VYUŽITIE INFORMAČNO-KOMUNIKAČNÝCH TECHNOLÓGIÍ V ZDRAVOTNEJ STAROSTLIVOSTI SO ZAMERANÍM NA OBLASŤ INFORMAČNEJ BEZPEČNOSTI

ANITA ROMANOVÁ[1] – NATÁLIA ŠVEJDOVÁ[2]

Use of Information-communication Technologies in Healthcare with a Focus on Information Security

Abstract: *Information and communication technologies play an irreplaceable role in the economies of the 21st century and have also had a significant impact on the health sector. As part of the informatisation of society, e-health is not only able to achieve a significantly higher level of healthcare, but also speeds up processes and, last but not least, cuts costs that are particularly important in healthcare organizations. The aim of the paper is to use the analysis to evaluate the state and level of ICT security in Slovak hospitals as the largest providers of health care in the Slovak Republic. The article analyzes the potential and infrastructure of ICT in health conditions as well as security in this area. The second part of the paper deals with the analysis of research in the field of ICT security in Slovak hospitals and evaluates the conclusions of this questionnaire survey.*

Keywords: *informatization of health care, ehealth, ICT security, hospital, questionnaire survey*

JEL Classification: L86, D83, I19

[1] doc. Ing. Anita Romanová, PhD., University of Economics in Bratislava, Slovak Republic, e-mail: anita.romanova@euba.sk
[2] Ing. Natália Švejdová, University of Economics in Bratislava, Slovak Republic, e-mail: natalia.svejdova@euba.sk

1 Úvod

Plánovanie, implementácia a údržba informačno-komunikačných technológií (IKT) v podmienkach zdravotníctva sú veľmi náročný proces, keďže sektor poskytovania zdravotnej starostlivosti vykazuje určité špecifiká – nedostatok finančných prostriedkov, neštandardné nároky vyplývajúce najmä z legislatívy a požiadaviek poisťovní a úradov (je skoro nemožné využívať štandardné informačné systémy (IS), a preto sú vytvárané na mieru, čo sa odráža v ich finančnej náročnosti), potreba bezpečných a spoľahlivých IKT či nutnosť spracovania veľkých objemov dát, ktoré musia byť bezpečne uložené, avšak kedykoľvek prístupné pre zdravotnícky personál. IKT, ktoré sú uplatňované v zdravotníctve, majú potenciál prispieť k zvýšeniu kvality, nákladovej efektivity, časovej dostupnosti a mobility služieb v zdravotníctve. Zároveň však podporujú vznik nových foriem poskytovania zdravotnej starostlivosti, ktoré by bez využitia IKT neboli možné.

IS zdravotníckych zariadení nemožno chápať len v rovine zdravotníckej, tieto IS musia zabezpečiť aj bežnú prevádzku celej organizačnej jednotky. Z tohto dôvodu je potrebné na IS v zdravotníctve nahliadať ako na komplexné IS zabezpečujúce chod celej organizácie vrátane poskytovania zdravotnej starostlivosti pri zachovaní maximálnej úrovne bezpečnosti.

Hlavným cieľom článku je v slovenských nemocniciach vyhodnotiť súčasný stav a úroveň informačnej bezpečnosti, ako najväčších poskytovateľov zdravotnej starostlivosti na území Slovenskej republiky. V rámci výskumu boli využité všeobecné aj špecifické metódy vedeckého skúmania (matematicko-štatistické metódy, grafické metódy, dotazníkový prieskum doplnený pološtruktúrovanými rozhovormi).

2 Potenciál IKT v zdravotníctve

Uplatňovanie počítačov v službách zdravotníctva v technologicky a vedomostne vyspelých krajinách sa začalo, len čo sa tieto zariadenia objavili v dosahu medicíny. Dá sa teda hovoriť už asi o polstoročnej histórii. Obzvlášť uplynulá dekáda je veľmi významná, keďže sa zrýchlil rozvoj IKT najmä vďaka miniaturizácii počítačových technológií a dramatickému poklesu ich ceny.

Rozvoj počítačov a komunikačných technológií v 90. rokoch 20. storočia možno považovať za prelomový. V tomto období vznikli aj prostriedky, ktoré

umožnili vzájomné prepájanie počítačov (aj bezdrôtovo) do informačných sietí a taktiež nie celkom ocenený potenciál využívania internetu v zdravotníctve. Preto možno tvrdiť, že práve v tomto období vznikol veľký informačný a vedomostný potenciál – systém informačných diaľnic, ktorý tvorí nielen významný poznatkový, ale i organizačný fenomén. Rýchly rozvoj IKT zdokonalil nielen technické, ale aj programové prostriedky, čím bolo umožnené vytvoriť rozsiahle databázové IS, prístupné viacerým používateľom súčasne v reálnom čase. Využitie IKT v zdravotníctve však neostalo len pri komunikácii a archivácii záznamov. Nové technológie umožňujú pre počítače integrovať medicínske zariadenia, čím sa stávajú neoddeliteľnými pomocníkmi pri poskytovaní zdravotnej starostlivosti. Ide napríklad o sústavy počítač a EKG, EEG, EMG, sledovanie vitálnych funkcií, zariadenia na laboratórne vyšetrenia (hematológia, mikrobiológia či biochémia) alebo zobrazovacie zariadenie pripojené k počítaču, ako napr. RTG, CT, sonograf a iné.

Výskumu informačných systémov a informačných technológií využívaných v oblasti zdravotníctva sa venuje veľký okruh najmä zahraničných odborníkov. Ehrenfeld a Cannesson (2013) poukazujú na to, že použitie IKT v zdravotníctve je nevyhnutné. Pre IKT v oblasti zdravotníctva využívajú termín zdravotnícke informačné technológie (health information technology = HIT), ktoré sa používajú na zhromažďovanie, prenos, zobrazovanie alebo uchovávanie údajov pacientov v elektronickej podobe. HIT je takisto koncept, ktorý zahŕňa používanie počítačových systémov na sprístupňovanie informácií o zdravotnej starostlivosti pacientom, poskytovateľom zdravotnej starostlivosti či poisťovniam. Využívanie HIT pomáha znižovať chyby lekárov, náklady a administratívnu náročnosť, zvyšuje účinnosť a kvalitu zdravotnej starostlivosti.

Sayles (2012) uvádza, že HIT zahŕňa širokú škálu produktov, technológií a služieb, ako sú vzdialená a mobilná zdravotnícka technika, cloudové služby, zdravotnícke pomôcky, telemonitoringové nástroje, asistenčné a senzorické technológie, elektronické zdravotné záznamy (EHR) a i. Tieto technológie umožňujú používateľom zhromažďovať, uchovávať a používať zdravotnícke informácie.

Cresswell a Sheikh (2015) vo svojom výskume potvrdili, že používanie nástrojov HIT je veľmi rozšírené v zdravotníckych zariadeniach. Vzhľadom na preukázané prínosy HIT je použitie týchto technológií v súčasnosti nevyhnutné. Avšak rovnováha medzi prínosmi a rizikami využívania informačných technológií v zdravotníckych zariadeniach v nasledujúcich rokoch nie

je jasná. Z tohto dôvodu, aby sa zlepšilo plánovanie a úspešná implementácia týchto technológií, dospeli k názoru, že je potrebné používať metódy prognózovania technológií.

