Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Návrh metodiky bezpečnosti IS v mikropodniku

Bc. Tomáš Vyskot

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Tomáš Vyskot

Veřejná správa a regionální rozvoj – c.v. Hradec Králové

Název práce

Návrh metodiky bezpečnosti IS v mikropodniku.

Název anglicky

Proposal of IS security methodology in a micro-enterprise.

Cíle práce

Hlavním cílem diplomové práce je analýza IS a vytvoření návrhu metodiky bezpečnosti informačního systému v mikropodniku. Aplikační prostředí bude ambulance praktického lékaře.
Dílčím cílem je zjištění stavu provozu informačního systému, analýza a popis procesů mikropodniku.
Osnova práce:
IS a přístup k systémem řízení bezpečnosti informací.
Legislativa bezpečnosti IS v mikropodniku.
Provoz IS v mikropodniku při komunikaci s veřejnou správou.
Analýza IS v ambulanci praktického lékař.
Návrh metodiky bezpečnosti IS v mikropodniku.

Metodika

Rešerše odborné literatury, standardů a legislativních norem v ČR.

Popis provozu IS v mikropodniku při komunikaci s veřejnou správou.

Modelování procesů.

Analýza IS mikropodniku v aplikačním prostředí.

SWOT analýza mikropodniku.

Matice rizik – nástroj pro analýzu rizik bezpečnosti informací v mikropodniku.

Prezentace přínosu diplomové práce

Doporučený rozsah práce

55

Klíčová slova

Norma ČSN ISO/IEC 27001, bezpečnost informací, informační systém, mikropodnik, modelování procesů, matice rizik, digitální certifikát.

Doporučené zdroje informací

ČSN EN ISO/IEC 27001 (369797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Druhé vydání, Praha. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

Gála, L. Pour, J. Šedivá Z. Podniková informatika, 2.vydání. Praha: Grada Publishing, a. s., 2009, ISBN 80-247-2615-1.

VOŘÍŠEK, Jiří, POUR, Jan, BUCHALCEVOVÁ, Alena. Management of Business Informatics Model – Principles and Practices. E+M. Ekonomie a Management [online], 2015, roč. 18, č. 3, s. 160–173. ISSN 1212-3609. URL: http://www.ekonomie-management.cz/download/1441645370_f8e8/14_MANAGEMENT+OF+BUSINESS+INFORMATICS.pdf

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, 2000.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Ing. Karel Kubata, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 2. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 23. 09. 2023

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Návrh metodiky bezpečnosti IS v mikropodniku" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 25. 11. 2023 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Karlu Kubatovi, Ph.D. za vedení práce, cílené připomínky, vstřícný a odborný přístup. Děkuji MUDr. Ivě Martinkové za umožnění rozhovorů o lékařské praxi, poskytnutí důvěry při řešení jednotlivých problémů v průběhu zavádění nového aplikačního IS v ambulanci praktického lékaře a umožnění postupné realizace opatření dle navrhnuté metodiky bezpečnosti IS do praxe. Za právní rady, poskytnutí konzultací a výkladu zdravotnického práva děkuji Mgr. MUDr. Danielu Thibaudovi z Armády České republiky. Dále děkuji za poskytnutí brainstormingu chápání kybernetické bezpečnosti ve zdravotnictví Ing. Ctiradu Procházkovi z MZČR. Děkuji Františku Janů konzultantovi z GORDIC spol. s.r.o. za poskytnutí konzultace způsobu chápání analýzy rizik ve zdravotnickém zařízení.

Návrh metodiky bezpečnosti IS v mikropodniku

Abstrakt

Diplomová práce je zaměřena na vytvoření návrhu metodiky bezpečnosti informačního systému v mikropodniku. Aplikačním prostředím je ambulance praktického lékaře.

V úvodu teoretické části je definován rozsah systému řízení bezpečnosti informací a právní rámec chápání informační bezpečnosti v mikropodniku s přesahem do zdravotnictví. V praktické části autor vypracoval SWOT analýzu, kontext organizace a vytvořil model poskytování zdravotnické péče, který vede k vymezení primárních aktiv a to: zdravotní péče, zdravotnická dokumentace, účtování zdravotních služeb a aplikační IS. Byl identifikován proces manipulace s informacemi na základě opatření GDPR. Hodnocení primárních aktiv bylo provedeno dle prováděcí vyhlášky o kybernetické bezpečnosti. Byly identifikovány hrozby, zranitelnosti a rizika. Na základě analýzy rizik byla navrhnuta opatření.

Autor navrhl metodický postup bezpečnosti IS v mikropodniku s implementací systému řízení bezpečnosti informací na základě ISO/IEC 27001 v ambulanci praktického lékaře. Metodika je návrhem základních kroků vedoucích k zákonitosti, účelu, způsobu manipulace a ochraně zdravotnických informací, interních informací mikropodniku a informací obsahující osobní údaje. Cílem metodiky bezpečnosti IS je dodržování principu důvěrnosti, integrity a dostupnosti při provozu mikropodniku s přijatými opatřeními k ochraně aktiv.

Klíčová slova: Ambulance, analýza rizik, bezpečnost informací, digitální certifikát, informační systém, ISMS, kybernetická bezpečnost, matice rizik, metodika, mikropodnik, modelování procesů, norma ČSN ISO/IEC 27001, politika bezpečnosti IS, zdravotní péče.

Proposal of IS security methodology in a micro-enterprise

Abstract

The diploma thesis is focused on the creation of a proposal for the methodology of information system security in a micro-enterprise. The application environment is the general practitioner's ambulance.

The introduction of the theoretical part defines the scope of the information security system and the legal framework of understanding information security in a micro-enterprise with an overlap into health care.

In the practical part, the author elaborated a SWOT analysis, the context of the organization and created a model of health care provision, which leads to the definition of primary assets, namely: health care, medical documentation, billing of health services and application IS. The process of information manipulation based on GDPR measures has been identified. The evaluation of primary assets was carried out in accordance with the Cybersecurity Implementing Decree. Threats, vulnerabilities, and risks have been identified. Based on a risk analysis, measures were proposed.

The author proposed a methodological procedure of IS security in a micro-enterprise with the implementation of an information security management system based on ISO/IEC 27001 in a general practitioner's ambulance. The methodology is a proposal of basic steps leading to the law, purpose, method of manipulation and protection of health information, internal information of a micro-enterprise and information containing personal data. The aim of the IS security methodology is to adhere to the principle of confidentiality, integrity and availability in the operation of a micro-enterprise with measures taken to protect assets.

Keywords: Ambulance, risk analysis, information security, digital certificate, information system, ISMS, cyber security, risk matrix, methodology, microenterprise, process modelling, ČSN ISO/IEC 27001 standard, IS security policy, health care.

Obsah

1 Úvod ... 11

2 Cíl práce a metodika ... 12

3 Teoretická část práce ... 14

3.1 Informační systém ... 15

3.2 Systém řízení bezpečnosti informací ... 18

3.2.1 Definice ISMS ... 19

3.2.2 Interpretace přístupu k rozsahu ISMS ... 20

3.2.3 Obecné zásady implementace ISMS ... 22

3.2.4 Metodika ISMS ve zdravotnictví ... 25

3.2.5 Hodnocení bezpečnosti informací CIA ... 27

3.3 Legislativa bezpečnosti IS v mikropodniku ... 28

3.3.1 GDPR a minimální standardy zabezpečení osobních údajů ... 31

3.3.2 Zákony a vyhlášky ... 33

3.3.3 Normy ... 34

3.4 Porovnání vybraných bezpečnostních standardů ... 39

3.4.1 Porovnání ISMS, ITIL, COBIT ... 39

3.4.2 MBI model ... 42

4 Praktická část práce ... 47

4.1 Realizace ISMS ve zdravotnickém zařízení ... 47

4.2 Rámec hlavního aktiva organizace ... 49

4.3 Kontext modelu zdravotnického zařízení ... 50

4.4 Analýza vstupního stavu ISMS mikropodniku ... 54

4.4.1 SWOT analýza ... 55

4.4.2 GAP analýza ... 56

4.5 Model zdravotní péče v mikropodniku ... 59

4.5.1 Model zdravotní péče ... 59

4.5.2 Aplikační IS ... 61

4.5.3 Řízení zpracování informací ... 63

4.6 Organizace bezpečnosti informací ... 67

4.6.1 Základní řešení bezpečnosti informací v mikropodniku ... 67

4.6.2 Rozsah systému řízení bezpečnosti informací ... 67

4.6.3 Fyzická bezpečnost ... 68

4.6.4 Role v ISMS organizace ... 69

4.7 Identifikace a správa informačních aktiv ... 71

4.7.1 Identifikace aktiv ... 74

4.7.2 Hodnocení aktiv ... 78

4.8 Analýza a řízení rizik 80
4.8.1 Hrozby 82
4.8.2 Zranitelnosti 83
4.8.3 Matice rizik 83
4.8.4 Registr rizik 85
4.8.5 Posouzení dopadu 88
4.8.6 Ošetření a akceptace rizik 89
4.8.7 Řízení rizika 89
4.9 Návrh metodiky bezpečnosti IS v mikropodniku 93
4.9.1 Analýza počátečního stavu 94
4.9.2 Zpracování kontextu organizace 94
4.9.3 Rozsah aplikovatelnosti ISO 27001 94
4.9.4 Identifikace aktiv a analýza rizik 95
4.9.5 Ošetření rizik a nastavení bezpečnosti IS 95
4.9.6 Zpracování dokumentace a stanovení rolí ISMS 101
4.9.7 Školení zaměstnanců 101
4.9.8 Poskytování zdravotní péče 101
4.9.9 Audit a certifikace 101

