	4	4	2	4	4	4	1	1	1	4	3	3	1	4
IA19	2	3	4	4	4	3	3	3	2	3	4	4	3	4	4	4	1	4	3	3	3	1	3	4	4	1	1	2	4	4	4	2	4	3	2	4	4	4	3	2	1	4	1	3	4	4
IA20	2	3	4	4	4	3	1	3	1	1	3	4	3	4	3	4	1	4	3	3	4	1	4	3	4	1	1	2	4	3	4	3	1	4	4	3	4	4	3	1	2	4	1	2	1	4
IA21	2	3	1	4	4	1	1	1	1	4	4	4	2	4	1	4	1	4	3	3	4	1	4	1	4	3	1	2	4	3	4	2	4	3	2	4	4	4	1	1	1	4	3	2	4	4
IA22	3	4	4	4	4	1	3	3	2	4	4	4	3	4	4	4	4	1	3	3	4	1	4	3	4	1	4	2	4	4	4	2	4	4	4	4	4	4	4	4	4	4	4	4	4	4
IA23	4	4	3	4	4	4	3	4	1	3	4	4	2	4	4	4	1	4	2	3	4	1	4	4	4	1	1	2	4	4	4	4	4	4	1	4	4	4	3	3	3	4	1	3	4	4
IA24	2	4	2	4	4	4	1	4	2	3	3	4	2	4	3	4	1	3	3	3	4	1	3	4	4	3	1	2	4	2	3	4	4	3	2	3	4	4	4	1	3	4	1	4	4	4
IA25	2	4	2	3	4	3	1	4	2	1	2	4	1	4	3	4	1	1	1	3	4	3	3	1	4	1	1	2	4	1	4	2	4	3	2	1	1	3	4	1	1	4	1	4	3	4
IA26	3	4	4	3	4	4	4	4	2	4	4	4	2	4	3	4	1	4	4	4	4	1	4	1	4	3	1	2	4	4	4	4	4	4	4	4	4	3	4	4	2	4	4	2	4	4
IA27	2	4	4	3	4	4	2	4	1	1	4	4	3	4	2	4	1	1	4	4	4	1	4	4	4	3	1	2	4	3	4	3	4	4	4	4	4	4	4	4	3	4	4	2	3	4
IA28	3	4	4	3	4	4	4	4	2	4	4	4	3	4	4	4	4	3	4	4	4	1	4	4	4	3	4	2	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4
IA29	3	4	4	4	4	4	1	4	2	1	2	1	3	4	1	4	1	1	3	4	4	1	4	2	4	1	1	2	4	3	4	1	4	1	1	4	4	3	1	1	4	4	1	1	1	4
IA30	4	4	1	4	4	4	4	1	2	1	4	4	3	3	1	4	4	4	4	4	4	1	4	2	4	3	1	2	4	4	4	4	4	4	4	4	4	4	4	1	4	4	4	3	1	4
IA31	4	4	1	4	4	1	2	1	2	1	4	4	3	3	1	4	4	2	4	4	4	1	4	1	4	1	1	2	4	4	4	2	4	4	4	4	4	4	4	1	4	4	4	1	1	4
IA32	4	4	1	4	4	4	1	1	2	1	4	4	3	3	1	4	4	1	4	4	4	1	4	1	4	1	1	2	4	4	4	3	4	4	4	3	4	4	4	1	3	4	1	1	1	4
IA33	3	3	1	4	4	1	4	1	2	1	3	1	3	1	3	4	1	4	3	4	4	1	4	1	3	1	1	2	4	4	4	3	2	4	1	1	4	3	2	1	3	4	1	4	1	3
IA34	2	3	1	4	4	1	3	1	1	1	2	1	3	1	3	4	1	1	3	4	4	1	4	1	3	2	1	2	4	4	3	2	2	2	1	1	4	3	2	1	2	4	4	1	1	3
IA35	2	3	1	3	4	4	1	1	2	1	4	1	2	1	1	4	1	3	3	4	4	1	4	1	4	1	1	2	4	4	4	3	4	4	1	1	4	3	2	1	1	4	1	1	1	4
IA36	2	3	1	4	4	4	1	1	1	1	4	1	3	1	1	4	1	4	3	4	4	1	4	1	3	3	1	2	4	4	1	1	4	2	1	1	3	3	1	1	1	4	1	1	3	4
IA37	2	3	1	1	4	3	1	1	2	1	4	1	2	1	1	4	1	1	1	3	4	1	3	1	1	1	1	2	4	4	1	1	3	4	1	1	2	1	1	1	1	4	1	4	4	2
IA38	1	3	1	1	4	3	2	1	2	1	4	4	3	3	4	4	1	1	1	3	4	1	1	1	4	1	1	2	4	4	1	1	4	4	1	4	2	3	4	1	1	4	4	2	4	3

Číslo	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91
IA01	4	4	4	4	4	4	4	4	4	4	3	4	3	4	4	4	4	4	4	2	4	2	1	4	2	3	4	1	4	1	4	1	3	1	4	3	3	3	4	3	3	4	4	4	1
IA02	4	4	4	3	4	4	4	4	4	4	4	4	2	4	4	2	4	2	1	4	4	2	4	4	1	3	3	1	4	3	4	1	3	4	4	4	4	3	3	4	3	4	4	4	1
IA03	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	1	4	4	2	4	4	4	4	1	4	1	3	4	4	4	3	4	4	4	3	4	4	4	4
IA04	4	3	4	4	4	3	1	4	3	4	4	4	4	4	4	4	1	4	4	3	4	1	4	4	2	4	4	4	3	3	4	1	3	2	4	1	3	4	3	3	3	4	4	4	1
IA05	4	4	4	4	3	4	4	4	4	4	3	4	4	4	4	3	4	3	1	3	4	1	4	4	1	3	4	3	3	1	4	2	3	1	4	3	3	4	4	4	3	4	4	4	1
IA06	4	4	3	3	4	3	2	4	4	3	3	4	4	4	4	3	4	3	1	4	1	1	3	2	3	3	3	4	2	1	4	2	4	3	4	4	3	4	4	2	3	4	4	4	4
IA07	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	3	1	3	4	1	4	3	3	3	3	4	3	2	4	2	4	3	4	4	3	3	4	4	3	3	4	4	4