Výskumu zdravotníckych informačných systémov (health information system = HIS) sa venujú aj Almunawar a Anshari (2012). V ich výskume HIS: Concept and Technology, dospeli k názoru, že používanie IKT v zdravotníckych zariadeniach rástlo rovnakým tempom ako v ostatných oblastiach priemyslu či služieb. Uvádzajú, že rastie tendencia ľudí poznať a aktívne sa podieľať na prevencii a starostlivosti o svoje zdravie, pričom práve tento fakt vedie k rozvoju informačných systémov v zdravotníctve. Tento trend smeruje k väčšiemu zapojeniu pacientov do prijímania informácií, rozhodovania a zodpovednosti za vlastné zdravie práve prostredníctvom IKT. Táto vízia je dosiahnuteľná poskytovanou starostlivosťou, ktorá vychádza zo zdravotníckych telematických sietí a služieb, spájajúcich nemocnice, laboratóriá, lekárne, poskytovateľov primárnej zdravotnej starostlivosti a pacientov pomocou „virtuálneho zdravotníckeho centra“, ktoré je dostupné pomocou jedného vstupného online bodu (Almunawar a Anshari, 2012). Hansen (2012) však dospel k záveru, že najväčším problémom HIS a HIT sú výmena údajov medzi používateľmi, ako i samotné využívanie údajov zo zdravotníckych systémov na poskytovanie inteligentnej podpory rozhodovania.

Rozvoj IKT, ako i umelej inteligencie sa postupom času prejavuje aj v medicíne. V súčasnosti už existujú IT, ktoré si pamätajú a účinne uplatňujú znalosti popredných expertov. Možno ich teda nazvať inteligentnými alebo znalostnými systémami, pričom ich využitie možno nájsť v procese diagnostiky, voľby zdravotníckych postupov a v rozhodovacích procesoch. Takýmto inteligentným systémom je napr. Watson Health od spoločnosti IBM. Ide o kognitívny systém s umelou inteligenciou, ktorý slúži na diagnostiku zdravotných záznamov pacienta a navrhnutie odporúčanej liečby. Watson taktiež navrhne liečbu, ktorá by bola neefektívna, a taktiež stanoví pravdepodobnosť úspechu/neúspechu danej liečby. Po zhodnotení zdravotného stavu pacienta a návrhu postupu liečby má ošetrujúci lekár dostupné odborné články z celého sveta s cieľom odbornejšieho pohľadu na diagnostiku od IBM Watson Health. Na vývoj tohto znalostného systému vynaložila spoločnosť IBM viac ako 6 biliónov amerických dolárov.

Jedným z prvkov zdravotníckeho informačného systému je nemocničný informačný systém (NIS). Moghaddasi a kol. (2018) vo svojej štúdii uvádzajú,

že NIS je integrovaný informačný systém, ktorý nielen poskytuje informácie o pacientoch, ale podporuje i všetky nemocničné aktivity vrátane klinických, administratívnych a finančných aktivít. Okrem toho NIS tvorí dôležitú položku rozpočtu nemocnice. Obvykle 2 až 5 % nemocničného prevádzkového rozpočtu je vynaložených na informačný systém. Štúdie tiež ukazujú, že zamestnanci nemocnice trávia väčšinu času zaznamenávaním informácií, ale iba 42 % ich času sa venuje klinickým aktivitám. Na základe zahraničnej štúdie realizovanej tímom odborníkov možno za najväčší a najdôležitejší problém nemocničných informačných systémov považovať ľudský faktor. Na základe tohto výskumu vyplynulo, že NIS zlyháva z dôvodu, že zdravotnícky personál má negatívny postoj k IS a že neexistuje žiadny stimul na využívanie (efektívne) IS (Ahmadian a kol., 2017).

Rovnaký pohľad na NIS ako Moghaddasi uvádza aj Středa z Národného inštitútu zdravia: Nemocničné integrované systémy sú komplexné integrované informačné systémy, ktoré riadia prevádzku nemocnice a spravujú všetky jej aspekty, napríklad zdravotné, administratívne, finančné alebo právne. V praxi ide o nahradenie klasického papierovania počítačovým systémom, a teda zjednodušenie administratívnej práce spojenej so zdravotníckymi zariadeniami (Středa, 2018).

Na využívanie IKT v sektore zdravotníctva nemožno nahliadať len z pohľadu administratívy, je potrebné plne využiť ich potenciál. Výdobytky 21. storočia nielen skvalitnia zdravotnú starostlivosť a znížia náklady v zdravotníctve, ale zabezpečia aj efektívnejšiu liečbu či prevenciu, a tým skvalitnia a predĺžia život ľudí. Faktom však ostáva, že kognitívne systémy, ktoré vo veľkej miere pomáhajú lekárom pri diagnostike a liečbe pacientov (ako napr. spomenutý Watson Health) sú finančne náročné a len máloktoré zdravotnícke zariadenia (či už na Slovensku, ale i v zahraničí) si môžu takýto systém dovoliť obstarať.

Využitie a prínosy IKT v zdravotníctve sú určité nespochybniteľné. Domáci, ale i zahraniční autori vymedzujú pozitíva využitia prostriedkov IKT v medicíne, netreba však zabúdať ani na riziká, ktoré sú s nimi spojené. V sektore zdravotníctva sú spracúvané citlivé osobné údaje, o ktoré sa treba starať z hľadiska nielen ich nadobudnutia, ale najmä uchovávania. Oblasť IKT je neustále sa meniacou oblasťou, a preto je veľmi dôležité, aby si poskytovatelia zdravotnej starostlivosti veľmi dobre naplánovali obstaranie, implementáciu a údržbu týchto zariadení. Keďže oblasť IKT je veľmi dynamická ─ to, čo je dnes inovatívne, je už „zajtra“ zastarané ─ preto vynaloženie financií do

týchto moderných prostriedkov musí byť čo najefektívnejšie a najúčinnejšie (keďže IKT sa môžu podieľať na rozpočte poskytovateľov zdravotnej starostlivosti až 5 %, čím sa stávajú veľmi významnou a nákladnou položkou celého rozpočtu). Kým v minulosti bol problémom zlyhania moderných technológií výpadok hardvéru alebo softvéru, v súčasnosti možno za najväčšiu hrozbu pre NIS považovať ľudský faktor. Neochota učiť sa, využívať IKT, chybné zápisy do IS znižujú prínosy celého IS pre zdravotnícke zariadenia. Z tohto dôvodu je potrebné nielen zamerať sa na implementáciu nových informačných riešení, ale zabezpečiť i školenia pracovníkov zdravotníckych zariadení. Využívanie IKT v zdravotníctve by malo priniesť najmä zlepšenie zdravotnej starostlivosti pre pacientov. V dnešnej – informačnej – dobe, keď chcú byť ľudia informovaní o všetkom a kdekoľvek na svete, vyvstáva nová možnosť zapojenia pacienta do elektronického zdravotníctva. Zlepší sa tým informovanosť pacientov nielen o ich zdravotnom stave, ale i o stave ich príbuzných, o užívaných liekoch a predpísaných pomôckach, o preventívnych prehliadkach a pod. Zapojením pacienta do systému informatizácie zdravotníctva sa predpokladá zlepšenie zdravia občanov, ako i zníženie nákladov na zdravotnú starostlivosť.