5 Zhodnocení výsledků 102

6 Závěr 105

7 Seznam použitých zdrojů 106

8 Seznam obrázků, tabulek, grafů a zkratek 112
8.1 Seznam obrázků 112
8.2 Seznam tabulek 112
8.3 Seznam grafů 112
8.4 Seznam použitých zkratek 113

Přílohy 115

1 Úvod

Zdravotnictví, ambulance, lékař, pacient a informace asi každému z nás evokují návštěvu našeho praktika. V nedávné minulosti, před příchodem počítačů a elektronizace zdravotnictví, byla v ambulancích typická osobní komunikace převážně lékař – pacient. Zdravotníci zaznamenávali informace na papír a lékařské správy se zakládali do rozsáhlých papírových karet pacientů. Tyto informace se uchovávali v kartotékách a při potřebě přenosu lékařské správy se využívalo poštovních služeb pošty. Tyto záznamy obsahovaly detaily o diagnózách, léčbě a dalších důležitých informacích o pacientech. Recepty a neschopenky měli pouze papírovou podobu. Lékaři se spoléhali na své paměťové schopnosti a znalosti při poskytování péče pacientům a s jinými lékaři, pojišťovnami a veřejnou správou komunikovali telefonem a na stroji psaným dopisem. Pro bezpečnost informací stačilo zdravotní dokumentaci zamknout do kartotéky.

V moderním zdravotnictví jsou provozovány rozsáhlé informační systému, postavené na výměně dat v prostředí internetu. Podle Riana a Švarcové (2010) internet nerespektuje hranice států a kontinentů, časová pásma nehrají svou roli, dokonce ani fyzická poloha komunikujících subjektů není podstatným prvkem komunikace. Podle Kofránka a kol. (2017) informace o pacientech jsou elektronickými informacemi a elektronickými zdravotními záznamy, zpracovávány, ukládány a sdíleny v registrech a informačních systémech veřejné správy, zdravotních pojišťoven. Databáze v informačním systému poskytovatelů zdravotní péče jsou zdrojem osobních údajů občana a zdravotnických informací o pacientovi napojené na agendové systémy. Informační systémy poskytovatelů zdravotní péče podle PostSignum (2023) pro komunikaci v prostředí internetu se státními orgány a veřejnou správou užívají kvalifikovaných certifikátů a datových schránek.

V současnosti NÚKIB (2020a) upozorňuje na hrozby, především kybernetické útoky na informační systémy a komunikační infrastrukturu zdravotnictví. Podle NÚKIB (2020b) útočník využívá slabých míst informačního systému k zisku informací, například pomocí zneužití identifikace a autentizace uživatele, nefunkční ochrany proti škodlivému kódu či nedostatečným opatřením v komunikační bezpečnosti. Existuje riziko hrozby zneužití zranitelnosti a tím narušení důvěrnosti, integrity a dostupnosti informací. Přijetí vhodných opatření pro ochranu systémů a informací podle ISO 27799 (2019) povede k snížení intenzity rizika nebo riziko zcela eliminuje.

2 Cíl práce a metodika

Hlavním cílem této diplomové práce je vytvoření návrhu metodiky bezpečnosti informačního systému v mikropodniku, která zakládá na nezbytnosti implementace systému řízení informační bezpečnosti ISMS dle ISO/IEC 27001.

Dílčím cílem je zjištění stavu provozu informačního systému, identifikace rámce činnosti, analýza a popis procesů mikropodniku. V souvislosti bude nutné identifikovat aktiva, informační toky pro manipulaci s informací, provést analýzu rizik a navrhnout opatření pro nastavení bezpečnosti informací a provozu IS. Zavedení bezpečnosti IS dokumentovat vhodnou politikou a směrnicí.

Postup provedení diplomové práce:

1. Definice informačního systému, přístupu k systému řízení bezpečnosti informací, porovnání ISMS s vybranými metodikami pro správu a řízení IS.
2. Provedení rešerše informačních zdrojů odborné literatury, norem, standardů a užité legislativy.
3. Analýza IS mikropodniku v souvislosti s ISO/IEC 27001.
4. Návrh metodiky bezpečnosti IS v mikropodniku.
5. Zhodnocení přínosu diplomové práce pro praxi.

Použité metody a metodiky pro splnění cílů diplomové práce jsou:

- Kvalitativní výzkum formou nestrukturovaných a polostrukturovaných rozhovorů.
    - Rozhovor č.1 s lékařem (poskytovatel zdravotní péče) a administrátorem IS mikropodniku dne 8. a 9. prosinec 2022 na téma:
        - porozumění organizaci podle kap. 4, kontext organizace, ISO/IEC 27001 (polostrukturovaný rozhovor, kapitola 4.3);
        - informace o provozovaném IS a podnikatelské činnosti, které jsou vstupem pro analýzu a identifikaci procesů, aktiv (polostrukturovaný rozhovor, kapitola 4.7), zjištění aktuálního stavu užívání opatření informační bezpečnosti v mikropodniku pro SWOT a GAP analýzu za přítomnosti správce IS (polostrukturovaný rozhovor na základě PoA, kapitola 4.4).

- Rozhovor č.2 s lékařem a právníkem dne 27. ledna 2023 na téma:
  - stanovení rámce poskytování zdravotní péče jako primárního aktiva dle zákona č.372/2011 a souvislosti s ISMS v ISO 27799) (nestrukturovaný rozhovor, kapitola 4.3);
  - identifikace postupů manipulace s informacemi dle metodiky GDPR (polostrukturovaný rozhovor, kapitola 4.5.3).
- Rozhovor č.3 s vedoucím oddělení informačních a komunikačních technologií MZČR dne 30. ledna 2023 na téma:
  - zkušenost s ISMS a KB ve zdravotnickém zařízení (nestrukturovaný rozhovor).
- Rozhovor č.4 s konzultantem kybernetické bezpečnosti, dne 15. února 2023 :
  - uchopení analýzy rizik ve zdravotnictví, hodnocení navržených aktiv (dle CIA), hrozeb , zranitelností, rizik dle VKB přílohy č.1, 2, 3 a analýza rizik dle ISO/IEC 27005 (nestrukturovaný rozhovor).

- Metoda popisu aktuální vybrané legislativy, technických norem a dostupných informačních zdrojů v souvislosti s ISMS.
- Explorace základních teoretických znalostí o MBI a metodikách pro řízení IT ITIL4 a COBIT 2019.
- Analýza metodiky ISMS dle norem ISO/IEC 2700x.
- Metoda EPC (Event-driven Proces Chain) pro modelování procesu mikropodniku.
- SWOT analýza informační bezpečnosti organizace (stávající stav).
- GAP analýza k porovnání rozdílu stávajícího a cílového stavu opatření ISO/IEC 27001.
- Kvalitativní metoda analýzy rizik dle metodiky normy ISO/IEC 27005.

3 Teoretická část práce

Bezpečnost, informační bezpečnost, bezpečnost informačních systémů jsou pojmy, které od roku 2000, kdy byl vydán zákon č. 365/2000 Sb., „O informačních systémech veřejné správy“ se staly nedílnou součástí implementace nově nasazovaných informačních systémů ve veřejné správě a v podnicích. V současné době mezi standarty implementace systému řízení bezpečnosti informací řadíme také požadavky ČSN EN ISO/IEC 27001:2014. Každý řídící pracovník by měl znát základní principy řízení bezpečnosti informací a prosazovat je.

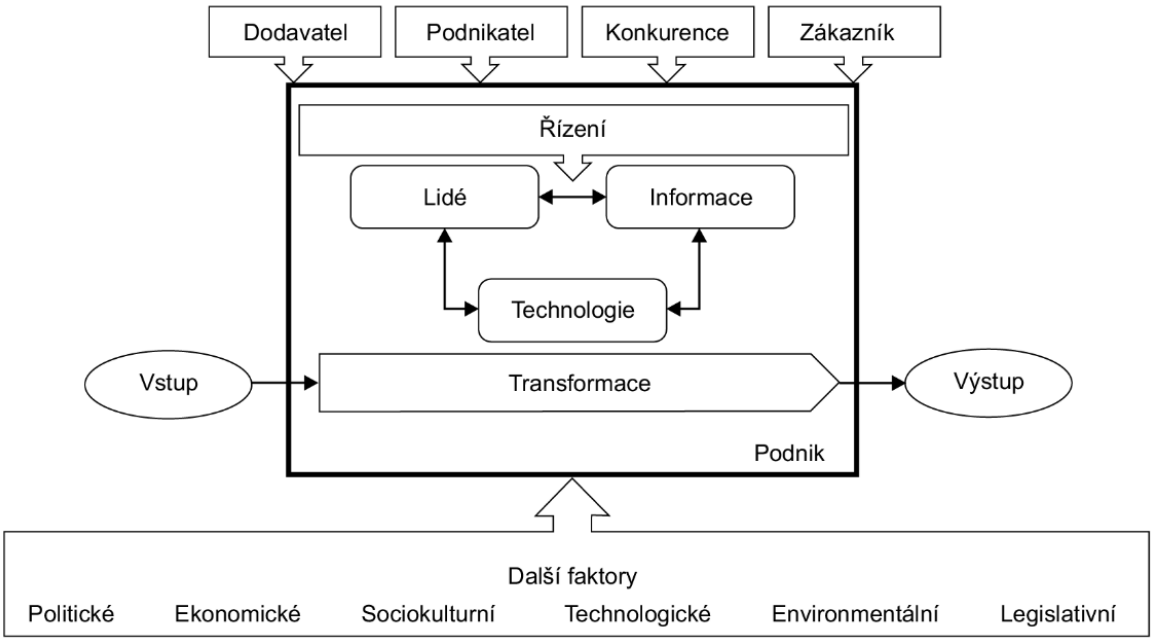
Podnik jako ekonomický subjekt a je zaměřen na svoji profesní působnost na trhu. Jeho cílem je vyrábět a prodávat výroby či poskytovat služby. Základním cílem je růst a zisk. Podporou pro dosažení cíle může být systém řízení bezpečnosti informací.