IA08	1	4	3	4	4	3	1	4	4	4	3	4	3	4	4	4	4	1	1	3	1	1	4	2	1	3	3	2	4	4	3	2	4	2	4	3	3	4	3	3	3	4	4	4	1
IA09	4	4	4	2	4	4	1	4	4	4	3	4	4	3	4	4	4	1	1	3	1	2	4	3	1	3	4	4	1	1	4	4	4	3	4	3	4	3	3	3	3	4	4	3	4
IA10	4	4	4	3	4	4	3	4	4	4	3	4	4	3	4	4	4	3	4	3	4	3	4	4	2	3	4	4	1	2	4	4	4	1	4	3	2	3	3	4	3	4	4	3	4
IA11	4	4	4	2	4	4	1	4	4	4	3	4	4	3	1	4	4	1	3	3	2	3	3	2	3	4	2	4	1	2	4	2	4	3	4	2	3	3	3	1	3	3	4	3	4
IA12	4	4	4	1	4	4	2	4	4	4	3	4	4	3	4	4	4	2	1	3	2	3	4	2	2	4	2	4	1	3	4	1	4	4	4	2	3	3	4	1	3	4	4	3	4
IA13	4	4	4	1	4	4	1	1	4	4	4	4	4	4	4	4	4	2	3	3	2	2	4	4	2	2	3	4	2	1	4	3	4	4	4	2	3	4	4	4	3	3	4	3	1
IA14	4	1	4	3	4	3	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	2	4	4	1	2	3	4	2	1	4	4	4	1	4	3	2	3	4	4	3	3	4	3	1
IA15	4	1	4	3	4	3	3	2	3	4	4	4	3	3	4	4	4	4	3	3	3	2	4	1	3	2	3	4	3	1	4	4	4	2	4	3	2	3	3	1	3	1	4	3	1
IA16	1	1	4	1	4	4	3	4	3	3	4	4	4	3	1	4	4	3	1	4	3	2	1	3	1	2	3	4	1	1	3	3	4	1	4	1	3	3	3	2	3	2	4	2	1
IA17	1	1	4	1	4	2	1	1	4	3	3	4	1	1	1	4	4	1	1	3	3	2	1	3	2	2	2	4	1	1	4	1	4	4	4	1	3	1	3	4	3	3	4	3	1
IA18	3	1	4	1	4	3	1	1	4	4	4	4	4	4	1	4	4	1	3	4	1	2	1	3	2	3	2	4	3	1	3	4	4	1	4	3	3	1	1	4	3	2	3	2	4
IA19	3	1	4	1	4	3	2	4	4	4	4	4	1	4	1	4	4	4	3	4	2	2	4	3	2	2	2	4	3	1	4	4	4	1	4	2	3	3	4	1	3	1	3	2	4
IA20	3	1	4	1	4	3	4	4	4	4	3	4	4	4	1	4	4	1	1	4	2	2	4	3	2	3	3	4	3	1	4	4	4	3	4	1	3	4	3	1	3	3	3	2	1
IA21	3	1	4	1	4	3	1	3	4	4	3	4	4	1	1	4	4	1	1	4	2	2	1	4	1	4	4	4	1	1	4	3	4	3	4	1	3	1	1	4	3	4	4	2	1
IA22	4	4	4	4	4	4	3	4	4	4	3	4	4	2	3	4	4	4	4	4	1	3	3	4	2	3	4	4	4	2	4	4	4	3	4	4	2	4	4	4	3	4	4	2	4
IA23	4	4	4	1	4	3	2	4	4	4	3	4	3	4	4	4	4	2	1	4	1	3	3	4	3	4	3	4	3	1	4	4	4	1	4	1	3	3	4	2	3	4	4	2	4
IA24	4	1	3	1	4	2	3	4	3	3	4	4	3	1	1	4	4	3	1	4	2	2	3	2	2	4	2	4	3	1	4	4	4	3	4	1	3	3	4	1	3	3	4	2	4
IA25	3	1	3	1	4	3	1	1	3	4	2	4	1	1	1	1	4	4	3	4	2	2	4	1	1	2	2	4	3	1	3	4	4	1	4	1	3	2	4	1	3	3	4	2	1
IA26	4	1	4	1	3	3	3	4	3	4	3	4	4	4	4	4	4	4	1	4	1	2	2	4	2	3	4	4	2	1	3	4	4	4	4	4	3	3	4	1	3	4	4	2	4
IA27	4	4	4	1	4	3	3	4	4	4	3	4	4	4	1	4	4	3	4	4	2	3	4	4	3	3	4	4	2	1	3	2	4	2	4	4	3	2	4	4	3	4	4	2	4
IA28	4	4	4	3	4	4	4	4	4	4	3	4	4	3	4	4	4	4	4	4	2	3	4	4	3	3	4	4	4	1	4	4	4	2	4	4	3	3	4	4	3	4	4	2	4
IA29	4	1	4	1	4	4	3	1	4	4	3	4	4	4	1	4	4	2	1	4	2	2	1	3	1	3	4	4	3	1	3	4	1	2	4	1	3	1	4	2	3	4	4	2	4
IA30	4	4	4	4	4	3	1	2	4	4	4	4	4	3	4	4	1	4	4	4	2	2	1	4	2	4	4	4	4	1	4	3	4	3	4	1	3	4	4	4	3	4	4	2	4
IA31	4	1	4	4	3	3	1	4	4	4	3	4	4	3	4	4	1	4	4	4	3	2	1	4	2	4	4	4	4	1	4	3	4	3	4	1	3	4	4	3	3	4	4	2	1
IA32	4	1	4	4	4	3	1	4	4	4	3	4	4	3	1	4	1	2	4	4	3	2	1	3	2	4	4	4	4	1	4	4	4	3	4	1	3	3	4	3	3	4	4	2	1
IA33	4	1	3	1	4	4	3	3	3	3	3	4	4	2	1	1	4	1	3	4	1	2	3	1	2	3	1	4	1	1	1	1	4	4	3	1	3	4	1	1	3	2	4	2	1
IA34	4	1	4	1	4	4	1	1	4	3	3	4	4	2	1	4	4	2	3	4	1	2	1	1	1	3	1	4	1	1	1	1	4	2	3	1	3	4	1	1	3	2	4	2	1
IA35	4	1	4	1	4	4	1	1	4	4	3	4	3	2	1	4	4	1	4	4	1	2	1	3	1	3	2	4	2	1	3	1	4	1	4	1	4	3	1	1	3	3	3	2	1
IA36	4	1	4	1	4	4	1	3	3	3	3	4	4	2	1	1	4	1	1	4	1	2	1	4	2	2	2	4	2	1	3	1	4	1	4	1	2	2	1	1	3	3	3	2	1
IA37	1	1	4	1	4	3	1	3	3	3	3	4	2	2	1	1	1	1	4	4	1	2	1	3	1	3	2	1	1	1	1	1	4	1	3	1	3	4	1	1	3	2	2	2	1