3 Infraštruktúra IKT v zdravotníctve

Pod IKT infraštruktúrou v zdravotníctve možno rozumieť počítače jednotlivých odborníkov, ktoré sú vybavené vhodným a potrebným softvérom, vzájomné prepojenie týchto pracovných staníc, ktoré umožňuje komunikáciu medzi sebou, ale i s okolím, zabezpečenie prístupu do databáz, zdrojov poznatkov a informácií, prístup do jednotlivých informačných systémov na základe stupňa oprávnenia. Používanie prostriedkov IKT v dennej praxi pracovníkov rezortu zdravotníctva sa neustále zlepšuje, preto je možné tvrdiť, že Slovensko sa pomaly, ale isto približuje ostatným krajinám EÚ v informatizácii zdravotníctva. Aj prístup zdravotných poisťovní prispel k tomu, že poskytovatelia zdravotnej starostlivosti sú nútení využívať pri svojej práci IKT. Vykazované dávky na vyúčtovanie sú v súčasnosti akceptované už len v elektronickej podobe, čím sa významne prispelo k zvýšeniu používania počítačov v sfére poskytovania zdravotnej starostlivosti.

Menej uspokojivá je však oblasť vzájomného prepojenia organizácií a pracovísk poskytujúcich zdravotnú starostlivosť. Práve eHealth (na území Slovenskej republike ezdravie) má tento problém odstrániť. Realizácia tohto

projektu si vyžaduje, aby v zdravotníckych zariadeniach boli nainštalované IKT vo vhodných štruktúrovaných sieťových prepojeniach.

Problematikou IKT infraštruktúry sa treba zaoberať nielen vo fázach plánovania a implementácie, ale aj vo fázach prevádzky a údržby. Jedným z najdôležitejších špecifík je nutnosť urgentného riešenia IT problémov. Ako majú nemocnice urgentný príjem pre akútne prípady, rovnako majú aj IT tímy v nemocniciach urgentné situácie, ktoré treba bezodkladne riešiť, aby nebol ohrozený život pacienta a bol zaistený plynulý chod nemocnice. Nemocnice sú nepretržitou prevádzkou, a preto je na IT kladený dôraz, aby boli vždy k dispozícii (Fiala a Studený, 2016).

Špecifikom poskytovateľov zdravotníckych zariadení je aj ich práca s veľmi citlivými informáciami. Podľa IT odborníka na bezpečnosť v dôsledku digitálnej transformácie prechádza zdravotníctvo drastickými zmenami, pokiaľ ide o operácie a komunikáciu s pacientmi. Poskytovatelia zdravotnej starostlivosti zavádzajú nové technológie na jej zlepšenie. Takáto inovácia zjednodušila komunikáciu medzi lekármi a pacientmi prostredníctvom aplikácií a nositeľných pomôcok, ako aj spoluprácu lekárov prostredníctvom elektronických zdravotných záznamov a rôznych cloudových služieb. Tento pokrok otvoril obrovské príležitosti pre zdravotníkov, ale tiež pre počítačových kriminálnikov. Väčšie používanie technológií totiž prináša aj zvýšené riziko kybernetických útokov, ktoré cielia na krádež dôverných údajov (Hunková, 2018). Z tohto dôvodu je nutné, aby poskytovatelia zdravotnej starostlivosti pracovali s bezpečnými IKT a zabezpečili im náležitú ochranu. Pod bezpečnosťou IKT môžeme rozumieť vlastnosť znamenajúcu odolnosť systému proti stratám, poškodeniu alebo nežiaducim zmenám informácií.

4 Bezpečnosť IKT

Zabezpečenie IKT sa stáva čím ďalej tým dôležitejším, keďže sa stupňuje počet útokov na získanie osobných údajov či tajných informácií, ktoré sú súčasťou IS a majú byť utajené, resp. dostupné iba oprávneným osobám.

Jedným z najvýznamnejších dôvodov informatizácie verejnej správy je znižovanie výdavkov na jej prevádzku. Na druhej strane nové informačné systémy alebo prepojenie s existujúci systémami prinášajú nové riziká a bezpečnostné hrozby. Rovnako prevádzka existujúcich systémov vyžaduje neustále riadenie bezpečnostných rizík (ITAPA, 2011).

Bezpečnosť IKT teda predstavuje IS, v ktorom sú zaistené:

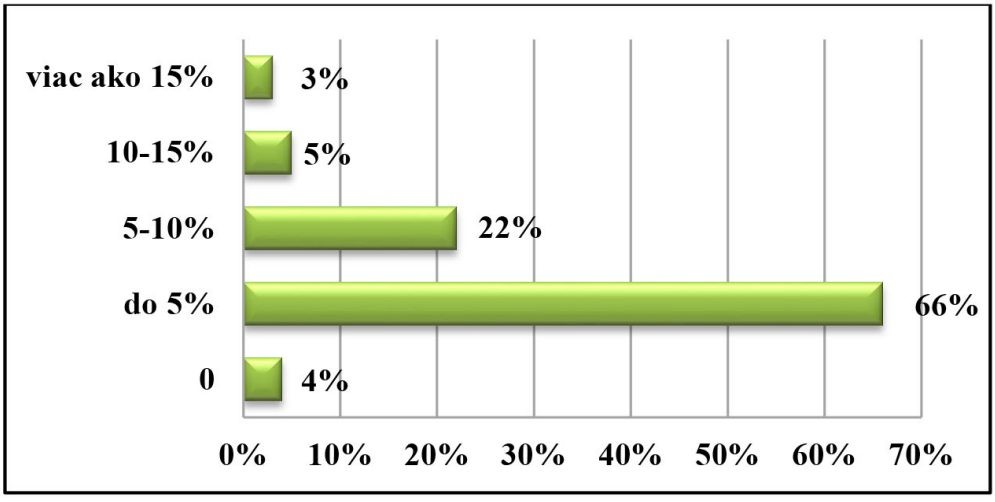
- spoľahlivosť prevádzky IS ako celku,
- ochrana údajov, ktoré IS spracováva a uchováva tak, aby nedošlo k úniku informácií neoprávneným osobám,
- zabezpečenie ochrany osôb využívajúcich IS.

Úrad podpredsedu vlády SR pre investície a informatizáciu (2019) definuje informačnú bezpečnosť ako:

- ideálny stav systému, organizácie, keď IKT fungujú bez narušenia a sú zaručené dôvernosť, integrita, autentickosť a dostupnosť údajov, resp. služieb,
- činnosť zameraná na dosiahnutie a udržanie požadovaného stavu IKT,
- multidisciplinárny odbor zaoberajúci sa skúmaním hrozieb pre údaje a systémy a hľadaním opatrení na elimináciu rizík, ktoré z nich vyplývajú.

V súčasnosti sa bezpečnosti IKT nevenuje až taká pozornosť, aká by mala byť, a preto výdavky do tejto oblasti nie sú priveľké. Túto skutočnosť zobrazuje štatistika, ktorú spracovalo Ministerstvo financií SR v prieskume stavu informačnej bezpečnosti, ktorej sa zúčastnilo 153 respondentov.

Graf č. 1: Podiel informačnej bezpečnosti na rozpočte IT (SR, 2013) (Ministerstvo financií SR, 2013)



Z grafu vyplýva, že najviac respondentov z oblasti verejnej správy SR vynakladá do informačnej bezpečnosti nie viac ako 5 % zo svojho rozpočtu smerujúceho do oblasti IT. Tento fakt nie je prekvapujúci, keďže organizácie sú primárne nútené vynakladať finančné prostriedky na zabezpečenie požadovanej funkčnosti a prevádzkyschopnosti IS a na prispôsobovanie IS zmenám. V súčasných finančných podmienkach verejnej správy nemožno však ani predpokladať, že by sa v blízkej budúcnosti pravdepodobne podiel výdavkov na informačnú bezpečnosť zvyšoval.