Podnik, který nakládá s informacemi (daty) vlastní společnosti, zákazníků, obchodních partnerů, veřejné správy (e-government), a je v komunikačním prostředí propojen do jiných informačních systému a registrů, by měla být implementace systémového přístupu řízení bezpečnosti informací požadována. Očekávaným přínosem podle ISO 27000 (2018) je:

- dosažení podnikatelských cílů organizace;
- znalost vytváření, zpracování, ukládání, přenášení a ochrany informací;
- přehled o informačních aktivech a znalosti jejich hodnoty CIA;
- znalost a řízení rizik informačních a obchodních aktiv;
- nastavený životní cyklus informačního systému;
- zavedení školení a vzdělávání zaměstnanců z bezpečnosti informací a IS;
- zvýšení důvěry organizace u zúčastněných stran;
- efektivní ekonomické řízení investic;
- podporuje certifikaci organizace dle ISO/IEC 27000.

Tato práce je zaměřena na vytvoření návrhu metodiky bezpečnosti informací v informačním systému v prostředí mikropodniku. **Mikropodnik** podle publikace EU „Uživatelská příručka k definici malých a středních podniků“ (2019) je definován dle směrnice Evropské unie jako podnik s méně než 10 zaměstnanci a obratem do 2 milionů euro.
Podle Buchalcevové (2008) mikropodniky mají specifické byznys modely a byznys cíle, malý podíl na trhu, limitované finanční a lidské zdroje, odlišnou organizační strukturu, a proto vyžadují odlišný přístup k zavádění a posuzování ICT procesů.

Obrázek 1 Vnímání podniku jako systému



Zdroj: Gála a kol. (2015)

Podnik podle Gály a kol. (2015) můžeme chápat jako systém. Pokud na podnik nahlížíme jako na systém, pak se jedná o živý, otevřený a komplexní systém. Pozornost vnímání podniku jako systému věnujeme proto, že jeho subsystém je podnikový informační systém. Na obrázku 1 je znázorněno vnímání podniku jako systému s vyznačením jeho klíčových prvků a také jejich vazeb a prvků okolí, resp. prostředí.

V této práci mikropodnik je reprezentován firmou s.r.o., ambulancí všeobecného praktického lékaře s čtyřmi zaměstnanci a přibližně 2000 pacienty (zákazníky). Ambulance všeobecného praktického lékaře je v komunikačním prostředí propojena s obchodními partnery, veřejnou správou a zdravotními pojišťovnami. Celý informační systém podniku zpracovává hlasovou komunikaci, analogové a elektronické dokumenty.

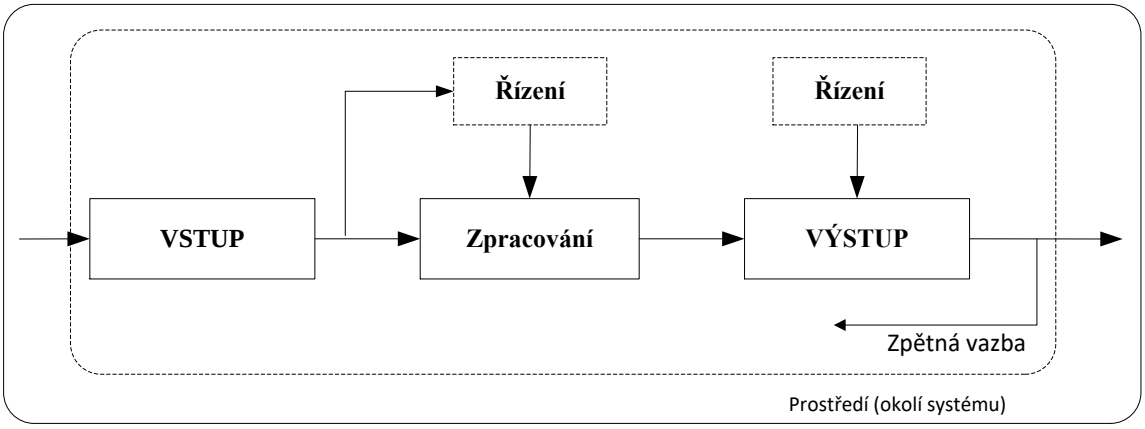
3.1 Informační systém

Dle Gály a kol. (2009) definujeme:

Systém je účelově definovaná neprázdná množina prvků a množina vazeb mezi nimi, přičemž vlastnosti prvků a vazeb mezi nimi určují vlastnosti (chování) celku. Pro takto definovaný systém identifikujeme především:

- **účel systému**, tj. cíl, resp. cílové chování systému;
- **strukturu systému**, tj. prvky systému a vazby mezi nimi;
- **vlastnosti prvků** systému významné pro celkové chování systému;
- **vlastnosti vazeb** mezi prvky systému, významné pro celkové chování systému;
- **okolí systému**, tj. vymezení prvků, které již nepatří do systému, ale jejichž vlastnosti a vazby systému na tyto prvky okolí významným způsobem ovlivňují chování systému;
- **případné subsystémy**, pokud zkoumání systému jako celku je příliš složité a je třeba (a hlavně je možné) systém rozdělit na menší relativně samostatné (uzavřené) celky uvnitř systému.

Obrázek 2 Komponenty informačního systému



Zdroj: vlastní zpracování, Gála a kol. (2009)

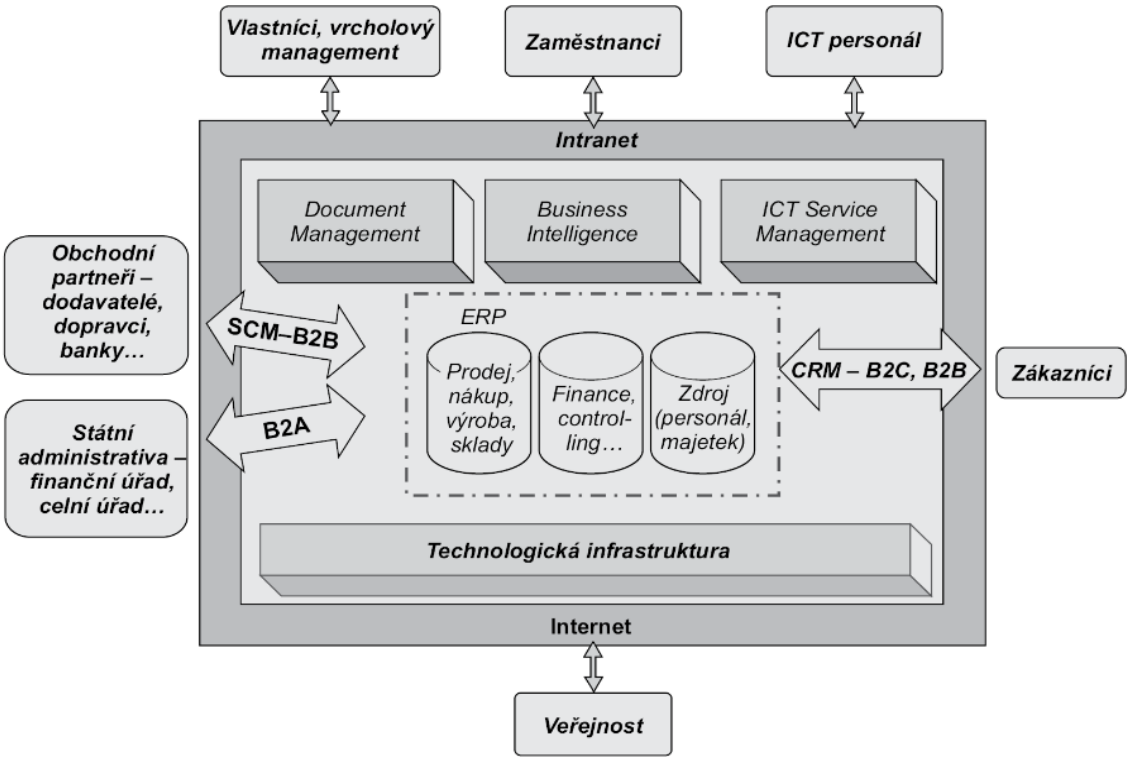
V informatice se takový systém označuje pojmem **informační systém**, který je znázorněn na obrázku 2. Jeho účelem je zajištění vhodného vyjádření informací, jejich zpracování a přenášení v rámci nějakého systému. Obecně je pak tvořen lidmi, vhodnými nástroji a metodami, které jsou seskupeny do tří základních komponent (Gála a kol., 2009):

- **vstup** – zahrnuje prvky, umožňující zachytit informační a další postupy, které mají být předmětem zpracování, případně vstupy vzájemně propojit;
- **zpracování –** zahrnuje prvky, které zajišťují transformaci vstupů do požadovaného výstupu;
- **výstup** – představuje prvky, které jsou schopny přenést informační a další výstupy k jeho příjemci (uživateli).