IA38	4	1	4	1	4	4	2	1	3	3	3	4	4	2	1	4	4	1	1	4	4	2	1	3	1	3	4	3	2	1	1	1	4	1	3	1	2	4	3	4	3	2	4	2	1

Zdroj: vlastné spracovanie

Príloha 2: Pravdepodobnosti výskytu hrozieb IB podľa respondentov

Číslo	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46
HR01	2	1	1	3	1	3	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	2	2	1	1	2	1	2	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1
HR02	1	1	1	2	1	1	1	1	2	1	1	1	1	1	2	1	2	1	1	1	1	1	2	1	1	2	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
HR03	2	1	1	3	2	1	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR04	1	1	1	2	2	1	1	1	2	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	3	1	1	1	1	1	1	1	1	1	1
HR05	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1
HR06	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR07	2	1	1	3	1	3	1	4	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	3	2	1	1	1	1	3	1	1	1	1	1	1
HR08	2	3	1	4	3	3	1	4	3	1	1	1	1	1	3	1	2	1	1	1	1	3	2	1	1	3	1	2	1	1	1	2	1	3	3	1	1	1	1	3	4	1	1	1	4	1
HR09	2	3	1	4	3	3	1	4	3	2	1	1	1	1	1	1	2	2	1	1	1	1	3	1	3	3	1	2	1	1	1	2	1	2	4	3	1	1	1	4	1	1	1	1	4	1
HR10	1	3	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	3	1	1	1	1	1	1	1	4	1	1	1
HR11	2	3	1	1	2	1	1	1	3	1	1	1	1	1	1	1	2	1	3	1	1	2	1	1	1	3	1	2	1	3	1	2	1	1	2	1	1	1	1	1	1	1	1	1	1	1
HR12	1	3	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR13	2	3	1	1	2	1	1	1	3	1	1	1	1	1	1	1	1	4	1	1	1	1	1	1	1	4	1	2	2	2	1	1	1	1	1	1	3	1	1	1	3	1	1	1	1	1
HR14	1	3	1	2	3	1	1	1	3	1	1	1	1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	2	2	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR15	1	3	1	2	2	1	1	1	4	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1
HR16	2	3	1	3	2	1	1	1	4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR17	2	3	1	3	1	1	1	1	4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	2	1	3	1	1	1
HR18	3	3	1	2	2	2	2	4	3	1	1	1	2	2	2	1	2	1	1	1	1	1	3	1	1	3	1	2	1	3	1	2	1	1	1	3	2	1	1	2	4	1	4	1	2	1
HR19	3	3	1	2	2	2	1	4	3	1	1	1	1	2	1	1	2	1	1	1	1	1	1	1	1	2	1	2	1	2	1	1	1	1	3	3	2	1	1	1	4	1	4	1	2	1
HR20	3	3	1	2	1	2	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	1	2	1	2	1	1	1	3	1	1	1	1	1	1	4	1	1	1
HR21	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR22	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR23	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR24	2	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR25	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR26	2	2	1	1	1	1	1	1	3	2	1	1	1	1	1	1	2	2	1	1	1	1	2	1	2	1	1	2	1	1	1	2	1	2	1	1	1	1	1	1	2	1	1	1	1	1
HR27	2	2	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1
HR28	3	1	1	2	2	2	2	4	2	3	1	1	1	1	1	1	2	1	1	1	1	1	1	4	1	3	1	3	1	2	1	2	1	1	1	4	1	1	1	1	3	1	4	1	2	1
HR29	3	1	1	3	1	1	2	4	3	3	1	1	1	1	1	1	2	1	1	1	1	1	1	4	1	1	1	2	1	1	1	1	1	1	1	3	1	1	1	1	3	1	4	1	1	1