Finančná náročnosť nie je jedinou prekážkou, prečo organizácie nevenujú dostatočnú pozornosť bezpečnosti IKT. Medzi ďalšie prekážky presadzovania bezpečnosti IKT v Slovenskej republike možno zaradiť všeobecne nízke bezpečnostné povedomie o IT bezpečnosti, nedostatočnú legislatívu v tejto oblasti, nedostatočnú podporu zo strany vedenia organizácie či technologickú náročnosť na zaistenie bezpečnosti IKT.

Najslabšími článkami v organizáciách sú koncové zariadenia – počítače, notebooky či mobilné telefóny. Cieľom útočníkov je získať prostredníctvom týchto zariadení citlivé dáta, ako napr. mená, heslá, čísla platobných kariet a pod.

Je dôležité, aby bezpečnostné nástroje používané vo firme boli komplexné. Mali by zahŕňať penetračné testovanie, bezpečnosť internetu, zabezpečenú sieť či správu prístupov. Kybernetickí útočníci využijú každú slabú stránku v IT bezpečnosti (Touchit, 2020).

Podnikatelia i manažéri si postupne začínajú uvedomovať dôležitosť spoľahlivého IS a jeho prínosov pri riadení organizácie. IS a IT sa stali neoddeliteľnou súčasťou efektívneho manažmentu a je len na manažéroch a samotných zamestnancoch, do akej miery ich využijú pri vykonávaní ich každodennej práce. V oblasti bezpečnosti IT môžeme stále sledovať pretrvávajúci trend – podceňovanie možného útoku na IS a zneužitie získaných údajov. Z tohto dôvodu by mali organizácie prehodnotiť svoj prístup k bezpečnosti a vyčleniť viac finančných prostriedkov na ochranu IS a IT.

5 Cieľ, metodika výskumu a metódy skúmania

Hlavným cieľom článku je vyhodnotiť v slovenských nemocniciach súčasný stav a úroveň informačnej bezpečnosti, najväčších poskytovateľov zdravotnej starostlivosti na území Slovenskej republiky.

Metodika výskumu pozostáva z krokov, ktoré na seba navzájom nadväzujú, pričom výsledkom je získanie požadovaných výstupov a zistení. Metodiku môžeme zhrnúť do nasledovných krokov:

1. identifikácia problému – vymedzenie oblasti ako základu pre uskutočnenie výskumu,

2. štúdium domácej i zahraničnej literatúry, štúdií – zber informácií a poznatkov z relevantných zdrojov,

3. zhodnotenie súčasného stavu riešenej problematiky – využitie všeobecných vedeckých metód na zhodnotenie súčasného stavu danej oblasti výskumu,

4. definovanie cieľa výskumu – vymedzenie hlavného cieľa výskumu,

5. výber metód skúmania – výber vhodných metód (všeobecných i špecifických) z dôvodu dosiahnutia cieľa výskumu,

6. dotazníkový prieskum, pološtruktúrované rozhovory – realizácia výskumu v slovenských nemocniciach,

7. spracovanie a analýza získaných údajov – triedenie, analýza a vyhodnotenie získaných dát,

8. interpretácia výsledkov – interpretácia výsledkov a vyvodenie záverov.

Vo výskume boli využité najmä všeobecné metódy, ktoré zahŕňajú množinu metód využívajúcich princípy logiky a logického myslenia. Do tejto skupiny patrí tzv. trojica párových metód:

- analýza – syntéza,
- indukcia – dedukcia,
- abstrakcia – konkretizácia.

Medzi všeobecné metódy vedeckého skúmania môžeme zaradiť aj komparáciu, generalizáciu a analógiu. V praxi sa všetky tieto vedecké metódy vzájomne dopĺňajú, kombinujú a, samozrejme, vo svojom účinku prekrývajú, a tým vytvárajú aj určitú synergiu.

Metóda analýzy bola využitá pri skúmaní aktuálneho stavu poznania v predmetnej oblasti a tiež pri vyhodnocovaní čiastkových zistení z realizova-

ného prieskumu a pološtruktúrovaných rozhovorov. Pomocou párovej metódy pre analýzu sme využitím syntézy spracovali jednotlivé čiastkové výsledky do komplexného systému v zmysle uceleného pohľadu na analyzovanú skutočnosť. Využitím metódy komparácie sme porovnali bezpečnostné incidenty najčastejšie sa vyskytujúce v slovenských nemocniciach s výsledkami výskumu realizovaného na území Slovenskej a Českej republiky od spoločnosti Data Security Management s cieľom zistenia podobnosti, resp. rozdielnosti dosiahnutých výsledkov. Metóda konkretizácie nám bola nápomocná pri vymenovávaní príkladov s cieľom lepšieho porozumenia danej problematiky.

Pri spracovaní výsledkov prieskumu z prostredia slovenských nemocníc sme využili i špecifické metódy vedeckého skúmania, a to:

- matematicko-štatistické metódy (deskriptívna štatistika, korelačná analýza),
- grafické metódy.

Zber dát v rámci nášho výskumu bol realizovaný dotazníkovým prieskumom doplneným o pološtruktúrované rozhovory. Dotazníky boli distribuované 40 respondentom (38 štátnych nemocníc a dvaja súkromní poskytovatelia zdravotnej starostlivosti).

Pri zostavovaní dotazníka sme vychádzali z teoretických poznatkov, ktoré sme získali pri štúdiu tejto vybranej problematiky, pričom veľmi nápomocným nám boli aj odborníci z oblasti nemocničných informačných systémov, elektronizácie zdravotníctva, správy sietí a ochrany osobných údajov.

Návratnosť dotazníka bola na úrovni 75 %, čo predstavovalo 30 respondentov. Údaje od súkromných poskytovateľov zdravotnej starostlivosti sa nám nepodarilo získať, s odôvodnením, že otázky v dotazníku sú veľmi citlivé z pohľadu ochrany obchodného tajomstva, IT bezpečnosti alebo tiež firemnej reputácie. Zo skupiny štátnych nemocníc sa nám nepodarilo informácie získať od 5 poskytovateľov zdravotnej starostlivosti z dôvodu zachovania informačnej bezpečnosti organizácie či s odvolaním sa na nepovinnosť poskytovať komplexné informácie vo forme dotazníka. Tri nemocnice boli zo štatistického súboru nakoniec vylúčené, keďže v súčasnosti už pôsobia len ako domov sociálnych služieb či diagnostické centrum.

Štruktúra analyzovanej vzorky 30 respondentov je uvedená v nasledujúcej tabuľke.

Tab. č. 1: Štruktúra respondentov v závislosti od zriaďovateľa a územnej pôsobnosti

Zriaďovateľ	Oblasť Slovenskej republiky			Celkový súčet
	Západoslovenská	Stredoslovenská	Východoslovenská	
MZ SR	33,34 %	20,00 %	10,00 %	63,34 %
VÚC	10,00 %	10,00 %	0,00 %	20,00 %
Iný orgán	3,33 %	3,33 %	10,00 %	16,66 %
Celkový súčet	**46,67 %**	**33,33 %**	**20,00%**	**100,00 %**

Prameň: vlastné spracovanie.