Takový systém je pak rozšířen o komponenty, které zajišťují jeho **řízení** a **zpětnou vazbu.**

Pro potřebu interpretace současného informačního systému v zájmovém mikropodniku použijeme interpretace dle Brucknera (2012) uvedené na obrázku 3, kdy využívání informačních a komunikačních technologií ICT překročilo hranice jednotlivých podniků. Nové aplikace, jako například EDI (Electronic Data Interchange), CRM (Customer Relationship Management) a SCM (Supply Chain Management), nové přístupy k integraci aplikací (B2B, B2C, B2G) se zaměřily na podporu vzájemné spolupráce a vzájemné komunikace podniků v dodavatelských řetězcích, podniků s jejich zákazníky a podniků se státní správou (sociální a zdravotní pojištění, daně, cla atd.).

Obrázek 3 Typická struktura současného IS



Zdroj: Bruckner (2012)

Podle Halbicha a kol. (2015) informační systémy se objevují jako kritické součásti v každém podniku a organizaci, kdy správný výběr informačních technologií, v širším slova smyslu, hraje klíčovou roli v moderních podnikových informačních systémech.

Současně s rozvojem informačních technologií a požadavků na propojení jednotlivých systémů přibyla řada dalších netriviálních problémů, zejména (Bruckner, 2012):

- jak umožnit propojení a vzájemnou komunikaci různých informačních systémů různých subjektů;

- jak současně zajistit vysokou bezpečnost a spolehlivost propojených systémů;
- jak byznys aplikacemi podpořit odpovídající kvalitu a včasnost dodávek.

V současnosti je zájmový mikropodnik na informačním systému životně závislý. Zpracovává velké množství informací a je součásti komunikačního prostředí B2A, B2B, B2C, B2G. Pro uchovávání informací v IS podle Tyrychtra (2015) je vhodná forma databáze, která je vymezena jako soubor souvisejících dat postačujících pro daný účel nebo pro daný systém zpracování dat. Pro přístup k informacím je vhodné zavést systém řízení báze dat, který představuje skupinu programů fungujících jako rozhraní mezi daty v databázi a uživatelem užitím aplikačního programu. Aplikační program (software) slouží pro manipulaci s daty, umožňuje vkládání a aktualizaci dat, vyhledávání, výběr, prezentaci, tvorbu formulářů a řízení přístupu uživatelů k datům. Databáze jsou základem IS.

Z těchto důvodů je potřeba nastavit kvalitní systém řízení podnikového IS především se zaměřit na systém řízení informační bezpečnosti neboli ISMS.

3.2 Systém řízení bezpečnosti informací

Aktuální stav informační bezpečnosti, ochrany a způsobu manipulace s informacemi v mikropodniku ambulance praktického lékaře vychází z *Nařízení Evropského parlamentu a Rady (EU) 2016/679* ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů. Česká verze daného nařízení Těšitelová a kol. (2018) je právní předpis, který metodicky zavedl praxi ochrany osobních údajů s účinností od 25. května 2018. Toto opatření informační bezpečnosti je známo jako politika GDPR, která je pro ambulance VPL povinná. Jedná se o základní pravidla informační bezpečnosti pro ochranu a zpracování informací (osobních údajů).

Zpracování informací podporuje podnikový IS. Podle NÚKIB (2022a) je informační systém tvořen technickým a programovým vybavením, komunikačními prostředky, objekty, zaměstnanci a dodavateli, informacemi, které systém zpracovává a službami (procesy), které daný systém poskytuje. Systém je vymezen procesy, informačními aktivy.

Informační aktiva dle Jiráska a kol. (2015) jsou výsledné, tj. vybrané či jinak zpracované údaje (data), prezentované ve formě snadno čitelné, pochopitelné a využitelné subjektem, jemuž jsou určeny. Mohou být v elektronické formě nebo napsané (vytištěné) v listinné formě, vyřčené při jednání nebo zaznamenané na jiném médiu.

Data obsažená v informačních aktivech prezentujeme jako informace. **Informace** dle ISO 27000 (2018) představují aktivum, které stejně jako další důležitá aktiva organizace je podstatné pro činnost organizace a vyžaduje odpovídající ochranu.

Příslušná opatření pro nastavení ochrany informací se v organizaci podle ISO 27000 (2018), specifikují jako **bezpečnost informací**, kde základem bezpečnosti je požadavek zachování důvěrnosti, integrity a dostupnosti informací s cílem zachování kontinuity činnosti organizace a minimalizací dopadů incidentů způsobených hrozbami na zranitelnostech IS organizace. Informační bezpečnosti v mikropodniku dosahujeme řízením bezpečnosti informací.

Systém řízení používá k dosažení cílů organizace systém zdrojů. Systém řízení zahrnuje strukturu, politiky, plánovací činnosti, odpovědnosti, praktiky, postupy, procesy a zdroje organizace. (ISO 27000, 2018)

3.2.1 Definice ISMS

ISMS (Systém řízení bezpečnosti informací) podle ISO 27000 (2014) se sestává z politik, postupů, směrnic a příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustanovení, implementování, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací organizace tak, aby byly dosaženy její cíle. Je založen na posuzování rizik a na úrovních přijetí rizik organizace, které byly navrženy pro efektivní ošetření rizik a pro jejich řízení. K úspěšné implementaci ISMS přispívá analýza požadavků na ochranu informačních aktiv a aplikace příslušných opatření s cílem zajistit ochranu těchto informačních aktiv v souladu s požadavky. K úspěšné implementaci ISMS rovněž přispívají dále uvedené základní principy (ISO 27000, 2018):

- povědomí o potřebě bezpečnosti informací;
- určení odpovědnosti za bezpečnost informací;
- začlenění závazku vedení a zájmů zúčastněných stran;
- zvýšení společenských hodnot;
- posouzení rizika, na jehož základě budou stanovena příslušná opatření, aby bylo dosaženo přijatelných úrovní rizika;
- bezpečnost začleněná jako základní prvek do informačních sítí a systémů;
- aktivní prevence a detekce incidentů bezpečnosti informací;

- zajištění komplexního přístupu k řízení bezpečnosti informací;
- neustálé opakované posuzování bezpečnosti informací a provádění modifikací podle potřeby.

Vhodné definice z praxe:

Dle Nováka (2011) ISMS je soubor pravidel a opatření, po jejichž zavedení má správné a úplné informace (princip integrity) včas k dispozici ten, kdo je skutečně potřebuje (princip dostupnosti) a pouze ten, kdo je k přístupu k nim oprávněn (princip důvěrnosti).

ISMS (Information Security Management System) je systém řízení informační bezpečnosti. Jde o metodický manuál, směrnice, politiky, cíle, pracovní postupy a procesní systém řízení. Jeho účelem je nastavit procesy v organizaci tak, aby byla maximálně posílena bezpečnost a minimalizovány rizika. A protože 100% bezpečnost neexistuje, ISMS se zabývá i tím, jak minimalizovat dopady plynoucí z narušení bezpečnosti a z bezpečnostních rizik. (Tayllorcox, 2022)

Pro vybudovaní systému řízení bezpečnosti informací je vhodné realizovat ISMS dle ISO/IEC 27001, kdy realizace bezpečnostních opatření se řídí postupy pro řízení bezpečnosti informací uvedených v ISO/IEC 27002, souvisejících normách ISO/IEC 2700x a je vhodné využít souvislostí v ZKB a VKB například pro interpretaci rozsahu ISMS a nastavení hodnocení požadavků bezpečnosti informací.

3.2.2 Interpretace přístupu k rozsahu ISMS

Národní úřad pro kybernetickou bezpečnost na svém úložišti publikovaných podpůrných materiálů „Metodiky, doporučení a standardy“[1] v dokumentu NÚKIB (2022a) interpretuje přístup k ISMS jako stěžejní organizační bezpečnostní opatření pro zajištění kybernetické bezpečnosti daného systému, jehož základ je upraven v § 3, VKB.
Podle NÚKIB (2022a), dle VKB je rozsah ISMS nutno stanovit dokumentovanou formou a s ohledem na požadavky dotčených stran a organizační bezpečnost. Smyslem stanovení rozsahu je určit organizační části a aktiva, jichž se ISMS týká, tedy fyzický perimetr,

[1] NUKIB, Podpůrné materiály [online].[cit. 2022-08-20]. Dostupný z: <https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/podpurne-materialy/>.

organizační celky, zainteresované osoby (zaměstnanci, dodavatelé) a technologie. Dokumentované stanovení rozsahu ISMS je nezbytné pro následnou přezkoumatelnost, případnou potřebu jeho rozšíření, či pro zajištění jeho jednotného výkladu v organizaci. Pevně daným je specifický požadavek zákona o kybernetické bezpečnosti, reprezentován povinností povinné osoby zabezpečovat určený nebo identifikovaný systém spadající do působnosti zákona o kybernetické bezpečnosti. Tímto je dán **minimální rozsah ISMS** odpovídající rozsahu určeného informačního nebo komunikačního systému, který je interpretován na obrázku 4 A).

Vedle nutnosti stanovit rozsah ISMS, má ale povinná osoba podle § 4 odst. 2 ZKB zavést ISMS (a další bezpečnostní opatření) v rozsahu nezbytném pro zajištění kybernetické bezpečnosti daného systému. Z toho vyplývá, že tato povinnost povede k tomu, že povinná osoba v souladu s § 3 písm. a) VKB zohlední požadavky dalších dotčených stran a požadavky organizační bezpečnosti, a zvolí rozsah ISMS na větší část aktiv povinné osoby, než jsou **aktiva určeného nebo identifikovaného systému**, tedy **zahrne i aktiva, která zabezpečují jeho kybernetickou bezpečnost**, viz. obrázek 4 B. To pak může vést také k tomu, že do rozsahu **ISMS zahrne všechna aktiva v organizaci**, viz. obrázek 4 C.