HR30	1	1	1	1	2	1	1	1	3	3	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	2	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR31	1	1	1	2	2	1	1	1	3	3	1	1	1	1	1	1	1	1	1	1	1	4	1	1	1	1	1	2	1	1	1	2	1	1	1	1	3	1	1	1	1	1	1	1	1	1
HR32	2	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1
HR33	2	1	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	1	1
HR34	2	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR35	1	1	1	2	1	1	1	1	3	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR36	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	3	1	2	1	1	1
HR37	3	1	1	2	1	1	2	1	3	3	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1	2	2	1	1	2	1	1	1	1	3	1	1	1	3	1	1	1	1	1
HR38	1	1	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1
HR39	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR40	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR41	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR42	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1
HR43	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1
HR44	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1
HR45	2	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	2	1	2	2	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
HR46	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1
HR47	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1
HR48	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
HR49	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Číslo	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91
HR01	1	1	1	1	1	1	1	1	3	1	1	3	1	1	1	3	1	1	1	3	1	1	2	2	1	3	2	3	1	1	1	1	1	1	1	1	3	1	3	2	2	1	1	3	1
HR02	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	3	1	1	1	3	2	3	1	1	1	1	1	1	1	1	3	1	1	1	3	1	1	3	1
HR03	1	1	1	1	1	1	2	1	1	1	1	3	1	1	1	1	1	1	1	3	2	3	1	1	1	2	2	1	1	1	1	1	1	1	1	1	4	1	3	1	2	2	1	3	1
HR04	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	1	3	1	4	1	1	1	2	3	1	1	1	1	1	1	1	1	1	3	1	1	1	3	1	1	3	1
HR05	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	2	3	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1	3	1	1	1	3	1	1	3	1
HR06	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	2	1	1	1	3	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	3	1
HR07	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	3	1	1	1	2	2	3	1	3	2	2	1	2	1	1	1	1	1	1	1	1	3	1	1	1	3	1	1	2	1
HR08	1	1	2	2	1	1	1	3	1	1	1	1	1	1	1	3	1	1	1	2	2	3	3	1	2	2	4	2	1	1	1	1	1	1	1	1	4	1	3	2	3	1	1	2	1
HR09	1	1	1	1	1	1	1	3	1	2	1	1	1	1	1	3	1	3	1	2	2	3	3	1	2	2	4	2	2	1	1	1	1	1	1	1	2	2	3	4	3	1	2	2	1
HR10	1	4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	1	2	1	2	1	1	1	2	2	1	1	1	1	1	1	2	1	2	3	1	1	1	3	1	1	2	1
HR11	3	4	1	1	1	1	1	1	3	1	1	1	2	1	1	2	1	2	1	2	1	2	1	1	1	2	2	3	2	1	1	1	2	2	1	1	3	1	1	1	3	1	1	2	1
HR12	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	1	2	1	1	1	2	2	1	1	1	1	1	1	1	1	1	3	1	1	1	3	1	1	2	1