Pri analýze bezpečnosti IKT v slovenských nemocniciach bolo potrebné diferencovať nemocničné subjekty do veľkostných kategórií. Keďže odporúčanie Európskej komisie č. 2003/361/EC by v našom prípade ohodnotilo 26 subjektov ako veľké podniky a len 4 subjekty ako stredné podniky, rozhodli sme sa na základe základných charakteristík o jednotlivých objektoch zostaviť vlastnú kategorizáciu nemocníc na území Slovenskej republiky.

Prvotným kritériom na zatriedenie subjektu je počet zamestnancov, pričom na základe našej analýzy sa tomuto členeniu najviac približuje rozdelenie na základe počtu vyšetrení ambulantných pacientov ($r = 0,7562$; $r2 = 57,18$ %; $p < 0,001$), potom na základe počtu hospitalizácií ($r = 0,8031$; $r2 = 64,50$ %; $p < 0,001$). Vychádzajúc z týchto vzťahov a analýzy dát pomocou štatistických ukazovateľov priemer a smerodajná odchýlka možno slovenské nemocnice kategorizovať na základe ukazovateľov uvedených v tabuľke č. 2.

Tab. č. 2: Navrhnuté kritériá kategorizácie slovenských nemocníc

Ukazovateľ	Kategória organizácie		
	Malá	Stredná	Veľká
1. Počet zamestnancov	$X \leq 178$	$178 < X \leq 1\,446$	$1\,446 < X$
2. Počet vyšetrení ambulantných pacientov	$X \leq 15\,355$	$15\,355 < X \leq 395\,196$	$395\,196 < X$
3. Počet hospitalizácií	$X \leq 2\,095$	$2\,095 < X \leq 27\,797$	$27\,797 < X$

Prameň: vlastné spracovanie.

Do jednej z uvedených kategórií spadá nemocničný subjekt vtedy, ak má príslušný počet zamestnancov (hlavné kritérium) a spĺňa aspoň jedno vedľajšie kritérium (počet vyšetrení ambulantných pacientov alebo počet hospitalizácií). Na základe nami navrhnutej kategorizácie možno respondentov výskumnej vzorky zaradiť nasledovne:

Tab. č. 3: Kategorizácia respondentov výskumnej vzorky

Zriaďovateľ	Kategória organizácie		
	Malá	Stredná	Veľká
MZ SR	13,33 %	36,68 %	13,33 %
VÚC	0,00 %	20,00 %	0,00 %
Iný orgán	3,33 %	13,33 %	0,00 %
Celkový súčet	**16,66 %**	**70,01 %**	**13,33 %**

Prameň: vlastné spracovanie.

V ďalších častiach tohto príspevku budeme vychádzať z tejto kategorizácie nemocníc na malé, stredné a veľké organizácie.

6 Výsledky a diskusia

Prvá časť výskumu sa zaoberala identifikáciou subjektu s cieľom jeho ďalšej kategorizácie. Nasledovala časť, ktorá sa zaoberala finančnými výdavkami do oblasti IKT. Skúmali sme, koľko percent z prevádzkového rozpočtu nemocnice smeruje do oblasti IKT.

Tab. č. 4: Percento z prevádzkového rozpočtu nemocníc vynaložené do oblasti IKT (r. 2018)

Organizácia	M	SD	Me	Mo	Min	Max
Malá	0, 81 %	0, 31 %	0, 79 %	–	0, 41 %	1, 37 %
Stredná	0, 82 %	0, 50 %	0, 65 %	–	0, 19 %	2, 15 %
Veľká	0, 66 %	0, 19 %	0, 74 %	–	0, 33 %	0, 81 %

Prameň: vlastné spracovanie.

Z vykonanej analýzy možno vidieť, že slovenské nemocnice dávajú priemerne od 0,66 % do 0,82 % z prevádzkového rozpočtu organizácie do oblasti IKT. V prvej časti nášho príspevku sme uviedli tvrdenie autora Moghaddasiho a kol. (2018), ktorý vo svojej štúdii tvrdí, že 2 až 5% nemocničného prevádzko-

vé rozpočtu je venovaných na informačný systém. Na základe nášho výskumu však toto tvrdenie v prostredí Slovenskej republiky nemôžeme potvrdiť, keďže sme zistili, že slovenské nemocnice vynakladajú v priemere 0,80 % (SD = 0,004) zo svojho prevádzkového rozpočtu do oblasti IKT. Len jeden respondent z našej výskumnej vzorky vynaložil viac ako 2 % zo svojho prevádzkového rozpočtu do tejto oblasti. Pri analýze, koľko percent z rozpočtu smerujúceho do oblasti IKT je vynaložených na bezpečnosť informačných technológií, môžeme potvrdiť štatistiku Ministerstva financií SR, ktorú sme uviedli v časti „Bezpečnosť IKT". Všetci naši respondenti – slovenské nemocnice, vynakladajú menej ako 5 % z rozpočtu smerujúceho do oblasti IKT na zabezpečenie ochrany svojich informačných technológií.

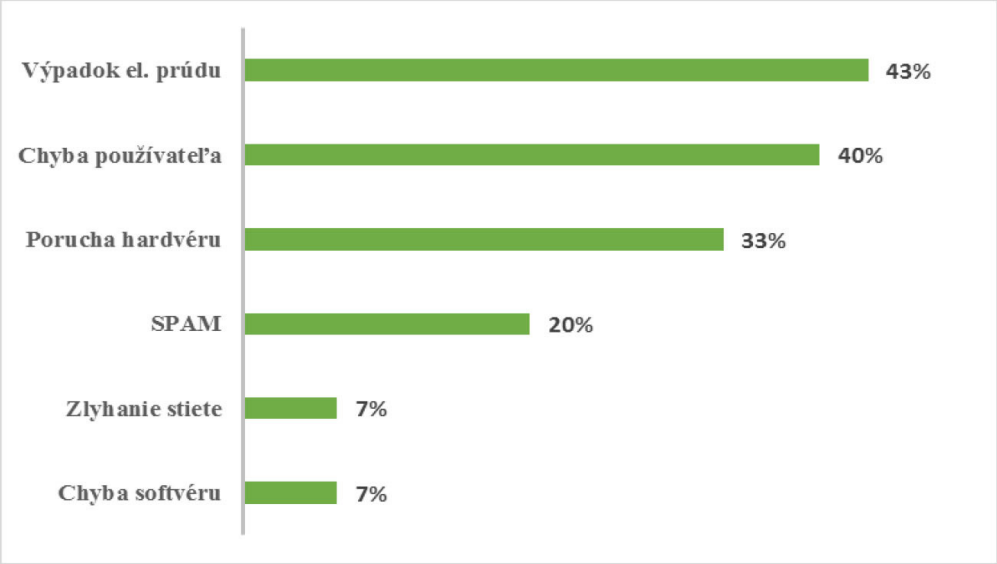
Ďalšou sledovanou oblasťou bola práve bezpečnosť IKT, ktorej sa vo veľkej miere venujú nielen odborníci, ale i verejnosť, z dôvodu citlivosti spracúvaných osobných údajov. 23,33 % našich respondentov vo svojich odpovediach uviedlo, že zaznamenali kybernetický útok v ich organizácii. Zvyšných 76,67 % organizácií sa zatiaľ s kybernetickým útokom nestretlo.