Jakmile povinná osoba stanoví rozsah ISMS, zavádí pro takto stanovený rozsah na základě cílů, bezpečnostních potřeb a hodnocení rizik přiměřená bezpečnostní opatření.

Obrázek 4 Rozsah ISMS varianta A, B, C

A) B) C)

Zdroj: NÚKIB (2022a)

3.2.3 Obecné zásady implementace ISMS

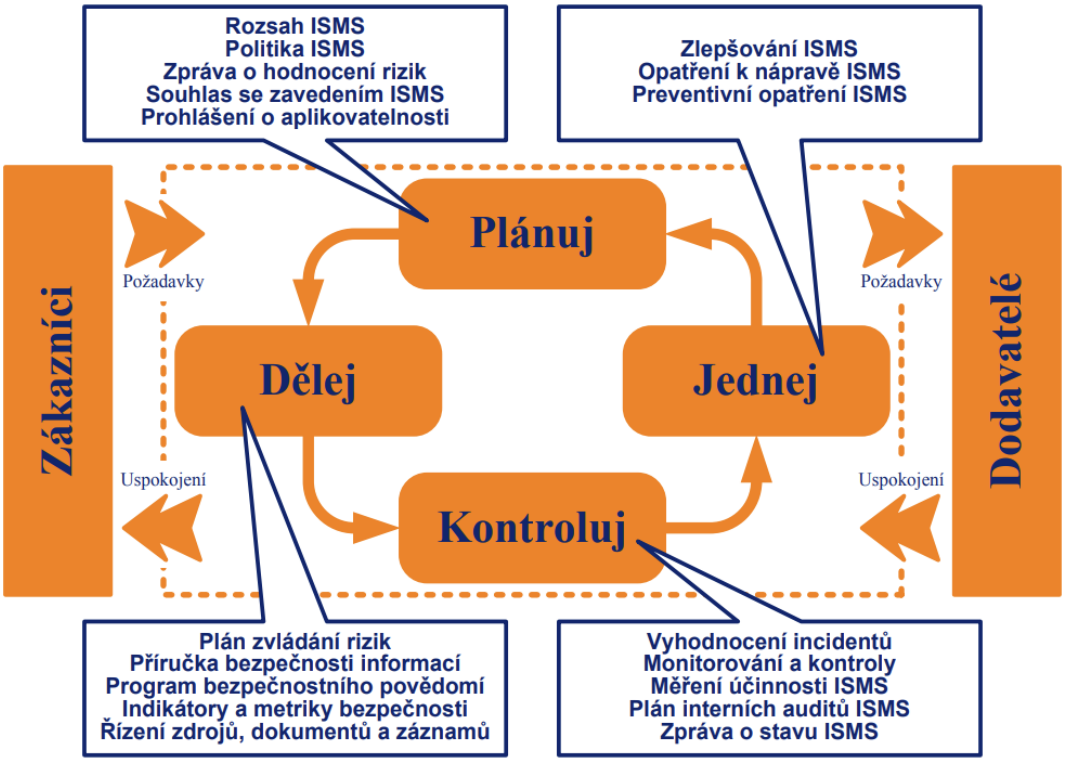
ISMS nabízí komplexní systém k řízení informační bezpečnosti, který je založen na využití Demingovova cyklu Plan – Do – Check – Act neboli **modelu PDCA** uvedeném na obrázku 5. Tento model je obecnou zásadou implementace ISMS dle ISO/IEC 27001, která je řídící normou. Prováděcí normou je ISO/IEC 27002, pomocí které realizujeme opatření k zavedení a udržení ISMS v organizaci. Cíle opatření a jednotlivá opatření k informační bezpečnosti jsou rozdělena do 14 oblastí. Dle přílohy A, (ISO 27001, 2014) to jsou:

- politiky bezpečnosti informací (A.5) – definice základních pravidel a principů bezpečnosti informací, jakým způsobem organizace má v úmyslu plnit požadavky na bezpečnost informací;
- organizace bezpečnosti informací (A.6) – stanovení rámce řízení k počáteční implementaci, řízení a provozování bezpečnosti informací v organizaci, kdy jsou stanoveny interní role, přiděleny odpovědnosti a definovány vztahy s externími příslušnými orgány, autoritami a zájmovými skupinami;
- bezpečnost lidských zdrojů (A.7) - cílem je zajistit, aby zaměstnanci a smluvní strany rozuměli svým povinnostem, pro jednotlivé role byly vybráni vhodní kandidáti a personál organizace byl si vědom a plnil určené povinnosti v oblasti bezpečnosti informací;
- řízení aktiv (A.8) – cílem opatření je identifikovat aktiva organizace, definovat odpovědnost za aktiva, klasifikovat informace a definovat manipulaci v souvislosti s přiměřenou ochranou informací;
- řízení přístupu (A.9) – cílem je definovat opatření organizace na řízení přístupu k informacím, nastavení práv a odpovědností uživatelů v souvislosti s řízením přístupu k informačnímu systému a aplikacím;
- kryptografie (A.10) – stanovit opatření k využívání kryptografie k ochraně důvěrnosti, integrity a dostupnosti informací;
- fyzická bezpečnost (A.11) – stanovit opatření pro fyzickou bezpečnost objektu s cílem předcházení neautorizovaného fyzickému přístupu, poškození, krádeži či kompromitaci informací a aktiv související se zpravováním a ukládáním informací;
- zařízení (A.12) – opatření k zajištění správného a bezpečného provozu vybavení pro zpracování informací v souvislosti s ochranou proti malwaru, nastavení zálohování,

možnosti auditování, řízení softwarového, hardwarového a technického vybavení organizace;

- bezpečnost informací (A.13) – cílem opatření je zajistit bezpečnost informací v komunikačních sítích v rámci organizace a s externími subjekty;
- akvizice, vývoj a údržba (A.14) – implementovat bezpečnost informací do celého životního cyklu informačních systémů;
- dodavatelské vztahy (A.15) – zajistit ochranu aktiv a bezpečnost informací organizace v rámci vztahů s dodavateli;
- řízení incidentů bezpečnosti informací (A.16) – zajistit řízení a efektivní přístup ke zvládání incidentů bezpečnosti informací a zlepšování;
- aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací (A.17) – plánování, implementace a verifikace kontinuity bezpečnosti informací jako součást systému řízení kontinuity a dostupnosti vybavení pro zpracování informací v souvislosti s činností organizace;
- soulad s požadavky (A.18) – zajistit soulad s právními a smluvními požadavky v souladu s informační bezpečností.

Obrázek 5 PDCA



Zdroj: Novák (2011)

Životní cyklus modelu PDCA řízení informační bezpečnosti má 4 fáze (Novák, 2011):

PLAN – ustanovení ISMS – cílem této etapy je upřesnit rozsah a hranice, kterých se řízení bezpečnosti týká, stanovit jasné manažerské zadání a na základě ohodnocení rizik vybrat nezbytná bezpečnostní opatření;

DO – Zavádění a provoz ISMS – cílem je účelně a systematicky prosadit vybraná bezpečnostní opatření do chodu organizace;

CHECK – Monitorování a přezkoumání ISMS – hlavním cílem je zajištění zpětné vazby a pravidelného sledování a hodnocení úspěšných i nedostatečných stránek řízení bezpečnosti informací;

ACT – Údržba a zlepšování ISMS – cílem je realizace možností zlepšování systému řízení bezpečnosti informací ať už soustavným zlepšování systému nebo odstraňování zjištěných slabin a nedostatků;

Model PDCA je zachycen například v ISO/IEC 27002 kapitola 0.5. „Přihlédnutí k životnímu cyklu“ kde je rozšířen pojem informace a informační systém v souvislosti s informační bezpečností, které byly zavedeny v úvodu této kapitoly.