HR13	4	4	1	1	1	1	1	1	1	1	1	1	2	1	4	1	1	1	1	2	1	2	1	1	1	1	3	1	1	1	1	1	1	1	1	2	3	2	1	2	3	1	2	2	1
HR14	1	4	1	1	1	1	1	1	1	1	1	1	2	1	4	1	1	1	1	2	1	3	1	1	1	2	2	1	1	1	1	1	1	1	1	1	3	1	1	2	3	1	1	2	4
HR15	1	4	1	1	1	1	1	1	1	1	1	1	1	1	4	1	1	1	1	2	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	3	1	3	1	1	2	1
HR16	1	4	1	1	1	1	1	1	1	1	1	1	2	1	4	1	1	1	1	2	1	2	1	1	1	1	2	1	1	1	1	1	1	2	1	1	3	1	3	1	3	1	1	2	4
HR17	1	4	1	1	1	1	1	1	2	2	1	1	1	1	4	1	1	1	2	2	1	3	1	1	1	1	3	1	1	3	1	1	1	1	1	2	3	1	3	2	3	2	1	2	4
HR18	4	1	2	1	1	1	1	1	3	1	1	2	1	3	1	3	3	1	1	2	1	3	1	2	1	1	4	2	1	1	1	1	1	1	1	1	2	1	3	4	3	1	1	2	1
HR19	4	1	2	1	1	1	1	1	3	1	1	2	2	3	1	1	3	2	1	2	2	3	2	2	2	1	3	2	1	2	1	1	1	1	1	1	2	1	3	4	3	1	1	2	1
HR20	4	1	2	1	1	1	1	2	2	1	1	1	1	3	1	1	3	2	1	2	2	3	1	1	3	1	3	2	1	2	1	1	1	1	1	1	2	1	3	1	3	1	1	2	1
HR21	1	1	1	1	1	1	1	1	1	1	1	1	2	3	1	1	1	2	1	2	1	3	1	1	1	1	3	1	1	1	1	1	1	1	1	1	2	1	1	2	3	1	1	2	1
HR22	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	3	2	1	3	1	1	1	1	3	1	1	1	1	1	1	1	1	1	2	1	1	1	3	1	1	2	1
HR23	1	1	1	1	1	1	1	1	3	1	1	1	1	2	1	1	1	2	3	2	1	3	1	1	1	1	3	1	1	1	1	1	1	1	1	1	2	1	1	2	3	1	1	2	1
HR24	1	1	1	1	1	1	1	1	1	2	1	1	1	3	1	1	3	2	3	2	1	3	1	1	1	1	2	2	1	2	1	1	1	1	1	1	2	1	1	2	3	1	2	2	1
HR25	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	4	2	1	3	1	1	1	1	3	1	1	1	1	1	1	1	1	1	3	1	1	2	3	1	1	2	1
HR26	1	1	1	1	1	1	1	2	1	2	1	2	1	1	1	1	1	2	3	2	1	3	1	1	1	1	4	1	1	1	1	1	1	1	1	1	2	1	1	2	2	1	1	2	1
HR27	1	1	1	1	1	1	1	2	1	2	1	2	1	1	1	1	1	1	1	2	1	3	1	1	1	1	3	1	1	1	1	1	1	1	1	1	2	1	1	2	3	1	1	2	1
HR28	4	1	1	1	1	1	1	3	1	2	1	2	1	1	3	2	1	3	3	2	1	4	1	2	1	1	3	1	1	2	1	1	1	1	1	1	4	1	3	3	3	1	2	2	1
HR29	1	1	1	1	1	1	2	3	1	2	1	2	1	1	3	1	1	3	3	2	1	3	1	2	2	1	4	1	1	3	1	1	1	1	1	1	3	3	1	3	3	1	1	2	1
HR30	1	4	1	1	1	3	1	1	1	1	1	2	1	1	1	1	1	3	2	2	1	2	1	1	1	1	3	1	1	1	1	1	1	1	1	1	4	1	1	2	1	1	1	2	1
HR31	1	4	1	1	1	4	1	2	1	2	1	3	1	1	1	1	1	2	4	2	1	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	4	1	1	1	2	1
HR32	1	4	1	1	1	3	1	1	3	1	1	3	1	1	1	1	1	3	3	2	1	3	1	1	1	1	3	1	1	2	1	1	1	1	1	2	2	1	1	2	1	1	1	2	1
HR33	1	4	1	1	1	2	1	1	1	1	1	3	1	2	1	1	1	3	1	2	1	3	1	1	1	1	3	1	1	2	1	1	1	1	1	1	3	1	1	2	1	1	1	2	1
HR34	1	4	1	1	1	3	1	1	1	1	1	3	1	2	1	1	1	3	3	2	1	3	1	1	1	1	3	1	1	1	1	1	1	1	1	1	3	1	1	2	1	1	1	2	1
HR35	1	4	1	1	1	2	1	1	1	1	1	3	1	1	1	1	1	3	3	2	1	3	1	1	1	1	4	1	1	1	1	1	1	1	1	1	3	1	1	2	1	1	1	2	1
HR36	1	4	1	1	1	2	1	1	1	1	1	3	1	1	1	1	1	3	3	2	1	3	1	1	1	1	3	1	2	3	1	1	1	1	1	2	2	1	1	2	1	2	1	2	1
HR37	1	4	1	1	1	3	1	1	3	1	1	3	1	1	1	2	1	2	3	2	2	3	1	1	1	1	3	1	1	3	1	1	1	1	1	2	2	1	1	3	1	1	1	2	4
HR38	1	1	1	1	1	3	1	1	1	1	1	3	1	1	1	1	1	3	2	2	1	3	1	1	1	1	3	1	1	1	1	1	3	1	1	2	3	1	1	2	1	1	1	2	1
HR39	1	1	1	1	1	3	1	1	1	1	1	3	2	1	1	1	1	2	3	2	1	2	1	1	1	1	2	1	1	1	1	1	3	1	1	2	2	1	1	2	1	1	1	2	1
HR40	1	1	1	1	1	2	1	1	1	2	1	3	1	1	1	1	1	2	1	2	1	3	1	1	1	1	2	1	1	1	1	1	4	1	1	1	2	1	1	2	1	1	1	2	1