V rámci bezpečnosti sme ďalej analyzovali, s akými bezpečnostnými incidentmi sa poskytovatelia zdravotnej starostlivosti najčastejšie stretávajú a akými prostriedkami je zaistená bezpečnosť IKT v organizácii. Na škále 1 až 6 mali ohodnotiť, s ktorým bezpečnostným incidentom sa stretávajú najčastejšie (hodnota 1) a, naopak, hodnota 6 znamenala, že daný bezpečnostný incident sa doposiaľ nevyskytol a nepovažujú ho tak za riziko pre organizáciu. Výsledky analýzy tejto oblasti sú nasledovné:

Z nášho výskumu vyplynulo, že najčastejšie sa vyskytujúcimi bezpečnostnými incidentmi sú výpadok elektrického prúdu, chyba spôsobená na strane používateľa IKT a porucha hardvéru. Naopak, medzi incidenty, ktoré sa doposiaľ nevyskytli, a preto ich organizácie nepovažujú za hrozby, patria falšovanie dokumentov, nepovolený prístup zvonka/zvnútra či krádež zariadenia. Na komparáciu našich zistení použijeme výsledky prieskumu stavu informačnej bezpečnosti, ktorý sa uskutočnil na území nielen Slovenskej, ale i Českej republiky.

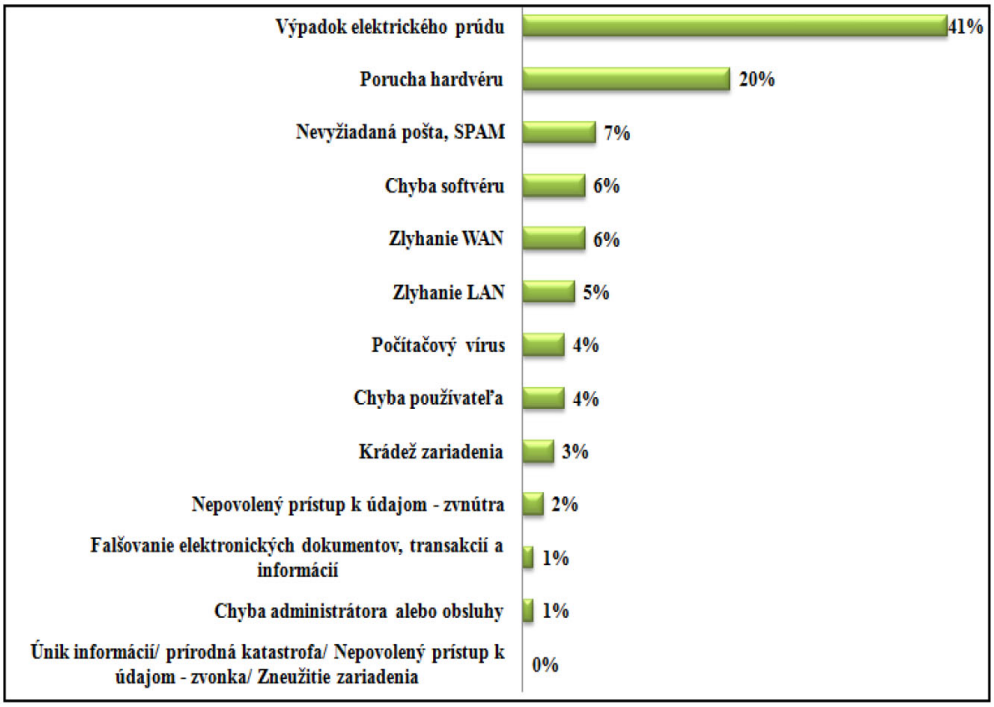
Porovnaním výsledkov týchto prieskumov so závermi nášho skúmania vidíme, že v našom výskume sme dosiahli veľmi obdobné výsledky, a preto možno tvrdiť, že medzi najčastejšie sa vyskytujúce bezpečnostné incidenty v súčasnosti patria výpadok elektrického prúdu a porucha hardvéru.

Graf č. 2: Bezpečnostné incidenty IKT v slovenských nemocniciach



Prameň: vlastné spracovanie.

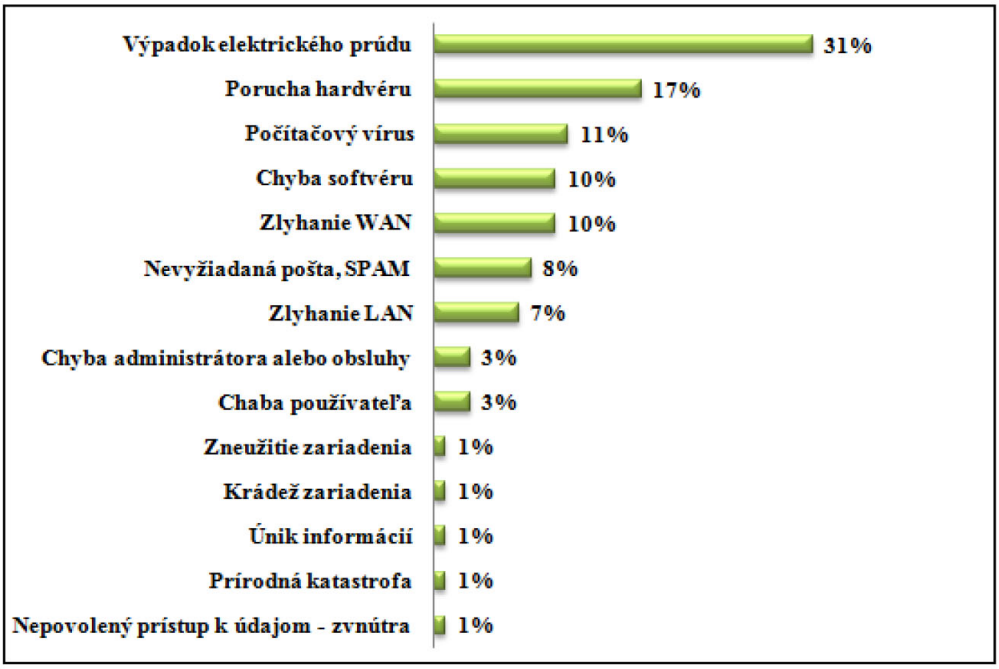
Graf č. 3: Bezpečnostné incidenty v slovenských podnikoch v roku 2008



Prameň: Data Security Management (2008)

Po zistení, ktoré bezpečnostné incidenty sú považované za najčastejšie sa vyskytujúce, sme skúmali, akými prostriedkami chránia organizácie svoje IKT.