Informace má přirozený životní cyklus, od vytvoření a vzniku přes uchovávání, zpracovávání, použití a přenos až do jejího případného zničení nebo rozpadu. (ISO 27002, str.8)

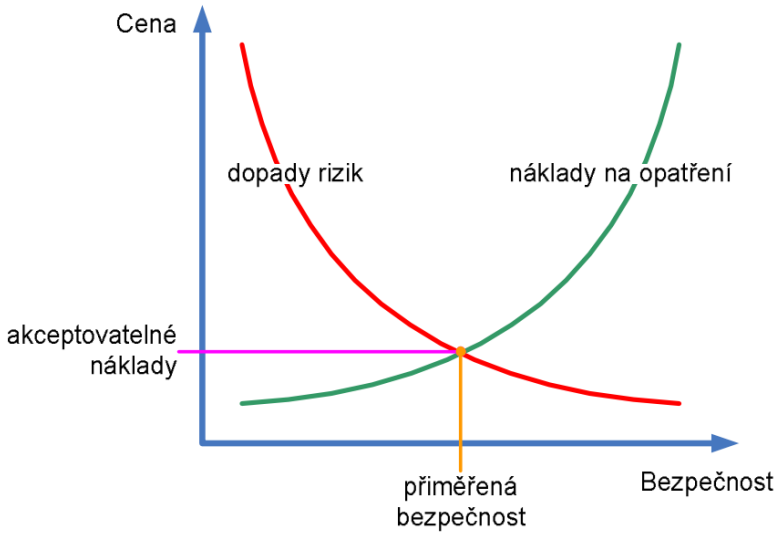
Informační systém má životní cyklus, ve kterém jsou IS koncipovány, specifikovány, navrženy, vyvinuty, testovány, implementovány, používány, udržovány, a nakonec odstaveny a odstraněny. (ISO 27002, str.8)

Bezpečnost informací by měla být vzata v úvahu v každé fázi. Vývoj nového a změna stávajícího sytému představuje pro organizaci příležitost aktualizovat a zlepšit opatření bezpečnosti. kdy organizace bere v úvahu aktuální incidenty, současná a očekávaná rizika bezpečnosti informací. (ISO 27002, str.8)

Podle Gogely (2011) pro vybudování ISMS v mikropodniku je důležité stanovit přiměřenou výši finančních prostředků. „Zajištění *bezpečnosti není hledáním dokonalého způsobu ochrany, ale aplikací takových opatření, která jsou přiměřená hodnotě předmětu ochrany (aktiv). Primárním předmětem ochrany jsou informace (nikoliv jejich nosiče nebo prostředky pro zpracování). Čím větší hodnotu pro nás informace mají, tím větší pozornost musíme věnovat bezpečnosti jejich nosičů. Každá organizace by si proto měla provádět alespoň základní hodnocení a kategorizaci svých informací a tomu přizpůsobit i způsob jejich*

ochrany. Velikost úsilí a investic do bezpečnosti musí odpovídat hodnotě aktiv a míře možných rizik. Změny v procesech organizace při zavádění ISMS a při aplikaci opatření v ICT systémech musí dostatečně redukovat dopady možných rizik za akceptovatelných nákladů.“(Gogela, 2011). Grafické znázornění vidíme na obrázku 6.

Obrázek 6 Přiměřená úroveň nákladů na ISMS



Zdroj: Gogela (2011)

3.2.4 Metodika ISMS ve zdravotnictví

V obecné praxi zdravotnictví jsou identifikovány informační systémy jako systémy kritické informační infrastruktury (KII) podle ZKB a VKB, kdy ve vyhlášce č. 573/2020 Sb., jsou určeni poskytovatelé zdravotní péče a to nemocnice, které jsou povinné zajistit opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti. Kybernetická bezpečnost není rozsahem zákona omezena (Mamrilla, 2021). V souvislostech pro **zavedení ISMS v mikropodniku** (ambulanci všeobecného praktického lékaře) **podle ISO/IEC 27001 nebrání skutečnosti**, kdy **provozovatel IS** v mikropodniku poskytovatele zdravotní péče **není povinen zajistit opatření dle ZKB**:

- informační systém v ambulanci praktického lékaře **není identifikován jako významný informační systém (VIS)** podle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 360/2020 Sb. §3;
- podle vyhlášky č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby, příloha 5. Zdravotnictví, informační systém v rozsahu poskytovatele ambulantní

zdravotní péče **není zařazen jako KII** mezi povinné provozovatele zajištění kybernetické bezpečnosti;

- mikropodnik v souvislosti s odbornou kvalifikací zaměstnanců (lékař, zdravotní sestra) **není schopen obsadit role podle ZKB** uvedených v §3 povinná osoba a §7 bezpečnostní role;
- **norma ISO/IEC 27001 poskytuje prostor** pro návrh implementace informační bezpečnosti v zájmovém prostředí mikropodniku.

Informační bezpečnost ve zdravotnictví je obecně řešena normou ČSN EN ISO 27799 Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002. Norma poskytuje rozšiřující výklad k upřesnění implementace požadavků ISO/IEC 27001 ve zdravotnictví. Pro vyhodnocení rizik v mikropodniku užívá zavedenou metodiku, která je uvedena v ISO/IEC 27005 řízení rizik v informační bezpečnosti.

Princip ISMS v ISO/IEC 27001 je podpořen:

- Zákonem č. 365/2000 Sb., „O informačních systémech veřejné správy“;
- Zákonem č. 181/2014 Sb., „O kybernetické bezpečnosti“;
- Vyhláškou č.82/2018 „Vyhláška o kybernetické bezpečnosti“;
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 „O ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů“;
- Zákonem č. 110/2019 Sb., „O zpracování osobních údajů“.

Tímto je definován možný přístup k implementaci ISMS v mikropodniku v ambulanci VPL. Rešerše legislativy k implementaci bezpečnosti IS je uvedena v kapitole 3.3 této práce.

V souvislosti s normami a zákony v roce 2019 Ministerstvo zdravotnictví České republiky (MZČR) publikovalo metodiku k realizaci informační bezpečnosti ISMS v oblasti kybernetické a informační bezpečnosti, která si klade za cíl oblast kybernetické a informační bezpečnosti zevrubně popsat a poskytnout odborné veřejnosti v sektoru zdravotnictví (nemocnic) nástroj pro alespoň základní řešení této komplexní problematiky. Jako taková si metodika klade za cíl poskytnout základní orientaci, vodítka a obecné principy a postupy s univerzální použitelností. Není detailním, všeobsažným nástrojem, ale jen základním vodítkem, které je třeba chápat jako výchozí bod pro realizaci prvních kroků a východisko

pro další kontinuální práci na zajišťování odborné ochrany citlivých informací a dat poskytovatelů zdravotních služeb. (MZČR, 2022)

V dokumentu "Metodický pokyn poskytovatelům zdravotních služeb k problematice kybernetické bezpečnosti v.2.0, MZČR stanovuje (Bezouška, 2019): „*Ministerstvo zdravotnictví doporučuje naplnění alespoň základních kroků popsaných v této metodice, tj. jmenování bezpečnostních rolí, inventarizace aktiv, provedení analýzy rizik a vytvoření základní dokumentace popisující problematiku informační a kybernetické bezpečnosti, základní procedury sloužící k ochraně informací a odpovědnosti za jejich dodržování. Míra detailu jednotlivých kroků by měla korespondovat s rozsahem a závažností informací, které daný poskytovatel zdravotních služeb spravuje.*"

Metodický pokyn byl zveřejněn ve Věstníku č. 7/2019 kapitola 2 a publikován na portále Národního centra elektronického zdravotnictví www.ncez.mzcr.cz.

3.2.5 Hodnocení bezpečnosti informací CIA

Podle vyhlášky č.82/2018, "Vyhláška o kybernetické bezpečnosti" je bezpečnost informací v informačním systému podniku charakterizována požadavkem na:

- důvěrnost – informace musí být chráněna podle předem daných pravidel, udržovaná v tajnosti;
- integritu – informace musí být kompletní a změnu může provádět pouze určený autorizovaný subjekt;
- dostupnost – informace musí být k dispozici daným autorizovaným subjektům.

V souvislosti s naplněním těchto požadavků ISO/IEC 27000 rozšiřuje možné podmínky pro bezpečnost informací na (ISO 27000, 2018):

- důvěrnost – vlastnost, že informace není dostupná nebo není zpřístupněna neoprávněným jednotlivcům, entitám nebo procesům (ISO/IEC 27000, str. 10);
- integrita – zajištění přesnosti a úplnosti (ISO/IEC 27000, str. 12);
- dostupnost – vlastnost vyjadřující přístupnost a použitelnost na žádost oprávněné entity (ISO/IEC 27000, str. 9);
- spolehlivost – soulad mezi zamýšleným chováním a výsledky (ISO/IEC 27000, str. 15);
- autenticita – vlastnost vyjadřující, že entita je tím, za co se prohlašuje (ISO/IEC 27000, str. 9);

- nepopiratelnost – schopnosti prokázat výskyt údajné události nebo činnosti entit, které ji vyvolaly (ISO/IEC 27000, str. 14).

Dále v diplomové práci je užito hodnocení bezpečnosti informací (aktiv organizace) obecně známé pod zkratkou CIA (C – Confidentiality, I – Integrity, A – Availibility), kdy hodnocení spolehlivosti, autenticity a nepopiratelnosti chápeme jako součást požadavků CIA.

3.3 Legislativa bezpečnosti IS v mikropodniku

Bezpečnosti informací v organizaci je dosaženo zavedením vhodných postupů a opatření, kdy základním cílem je nastavit pravidla pro nakládání s informacemi v organizaci. Informace je základní entitou, kterou po celý její životní cyklus PDCA (kap. 3.2.3), musíme chránit.

Legislativní základ bezpečnosti informací vychází z nezbytnosti, aby organizace identifikovala své požadavky na bezpečnost. V této části diplomové práce autor charakterizuje opatření k zavedení ISMS, kdy fakticky lze normou ISO/IEC 27001 definovat hlavní zdroje opatření pro kybernetickou bezpečnost obecnějším způsobem než ZKB.