HR41	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	3	1	1	1	1	2	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	2	1
HR42	1	1	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	3	2	1	3	1	1	1	1	3	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1
HR43	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	3	2	1	3	1	1	1	1	3	1	1	1	1	1	1	4	1	1	3	1	1	1	2	1	1	2	1
HR44	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	3	1	1	1	1	2	1	1	1	1	1	1	1	1	1	3	1	1	1	1	1	1	2	1
HR45	1	4	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	3	1	1	1	1	3	1	1	1	1	1	4	3	1	1	3	1	1	3	1	1	1	2	1
HR46	1	4	3	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	3	1	1	1	1	2	1	1	1	1	1	3	2	1	1	3	1	1	1	1	1	1	2	1
HR47	1	1	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	2	1	3	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1
HR48	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	3	1	1	1	1	2	1	1	1	1	1	1	1	1	1	3	1	1	2	1	1	1	2	1
HR49	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	3	2	1	3	1	1	1	1	2	1	1	1	1	1	1	2	1	1	2	1	1	2	1	1	1	2	1

Zdroj: vlastné spracovanie

Príloha 3: Matica priemerných mier rizík informačnej bezpečnosti

Riziko	HR01	HR02	HR03	HR04	HR05	HR06	HR07	HR08	HR09	HR10	HR11	HR12	HR13	HR14	HR15	HR16	HR17	HR18	HR19	HR20	HR21	HR22	HR23	HR24	HR25
IA01	4,41	3,90					4,20	5,32	5,52		4,65		4,73	4,29	4,15	4,22	4,54	5,51	5,31	4,69	3,80			4,02	3,99
IA02										4,12	4,49	3,65	4,68	4,23	4,04	4,18	4,49		5,29	4,63	3,73	3,60	3,75	3,92	3,81
IA03											5,24	4,20	5,33	4,93	4,63	4,84	5,13		6,02	5,26	4,26	4,19	4,33	4,54	4,36
IA04										4,01	4,55	3,68	4,60		4,01	4,14	4,46	5,42	5,25	4,69	3,75	3,67	3,78	3,95	3,84
IA05										4,14	4,63	3,75	4,74	4,41	4,21	4,32		5,52	5,35	4,71	3,80	3,67	3,82	4,01	3,84
IA06										4,05	4,65	3,73	4,69	4,49	4,20	4,42			5,16	4,59	3,75	3,65	3,78	4,00	3,84
IA07	4,71	4,11	4,27							4,23	4,82	3,87	4,84	4,57	4,29	4,54		5,71	5,55	4,87	3,92	3,79	3,93	4,13	3,97
IA08										3,78	4,21	3,40	4,18		3,82	3,98	4,27	5,03	4,85	4,21	3,43	3,32	3,45	3,67	3,48
IA09										4,10	4,73		4,88	4,54	4,19	4,42	4,66	5,70	5,43	4,68	3,78	3,65	3,78	4,02	3,81
IA10										4,25	4,74		4,71	4,58	4,25	4,48	4,85	5,75	5,62		3,90	3,85	3,99	4,19	4,09
IA11										3,63	4,22		4,14		3,70	3,92	4,10	4,81	4,67	4,20	3,34	3,31	3,42	3,66	3,46
IA12	4,46	3,93	4,04			3,53				3,92	4,54	3,59	4,62	4,41	4,07	4,31	4,47	5,30	5,12	4,53	3,63	3,54	3,65	3,91	3,64
IA13	4,42	3,79	3,96	3,91	3,58	3,42	4,15	5,08			4,42	3,53				4,18		5,36		4,45	3,63				
IA14	4,56	4,02	4,18	4,09	3,86	3,59	4,33	5,46			4,56					4,18		5,59			3,81				
IA15	4,11	3,66	3,76	3,74	3,40	3,24	3,88	4,95	5,19		4,19					3,85		4,91			3,42				
IA16	3,77	3,34	3,45	3,40	3,16	2,99	3,67	4,51			3,70					3,43		4,47			3,15				
IA17	3,73	3,20	3,36	3,29	3,01	2,86	3,56				3,62					3,37		4,41			2,96				