Graf č. 4: Bezpečnostné incidenty v českých podnikoch v roku 2009

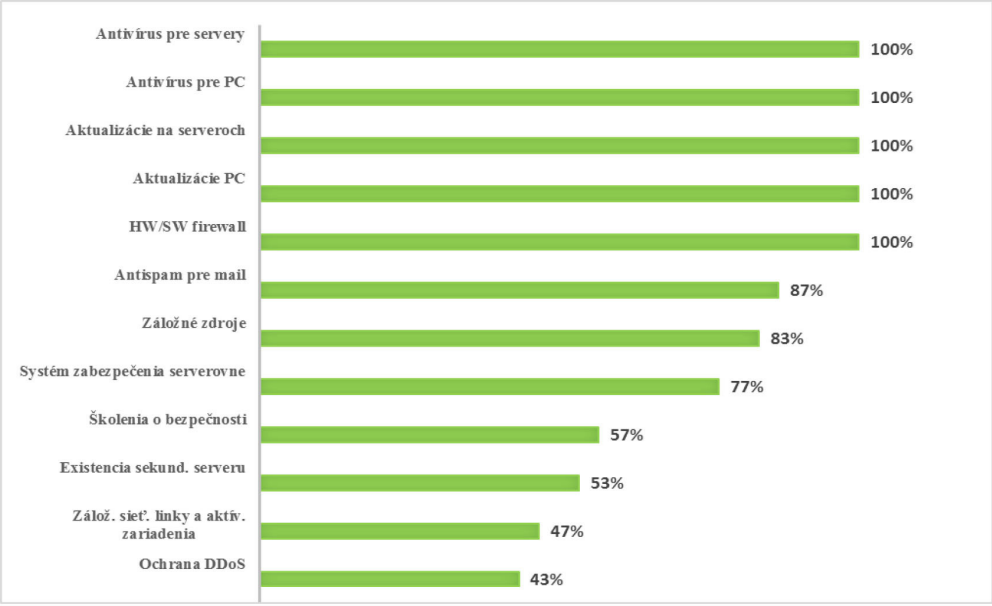


Prameň: Data Security Management (2009)

Z grafickej analýzy dát vyplýva, že slovenské nemocnice využívajú široké spektrum spôsobov, ako zabezpečiť bezpečnosť nielen IKT, ale i informácií, ktoré sa pomocou nich spracúvajú a uchovávajú. Viac ako polovica respondentov (57 %) uskutočňuje vo svojich organizáciách pravidelné školenia o bezpečnosti, čo považujeme za veľmi dôležité. Najmenej využívanými spôsobmi ochrany IKT sú existencia záložných sieťových liniek a aktívnych zariadení v prípade výpadku siete LAN a ochrana DDoS (ochrana proti nefunkčnosti akejkoľvek služby založenej na IP protokole). Testovaniu odolnosti informačného systému proti vonkajším útokom sa venuje len tretina respondentov.

V ďalšej časti výskumu o bezpečnosti IKT v slovenských nemocniciach sme analyzovali, aké sú najväčšie prekážky presadzovania a zvyšovania IKT bezpečnosti v organizácii. Respondenti mali pomocou hodnôt 1 až 6 usporiadať jednotlivé prekážky, pričom najväčšej prekážke mala byť priradená hodnota 1. Výsledky tejto analýzy sú uvedené v tabuľke.

Graf č. 5: Spôsob ochrany IKT v slovenských nemocniciach



Prameň: vlastné spracovanie.

Tab. č. 5: Najväčšie prekážky presadzovania IKT bezpečnosti v slovenských nemocniciach

Malé organizácie	Stredné organizácie	Veľké organizácie
1. Finančná náročnosť	1. Finančná náročnosť	1. Finančná náročnosť
2. Nízke bezpečnostné povedomie v organizácii	2. Technologická náročnosť	2. Nedostatočná podpora zo strany vedenia organizácie
3. Technologická náročnosť	3. Nízke bezpečnostné povedomie v organizácii	3. Technologická náročnosť
4. Nedostatočná podpora zo strany vedenia organizácie	4. Nedostatočná podpora zo strany vedenia organizácie	4. Nízke bezpečnostné povedomie v organizácii
5. Nedostatok informácií o IKT bezpečnosti	5. Nedostatok informácií o IKT bezpečnosti	5. Nedostatok informácií o IKT bezpečnosti

6. Nedostatočná legislatíva SR v oblasti bezpečnosti IKT	6. Nedostatočná legislatíva SR v oblasti bezpečnosti IKT	6. Nedostatočná legislatíva SR v oblasti bezpečnosti IKT

Prameň: vlastné spracovanie.

Z analýzy výsledkov je zrejmé, že za najväčší problém presadzovania IKT bezpečnosti považujú respondenti finančnú náročnosť. Je všeobecne známe, že slovenské nemocnice majú nedostatočné finančné zdroje, na úhradu miezd nielen svojim pracovníkom, ale najmä svojim dodávateľom. Z tohto dôvodu je pre ne nereálne, aby investovali do zvýšenia úrovne bezpečnosti IKT. Za najmenšie prekážky sú považované nedostatok informácií o IKT bezpečnosti a legislatíva SR, ktorá sa zaoberá touto problematikou. Pozitívne však hodnotíme fakt, že v malých a stredných organizáciách nie je prekážkou presadzovania IKT bezpečnosti podpora zo strany vedenia, a teda že si topmanažment organizácií uvedomuje dôležitosť zaistenia bezpečnosti svojich IKT.

V poslednej časti nášho výskumu sme sa zamerali na to, aké plány a zámery v oblasti IKT majú organizácie do budúcnosti. Na výber mali z 12 oblastí, pričom si mali zvoliť 5 oblastí a určiť ich prioritu (hodnota 1 znamenala najvyššiu prioritu). Analýzou získaných dát sme identifikovali týchto 5 najdôležitejších oblastí, v ktorých sa chcú slovenské nemocnice do budúcnosti polepšiť:

1. posilnenie IT infraštruktúry (sietí),
2. zvýšenie úrovne bezpečnosti IKT,
3. zvýšenie výkonu/ rýchlosti IS,
4. modernizácia serverov,
5. modernizácia hardvéru.

Zo záverov realizovaného výskumu vyplynulo, že bezpečnosti IKT sa organizácie chcú venovať (nie je im táto oblasť ľahostajná). Veľmi dobre si uvedomujú dôležitosť zabezpečenia IKT s ohľadom na charakter spracúvaných a uchovávaných údajov. Problémom však naďalej ostáva nedostatok finančných prostriedkov, ktoré by do tejto oblasti mohli byť investované.

7 Záver

Zdravie je jedným z najdôležitejších predpokladov kvality života a jednou z najvyšších hodnôt pre občana. Z tohto dôvodu si vyžaduje zvýšenú pozornosť tak zo strany jednotlivca, ako aj zo strany celej spoločnosti. Zameranie rezortu zdravotníctva sa presúva od liečenia pacienta na komplexnú starostlivosť o zdravie občana a manažment všetkých determinantov zdravia, nielen zdravotnej starostlivosti (Hrašková, 2014). Slovenská republika, ako člen Európskej únie, sa zaviazala implementovať elektronické zdravotníctvo na svojom území a zabezpečiť tak kvalitnú a efektívnu zdravotnú starostlivosť nielen pre svojich občanov, ale i občanov celej EÚ.

Informatizáciu v oblasti zdravotníctva preto možno považovať za jeden z kľúčových nástrojov efektívneho zdravotníctva. Elektronická výmena dát môže ušetriť množstvo financií, taktiež zvýšiť efektívnosť, kvalitu a dostupnosť zdravotnej starostlivosti. Finančná úspora, ktorá by mohla byť dosiahnutá efektívnou elektronizáciou zdravotníctva, by mohla byť využitá na lepšie mzdové ohodnotenie lekárov, resp. udržanie alebo prilákanie zdravotných odborníkov.

Domáca aj zahraničná odborná verejnosť a politici si začínajú uvedomovať, aký veľký prínos pre krajinu a najmä rezort zdravotníctva prinášajú IKT. Aby však plnili svoju funkciu, teda poskytovali správne informácie v správnom čase, je nevyhnutné, aby poskytovatelia zdravotnej starostlivosti disponovali vhodným a bezpečným hardvérovým aj softvérovým vybavením. Realizáciou nášho výskumu sme zistili, že najväčším problémom slovenských nemocníc je nedostatok finančných zdrojov, a preto len v priemere 0,80 % z prevádzkového rozpočtu nemocníc smeruje do oblasti IKT (v zahraničí je 2 – 5 %). Nedostatok finančných zdrojov sa prejavuje aj v rámci bezpečnosti IKT, keďže len tretina respondentov nášho dotazníkového výskumu vykonáva testovanie odolnosti IS.