„Podstatný rozdíl totiž je a vždycky byl v pojetí technických opatření, což má své logické opodstatnění – ISO 27001 je univerzální a to, jakým způsobem ji organizace implementují, je na nich samotných a jen při certifikačním auditu se dvoustupňově zjišťuje, jak byla příslušná doporučení aplikována. V prvním stupni se zjišťuje soulad dokumentace s normou, ve druhém soulad dokumentace s praktickým výkonem a vlastní implementací interních bezpečnostních předpisů. Oproti tomu ZoKB není obecným doporučením, ale závazným předpisem, který organizacím a firmám zajišťujícím životně důležité služby pro chod státu ukládá, jak mají příslušná aktiva chránit, lépe řečeno, jaká má být minimální ochrana, a tím zajistit základní funkce státu jak v oblasti kritické infrastruktury, tak i v případě významných systémů a nově i pro digitální služby. Pokud se organizace musí řídit ZoKB, má tento logicky přednost před ISO 27001, což je nutné vzít v potaz a strukturu dokumentace přizpůsobit zákonnému předpisu, až následně pak naplnit požadavky ISO 27001“ (Goll, 2023)

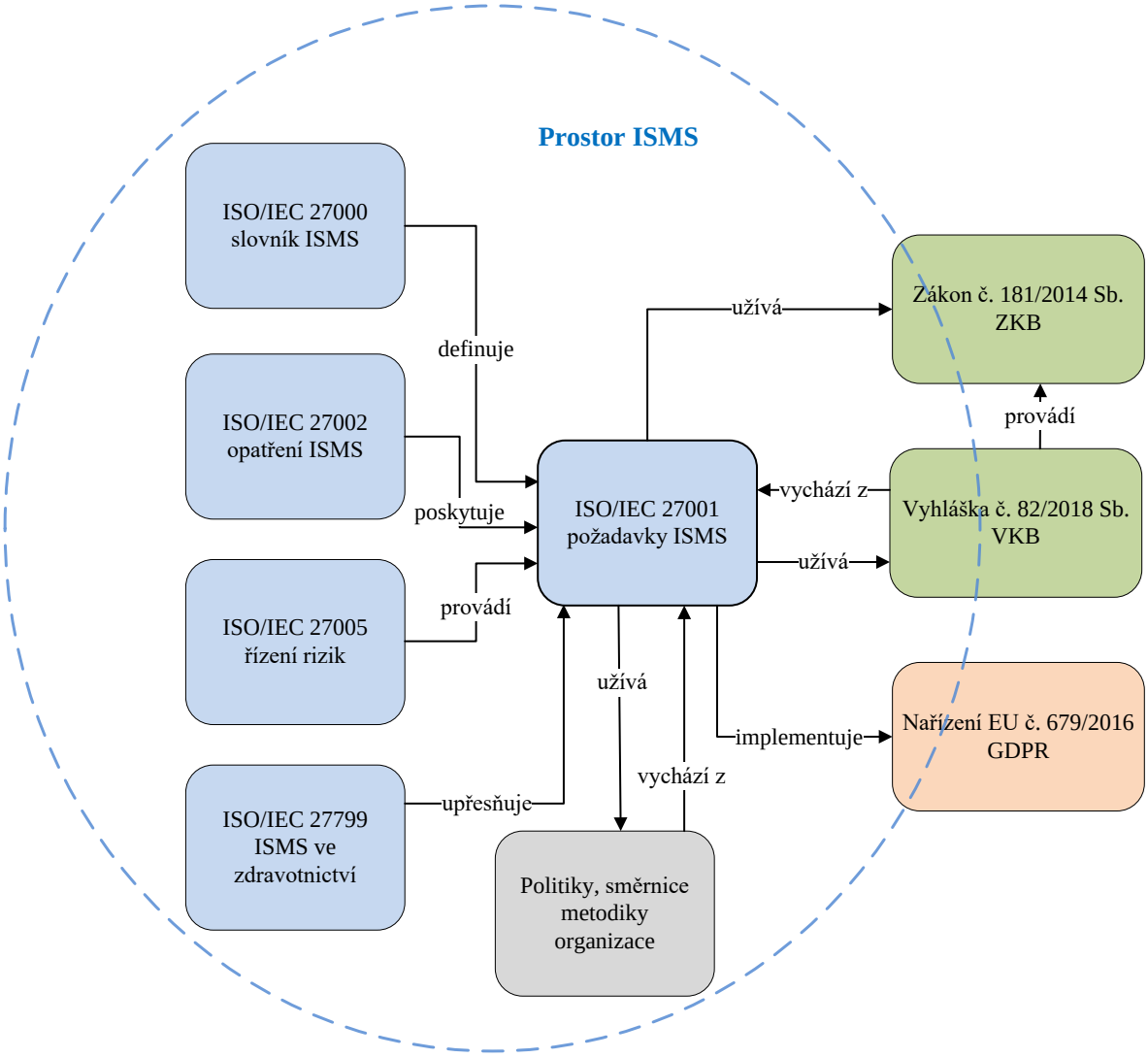
Hlavní zdroje požadavků na bezpečnost jsou (ISO 27002, 2014):

- posuzování rizik pro organizaci, s přihlédnutím k celkové podnikatelské strategii a cílům organizace. Prostřednictvím posuzování rizik jsou identifikovány hrozby vůči

aktivům, je vyhodnocena zranitelnost využitelná těmito hrozbami a pravděpodobnost výskytu a je proveden odhad potenciálního dopadu;

- právní, zákonné, předpisové a smluvní požadavky, které organizace, její obchodní partneři, smluvní strany a poskytovatelé služeb musí splnit, a jejich sociální a kulturní prostředí;
- soubor zásad, cílů a podnikatelských požadavků pro nakládání s informacemi, jejich zpracování, ukládání, sdělování/předávání a archivaci, které organizace vyvinula pro podporu své činnosti.

Obrázek 7 Prostor ISMS



Zdroj: vlastní zpracování

Základní legislativní rámec bezpečnosti IS v diplomové práci je stanoven oblastí systému řízení bezpečnosti informací na obrázku 7 v souvislosti se vstupními požadavky na bezpečnost. Autor vymezuje tyto požadavky do tří oblastí:

Oblast právní stanovená státem ve formě zákonů, vyhlášek a nařízení:

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (ZKB);
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (VKB);
- nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení GDPR).

Oblast norem, ISO standardů:

- ČSN EN ISO/IEC 27001 (369797) Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky;
- ČSN EN ISO/IEC 27002 (369798) Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací;
- ČSN EN ISO/IEC 27005 (369790) Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací;
- ČSN EN ISO 27799 (982021) Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002.

Oblast stanovená organizací:

- politika ISMS;
- prohlášení o aplikovatelnosti;
- politika bezpečnosti IS;
- plán kontinuity IS;
- směrnice uživatele.

Nastavení úrovně systému řízení informační bezpečnosti v dokumentaci souvisí s hodnocením informačních aktiv, jakou hodnotu pro organizaci tato aktiva představují v souvislosti s hodnocení jejich rizik, dopadů a plynoucích požadavků na jejich bezpečnost.

3.3.1 GDPR a minimální standardy zabezpečení osobních údajů

Co je osobní údaj?

Osobním údajem je každá informace o identifikované nebo identifikovatelné fyzické osobě (subjektu údajů). Identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor (jméno, číslo, síťový identifikátor) nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby. (Nezmar, 2017)

Základním dokumentem pro implementaci GDPR do prostředí zájmového mikropodniku je metodický pokyn MZČR a ÚZIS ČR „*Jak implementovat v ambulantní sféře nařízení Evropského parlamentu a rady 2016/679 o ochraně fyzických dokumentů v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES do resortu zdravotnictví“* z roku 2018.

Zpracováním osobních údajů chápeme *„Zpracováním je jakákoli operace nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoli jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení.“* (Nezmar, 2017)

V metodickém pokynu MZČR je k dosažení technických a organizačních opatření užito metodiky normy ISO/IEC 27001. *Technická opatření spočívají ve výběru vhodných technických prostředků ochrany osobních údajů Stejně jako v případě ostatních konkrétních implementačních kroků je možné vycházet z bezpečnostních norem ISO 27002 a je vhodné zavést systém řízení bezpečnostních opatření podle normy ISO 27001. Je tedy možné přiměřeně použít dokumentaci pro certifikaci, resp. aplikovat normy kvality ISO.* (Těšitelová a kol., 2018, str.28)

V souvislosti zpracování osobních údajů zvláště zdravotnické dokumentace, která obsahuje údaje o občanech společně s citlivými „důvěrnými“ informacemi o jejich zdravotním stavu, je součástí rámce výkonu poskytování zdravotních služeb. Rámec poskytování zdravotní péče je popsán v kapitole 4.

Poznámka: Informace a zdravotní dokumentace podléhající opatření GDPR jsou aktivy organizace. Tato aktiva podporují poskytování zdravotní péče. Potom zdravotní peče

organizace jako hlavní činnost mikropodniku je také aktivum (primární aktivum). V diplomové práci je aktivum vstupem pro proces analýzy, hodnocení a řízení rizik pro implementaci systému řízení bezpečnosti informací, tedy cílem je ochrana práv a svobod subjektů osobních údajů související s GDRP.

Správa a vedeni zdravotnické dokumentace vychází ze zákona č. 372/2011Sb., § 53–69 a prováděcí vyhlášky MZČR č. 98/2016 Sb., o zdravotnické dokumentaci. Organizace současně je povinna dodržovat zákon č. 101/2000 Sb., o ochraně osobních údajů.
Metodika od Těšitelové a kol. (2018) předkládá základní kroky k implementaci GDPR, které můžeme interpretovat a řešit opatřeními normy ISO/IEC 27002 (vlastní návrh):

- katalog osobních údajů a operací zpracování osobních údajů – A.8 Řízení aktiv;
- analýza připravenosti na GDPR s prokázáním souladu s GDPR – A.5 Politika bezpečnosti informací, A.18 Soulad s požadavky;
- agenda přístupů k osobním informacím – kap. A.9 Řízení přístupu;
- proškolení osob – A.7 Bezpečnost lidských zdrojů;
- technická a organizační opatření – A.10 Kryptografie, A.11 Fyzická bezpečnost a bezpečnost prostředí, A.12 Bezpečnost provozu, A.13 Bezpečnost komunikací;
- podepsaná smlouva s IT dodavateli – kap. A.15 Dodavatelské vztahy;
- srozumitelné informace pro pacienty, připravený informovaný souhlas – A.5 Politika bezpečnosti informací, A.6 Organizace bezpečnosti informací, A.8 Řízení aktiv, A.9 Řízení přístupu;
- pravidelná kontrola a aktualizace – A.5 Politika bezpečnosti, A.6 Organizace bezpečnosti informací, A.12 Bezpečnost provozu, A.17 Aspekty k řízení kontinuity činností organizace z hlediska bezpečnosti informací, A.18 Soulad s požadavky.