IA18											4,01				3,45	3,70	3,92	4,84	4,60	4,10	3,33	3,24	3,40		
IA19											4,15				3,73	3,91	4,07	5,02	4,84		3,48	3,46	3,58		
IA20											4,08				3,57	3,73	3,84	4,85	4,71	4,19	3,38	3,29	3,40		
IA21											3,92				3,36	3,52	3,71	4,71	4,51	3,96	3,21	3,11	3,25		
IA22									6,05		4,96				4,44	4,68	5,03	6,00	5,81		4,08	4,02	4,18		
IA23											4,55				4,16	4,41	4,59	5,57	5,30		3,77	3,65	3,77		
IA24											4,22				3,70	3,97	4,07	4,99	4,84		3,40	3,34	3,44		
IA25											3,54				3,15	3,32	3,47	4,14	4,11		2,92	2,93	3,03		
IA26	4,58	4,03	4,19	4,10	3,88	3,65	4,51	5,48	5,81		4,68					4,43	4,64	5,71			3,87				
IA27	4,63	4,02	4,18	4,10	3,87	3,64	4,49	5,53			4,70					4,35	4,68	5,77			3,88				
IA28							4,91	6,11	6,41		5,21					4,88	5,22	6,32	6,11		4,27		4,36		
IA29							3,70	4,52	4,69		3,91					3,73	3,90	4,96	4,76		3,29		3,30		
IA30	4,71	4,08	4,25	4,19	3,86	3,67	4,37	5,34	5,65	4,27	4,87		4,91	4,65	4,31	4,55	4,84	5,69	5,49	4,82	3,89	3,81	3,97	4,14	4,00
IA31	4,40	3,84	4,02	3,95	3,62	3,45	4,10	5,03	5,30	3,96	4,48		4,45	4,15	3,97	4,11	4,38	5,32	5,20		3,66	3,59	3,74	3,89	3,75
IA32	4,35	3,74	3,95	3,85	3,52	3,36	4,07			3,73	4,38		4,20	3,96	3,76	3,93	4,13	5,10	4,96	4,40	3,55	3,48	3,63	3,77	3,67
IA33	3,47	3,16		3,18	3,04						3,65														
IA34	3,35	3,01	3,08	3,00	3,04	2,70	3,11	3,77	3,85		3,52							4,15			2,77				
IA35	3,59	3,13	3,25	3,18	3,03	2,85	3,42	3,97			3,66							4,19			2,91				
IA36	3,34	2,97	3,04	2,98	2,82	2,67	3,16	3,81			3,44					3,05	3,15	4,00			2,77			2,98	2,78
IA37	2,91	2,58	2,71	2,68	2,56	2,40	2,80	3,43			2,93						2,86	3,40			2,46				
IA38	3,57	3,14	3,25	3,24	2,98	2,87	3,34				3,57										3,01				

Riziko	HR26	HR27	HR28	HR29	HR30	HR31	HR32	HR33	HR34	HR35	HR36	HR37	HR38	HR39	HR40	HR41	HR42	HR43	HR44	HR45	HR46	HR47	HR48	HR49
IA01	4,22	3,91	5,33	4,86	4,29	4,55	4,25	4,08	4,21	4,18	4,29	4,69	4,14	4,00	3,87	3,51	3,74	3,82	3,55	4,13	3,98	3,57	3,65	3,63
IA02	4,02				4,07		4,13	3,99	4,03		4,15	4,55	4,02	3,84	3,79	3,45	3,58	3,82	3,48	4,16	3,97	3,52	3,59	3,53
IA03	4,71		6,09	5,59	4,74	5,03	4,73	4,54	4,66	4,62	4,77	5,36	4,59	4,46	4,30	3,92	4,15	4,37	3,97	4,67	4,46	4,01	4,09	4,10
IA04	4,15				4,04		4,12	4,00	4,04		4,21	4,64	4,00	3,88	3,76	3,41	3,64	3,79	3,45	4,05	3,87	3,48	3,55	3,55
IA05	4,16				4,16		4,18	4,08	4,10		4,18	4,58	4,08	3,93	3,86	3,49	3,65	3,73	3,53	4,14	3,95	3,56	3,65	3,56
IA06	4,11				4,13		4,10	4,01	4,03		4,08	4,59	4,03	3,90	3,84	3,48	3,63	3,73	3,52	4,13	3,90	3,53	3,60	3,55
IA07	4,23				4,25		4,29	4,20	4,20		4,27	4,89	4,21	4,10	4,01	3,62	3,75	3,90	3,64	4,34	4,09	3,68	3,78	3,71
IA08	3,76				3,67	3,92	3,81	3,73	3,65	3,69	3,86	4,24	3,69	3,56	3,52	3,16	3,31	3,41	3,20	3,80	3,60	3,23	3,30	3,23
IA09	4,20		5,40		4,14		4,16	4,05	4,07		4,14	4,78	4,08	3,92	3,86	3,51	3,66	3,86	3,55	4,25	4,03	3,57	3,66	3,58