Limitom realizovaného výskumu bola pomerne malá výskumná vzorka, čo bolo zapríčinené špecificky stanovenými kritériami na to, ktorí poskytovatelia zdravotnej starostlivosti boli do prieskumu zaradení. Objektom nášho výskumu boli nemocnice na území Slovenskej republiky, pričom ich počet je v súčasnosti na úrovni 68. Počet respondentov, ktorí boli do nášho výskumu oslovení, bol na úrovni 40, a to z dôvodu, že celkovo 30 nemocníc je v zriaďo-

vateľskej pôsobnosti dvoch súkromných poskytovateľov zdravotnej starostlivosti a aj oblasť IKT je riadená centrálne pre všetky subjekty.

Naším zámerom bolo získať dáta ako zo štátnych, tak aj zo súkromných nemocníc. Návratnosť dotazníka bola na úrovni 75 %. Údaje sa nám nepodarilo získať od súkromných poskytovateľov zdravotnej starostlivosti, ako aj z 5 nemocníc zo skupiny štátnych nemocníc. 3 nemocnice boli zo štatistického súboru nakoniec vylúčené, keďže v súčasnosti už pôsobia len ako domov sociálnych služieb či diagnostické centrum. Dôsledkom týchto skutočností sa počet našich respondentov zúžil, len na vzorku pozostávajúcu zo štátnych nemocníc.

Ďalším limitom výskumu je fakt, že respondenti (najčastejšie vedúci oddelení IT) mohli vedome alebo nevedome prikrášľovať svoje odpovede, príp. mohli mať nekritický pohľad na oblasť informačnej bezpečnosti v danom nemocničnom subjekte.

Pozitívne však musíme hodnotiť fakt, že manažment nemocníc, ako i samotní zamestnanci oddelení informačných technológií sa snažia v rámci svojich finančných možností zaistiť čo najvyššiu mieru bezpečnosti nielen svojich IKT, ale i spracúvaných informácií. Z tohto dôvodu je nevyhnutné neustále venovať dostatočnú pozornosť nielen implementácii IKT do zdravotníckej praxe, ale aj bezpečnosti IKT, aby bolo možné využiť celý potenciál týchto technológií v prospech pacientov.

LITERATÚRA

[1] AHMADIAN, L. – DOROSTI, N. – KHAJOUEI, R. – GOHARI, S.H. 2017. *Challenges of using Hospital Information Systems by nurses: comparing academic and non-academic hospitals. Electronic Physician,* 2017, 9(6), 4625 ─ 4630.

[2] ALMUNAWAR, M. – ANSHARI, M. 2012. *Health Information Systems (HIS): Concept and Technology.* [online]. Brunei: Universiti Brunei Darussalam, 2012. [cit. 03. 02. 2020]. Dostupné na: https://www.researchgate.net/publication/221710863_ Health_Information_ Systems_HIS_Concept_and_Technology

[3] CRESSWELL, K. – SHEIKH, A. 2015. Health Information Technology in Hospitals: Current Issues and Future Trends. *Future Healthcare Journal.* 2015, 2(1), 50 – 56..

[4] DATA SECURITY MANAGEMENT. 2008. *Prieskum stavu informačnej bezpečnosti v SR 2008.* [online]. Praha: Data Security Management, 2008. [cit. 05. 02. 2020] Dostupné na: http://www.tate.cz/cz/psib-sr-2008/

[5] DATA SECURITY MANAGEMENT. 2009. *Průzkum stavu informační bezpečnosti v ČR 2009.* [online]. Praha: Data Security Management, 2009. [cit. 05. 02. 2020] Dostupné na: http://www.tate.cz/cz/psib-cr-2009

[6] EHRENFELD, J. – CANNESSON, M. 2013. *Monitoring Technologies in Acute Care Environments: A Comprehensive Guide to Patient Monitoring Technology.* USA: Springer.

[7] FIALA, J. – STUDENÝ, A. 2016. *Specifiká řízení IT v nemocnicích.* [online]. Brno: SystemOnLine.cz, 2016. [cit. 07. 02. 2020]. Dostupné na: https://www.systemonline.cz/ sprava-it/specifika-rizeni-it-v-nemocnicich.htm

[8] HANSEN, D. 2012. *Health Information Science.* Challenges and Opportunities for Health Information Systems Research. Nemecko: Springer.

[9] HRAŠKOVÁ, D. 2014. Telemedicína – nové trendy v zdravotníctve. *Verejná správa: školy, úrady, obce, kultúra, zdravotníctvo, rozpočtové, príspevkové, neziskové organizácie*. 2014, 8(11), 55 ─ 57.

[10] HUNKOVÁ, M. 2018. Zdravotnícke zariadenia často riešia IT bezpečnosť, keď je už neskoro. *TREND – týždenník o ekonomike a podnikaní.* 2018, 27(15), 55 ─ 56.

[11] ITAPA. *Prieskum stavu riadenia informačnej bezpečnosti.* [online]. Bratislava: ITAPA, 2011. [cit. 07. 02. 2020] Dostupné na: https:/www.itapa.sk/3169-sk/prieskum-stavu-riadenia--informacnej-bezpecnosti/

[12] MINISTERSTVO FINANCIÍ SR. *Prieskum stavu informačnej bezpečnosti vo verejnej správe v Slovenskej republike v roku 2013.* [online]. Bratislava: MF SR, 2013. [cit. 08. 02. 2020] Dostupné na: http://www.informatizacia.sk/prieskum-stavu-ib/12772s

[13] MOGHADDASI, H. – MOHAMMADPOUR, A. – BOURAGHI, H. – AZIZI, A. – MAZAHERILAGHAB, H. 2018. Hospital Information Systems: The status and approaches in selected countries of the Middle East. *Electronic physician.* 2018, 10(5), 6829 – 6835.

[14] SAYLES, N. 2012. *Health Information Management Technology: An Applied Approach.* USA: American Health Information Management Association.

[15] STŘEDA, L. 2018. *eHealth a telemedicína: Nemocničné informačné systémy.* [online]. Bratislava: Národný inštitút zdravia, 2018. [cit. 05. 02. 2020]. Dostupné na: http://www.niz.sk/zdravotnicke-noviny/ehealth-a-telemedicina-13/

[16] TOUCHIT. 2020. *IT bezpečnosť: Najviac ohrozené sú malé a stredne veľké firmy.* [online]. Bratislava: Touchit, 2020. [cit. 06. 02. 2020]. Dostupné na: https://touchit.sk/it-bezpecnost-najviac-ohrozene-su-male-a-stredne-velke-firmy/278623

[17] ÚRAD PODPREDSEDU VLÁDY SR PRE INVESTÍCIE A INFORMATIZÁCIU. 2019. *Strategická priorita – Informačná a kybernetická bezpečnosť.* [online]. Bratislava: Úrad podpredsedu vlády SR pre investície a informatizáciu, 2019. [cit. 06. 02. 2020]. Dostupné na: https://www.vicepremier.gov.sk/wp-content/uploads/2019/08/SP_Inform_kybern_ bezpecnost_schvalena_2019_07_25_v1.0.pdf