IA10	4,36		5,55	5,19	4,30		4,41	4,21	4,24		4,40	5,01	4,25	4,12	4,00	3,59	3,84	3,90	3,64	4,26	4,09	3,69	3,76	3,75
IA11	3,75				3,63		3,75	3,62	3,63		3,70	4,22	3,66	3,55	3,47	3,13	3,31	3,42	3,16	3,71	3,58	3,18	3,26	3,24
IA12	3,98		5,20	4,71	3,97		4,00	3,89	3,91		3,95	4,55	3,91	3,77	3,75	3,40	3,52	3,71	3,42	4,07	3,89	3,46	3,53	3,47
IA13	3,99				3,96		4,02	3,90	3,92	3,96	3,99	4,57					3,54	3,67	3,38		3,79	3,40	3,49	3,48
IA14	4,24				4,07		4,14	3,99	4,05	4,05	4,11	4,66					3,71	3,79	3,53		3,84	3,56	3,64	3,64
IA15	3,78				3,65		3,71	3,59	3,66	3,67	3,68	4,07					3,35	3,46	3,19		3,51	3,21	3,26	3,25
IA16	3,42				3,35		3,36	3,31	3,33	3,37	3,31	3,69					3,02	3,10	2,91		3,24	2,96	3,04	2,96
IA17	3,23				3,16		3,21	3,13	3,12	3,21	3,15	3,65					2,90	3,07	2,80		3,09	2,82	2,89	2,86
IA18	3,58	3,38			3,48		3,59	3,45	3,49	3,54	3,54	4,13					3,22	3,31	3,08		3,42	3,15	3,21	3,18
IA19	3,84	3,57			3,75		3,78	3,66	3,71	3,75	3,70	4,31					3,41	3,47	3,26		3,53	3,29	3,33	3,30
IA20	3,68	3,48			3,51		3,57	3,52	3,49	3,55	3,54	3,97					3,26	3,40	3,15	3,66	3,47	3,19	3,25	3,20
IA21	3,57	3,35	4,46		3,48		3,47	3,35	3,37	3,44	3,41	3,90					3,11	3,30	2,99	3,62	3,38	3,05	3,13	3,08
IA22	4,56	4,25	5,84	5,49	4,46	4,79	4,63	4,38	4,43	4,48	4,63	5,24					4,02	4,15	3,82	4,51	4,29	3,87	3,93	3,95
IA23	4,13	3,89	5,37		4,02		4,09	4,04	4,00	4,04	4,09	4,69					3,63	3,70	3,52		3,89	3,54	3,60	3,53
IA24	3,78	3,56	4,90		3,67		3,65	3,60	3,58	3,66	3,67	4,21					3,35	3,47	3,25		3,53	3,25	3,31	3,26
IA25	3,26	3,05	4,01		3,25	3,40	3,24	3,12	3,21	3,24	3,22	3,47					2,91	2,97	2,77		3,01	2,75	2,84	2,80
IA26	4,24		5,49	5,01	4,11		4,12	4,03	4,04	4,08	4,13	4,65					3,71	3,93	3,59		4,00	3,64	3,68	3,64
IA27	4,24		5,53	5,04	4,16		4,32	4,13	4,20	4,23	4,31	4,82					3,78	3,92	3,59		4,08	3,65	3,71	3,71
IA28	4,77	4,43	6,20	5,74	4,68		4,78	4,57	4,65	4,67	4,79	5,43					4,20	4,33	4,01		4,48	4,04	4,12	4,11
IA29	3,52	3,37	4,53	4,12	3,44		3,53	3,44	3,44	3,46	3,49	4,03					3,16	3,24	3,04		3,26	3,04	3,13	3,05
IA30	4,35	4,02	5,53	5,09	4,21		4,35	4,20	4,24	4,27	4,37	4,93	4,20	4,05	3,97	3,57	3,80	3,98	3,62	4,33	4,09	3,65	3,71	3,73
IA31	4,10	3,81	5,18	4,84	3,86	4,13	4,02	3,85	3,89	3,92	4,02	4,45	3,97	3,82	3,74	3,35	3,58	3,74	3,40	3,97	3,75	3,43	3,48	3,49
IA32	3,98	3,71	4,85	4,45	3,73	4,03	3,85	3,71	3,76	3,80	3,85	4,32	3,82	3,71	3,63	3,26	3,48	3,62	3,30	3,87	3,59	3,30	3,40	3,41
IA33								3,11	3,14		3,18	3,62					2,91	3,05						2,86
IA34							3,11	2,93	2,99		3,02	3,44					2,73	2,87	2,59		2,99	2,66	2,70	2,67
IA35							3,22	3,08	3,16		3,16	3,58					2,91	2,99	2,76	3,19	3,05	2,76	2,86	2,82
IA36	3,01	2,87					2,99	2,89	2,93	2,91	2,92	3,26					2,68	2,77	2,57	3,03	2,91	2,60	2,69	2,62
IA37	2,76	2,56					2,71	2,57	2,69	2,67	2,67	2,98					2,47	2,54	2,31	2,70	2,58	2,30	2,38	2,37
IA38							3,23	3,10	3,16		3,19	3,56					2,91	2,99	2,78	3,26	3,15	2,85	2,92	2,85

Zdroj: vlastné spracovanie