Výchozím bodem je zkoumání informačního toku (praktická část práce) a základní přehled pro vyhodnocení manipulace s informacemi v této diplomové práci je soupis činností uvedený v Těšitelová a kol. (2018, s. 15). Zpracovaný návrh toků informací a přehled manipulace (operací) s informacemi v ambulanci VPL autor uvádí v tabulce 2 v praktické části práce.

3.3.2 Zákony a vyhlášky

Tato kapitola obsahuje základní vysvětlení souvislosti ISMS v ZKB a VKB s normami ISO/IEC 27000. Zákon a vyhláška navazují na souvislosti s GDPR, kdy v další práci je teoretických znalostí využito pro analýzu rizik.

Zákon č. 181/2014 Sb.

Tento zákon upravuje práva a povinnosti osob, působnost a pravomoci orgánů veřejné moci. S ohledem na tuto skutečnost autor odůvodnil v kapitole 3.2.4 proč pro vytvoření metodiky bezpečnosti IS v mikropodniku místo primárního užití zákona o kybernetické bezpečnosti je použita norma ISO/IEC 27001. ZKB je velmi striktní zákonnou normou koncipovanou na užití ve velkých veřejných organizacích jako například je fakultní nemocnice, kdy taková organizace je schopna a povinna splnit povinnosti podle §3 jako správce a provozovatel významného informačního systému podle vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 360/2020 Sb. §3 určující kritéria. V souvislosti ZKB vychází z norem rodiny ISO/IEC 27000 což umožnuje využití prováděcí vyhlášky ZKB a to č.82/2018 Sb., přílohy č.1, 2, 3 k hodnocení aktiv podle důvěrnosti, integrity a dostupnosti.

Autor toto odvodil ze souvislostí v ZKB, VKB a vyjádření NBÚ ze dne 28.června 2013 v dokumentu „Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti a o změně souvisejících zákonů“, kde NBÚ uvádí *„Navíc je nutno zmínit, že bezpečnost jako taková je u části provozovatelů základních služeb a správců nebo provozovatelů informačních systémů základních služeb regulována i jinými právními předpisy. Zároveň je nutno zdůraznit, že nastavení bezpečnostních opatření vychází z principů mezinárodní normy ISO/IEC 27001, tj. z bezpečnostních pravidel, jimiž se již v současné době většina subjektů, které budou podléhat regulaci předmětného návrhu zákona, řídí.“* (NBÚ, 2013)

Vyhláška č. 82/2018 Sb.

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat je prováděcí vyhláškou ZKB. Stanovuje konkrétní opatření, která jsou pro organizace jednotlivými povinnými body k řešení kybernetické – informační bezpečnosti. V souvislosti s ISO/IEC 27001 je VKB rozdělena do 5 částí a příloh. Nejdůležitější jsou opatření v druhé části (VKB, 2018):

- Hlava I – organizační opatření (systém řízení bezpečnosti informací; řízení aktiv; řízení rizik; organizační bezpečnosti; bezpečnostní role; řízení dodavatelů; bezpečnost lidských zdrojů; řízení provozu a komunikací; řízení změn; řízení přístupu; akvizice, vývoj a údržba; zvládání kybernetických bezpečnostních událostí a incidentů; řízení kontinuity činnosti; audit kybernetické bezpečnosti).
- Hlava II – technická opatření (fyzická bezpečnost; bezpečnost komunikačních sítí; správa a ověřování identit; řízení přístupových oprávnění; ochrana před škodlivým kódem; zaznamenávání událostí; detekce kybernetických bezpečnostních událostí; sběr a vyhodnocování kybernetických bezpečnostních událostí; aplikační bezpečnost; kryptografické prostředky; zajišťování úrovně dostupnosti informací; průmyslové, řídící a obdobné specifické systémy; digitální služby).
- Hlava III – bezpečnostní politika a bezpečnostní dokumentace.

Pro další práci autor užívá přílohy VKB (2018):

- Příloha č. 1 hodnocení aktiv – jsou zde uvedeny hodnotící stupnice založené na čtyřech úrovních – nízká, střední, vysoká, kritická v souvislosti s hodnocením důvěrnosti, integrity a dostupnost. Tyto hodnotící stupnice jsou uvedeny v příloze 5 jsou využity dále v této práce při hodnocení aktiv a analýze rizik.
- Příloha č.2 hodnocení rizik – hodnota rizika je určena jako funkce součinu hodnot hodnocení hrozby, zranitelnosti a dopadu. ***R**iziko = **H**rozba x **Z**ranitelnost x **D**opad.* Hodnota dopadu je shodná s maximem hodnoty hodnocení aktiva dle CIA v příloze č.1 VKB. Stupnice hodnocení hrozeb, zranitelností a rizik jsou uvedeny v příloze 6 a budou užity v analýze rizik.
- Příloha č.3 Zranitelnost a hrozby – obsahuje vybrané kategorie hrozeb a zranitelností, které budou zdrojem pro analytickou část této práce.

3.3.3 Normy

ISO/IEC 27001

Tato norma specifikuje požadavky na ustanovení, implementování, udržování a neustálé zlepšování ISMS v rámci činnosti organizace. V souvislosti zahrnuje požadavky přizpůsobené potřebám organizace. Pro účely dokumentu této normy platí termíny a definice uvedené v ISO/IEC 27000. V příloze A (normativní) v ISO/IEC 27001 obsahuje cíle opatření a jednotlivá opatření propojená s ISO/IEC 27002, která jsou uvedena v kapitole

3.2.3 obecné zásady implementace ISMS této práce. Norma ISO/IEC 27001 je rozdělena do oblastí (ISO 27001, 2014):

- kontext organizace (kap.4) – porozumění organizaci, jejím potřebám a stanovení rozsahu systému řízení bezpečnosti informací;
- vůdčí role (kap.5) – stanovení politiky bezpečnosti informací, přiřazení odpovědností a pravomocí jednotlivým rolím v bezpečnosti informací, zajištění integrace požadavků a potřebných zdrojů pro ISMS;
- plánování (kap.6) – plánování opatření zaměřených na rizika a příležitosti, posouzení a ošetření rizik, stanovení a plánovaní dosažení cíle bezpečnosti informací;
- podpora (kap.7) – zajištění potřebných zdrojů pro celý PDCA ISMS, určení kompetencí jednotlivých osob v souvislosti ze zkušeností a školením, získání povědomí o politice bezpečnosti informací, nastavení procesu komunikace v organizaci a zavedení dokumentování informací;
- provozování (kap.8) – organizace plánuje, implementuje a řídí procesy s cílem splnění opatření v kapitole plánování (kap.6);
- hodnocení výkonosti (kap.9) – přezkoumávání, vyhodnocování výkonosti, vhodnosti a efektivnosti zavedeného ISMS v souvislosti prováděním interních auditů;
- zlepšování (kap.10) - reakce na neshodu v ISMS a vyhodnocení potřeby odstranění neshody formou implementace nápravného opatření s cílem neustálého zlepšování.

ISO/IEC 27002

Tato norma je určena pro organizace jako doporučení pro výběr opatření v rámci procesu implementace ISMS v souvislosti s ISO/IEC 27001. Obsahuje pokyny pro organizace veřejného a soukromého sektoru, které shromažďují, zpracovávají, uchovávají a předávají informace v elektronické, fyzické (analogové) a verbální formě. Norma nabízí k zavedení informační bezpečnosti vhodná opatření, která jsou specifikována do 14 oblastí, 35 hlavních kategorií bezpečnosti a 114 kontrol. Výčet oblastí opatření autor uvádí v kapitole 3.2.3 a jsou součástí „Prohlášení o aplikovatelnosti“ PoA uvedené v příloze 12. Norma specifikuje požadavky na bezpečnost:

- posouzení rizik s identifikovanými hrozbami aktiv, vyhodnocením zranitelnosti využitelnou hrozbami a možného dopadu na organizaci v souvislosti s její podnikatelskou strategie, činností a cíli, kdy využívá (ISO 27005, 2019);

- splnění právních, zákonných, předpisových a smluvních požadavků, které organizace, obchodní partneři, smluvní strany a poskytovatelé služeb musí plnit;
- soubor zásad, cílů a podnikatelských požadavků pro nakládání s informacemi, zpracovávání, ukládání, sdílení a archivaci nutných k činnosti organizace.

Pro implementaci ISMS organizace provede výběr z opatření uvedených v této normě na základě kritéria přijetí rizika, možnosti ošetření a přístupu k řízení na základě vlastního rozhodnutí v souvislosti s národní legislativou a nařízeními. Tato skutečnost je zachycena v „Prohlášení o aplikovatelnosti ISMS“ jak je uvedeno v kapitole 4.4.2, kde autor řeší rozsah systému řízení bezpečnosti informací.

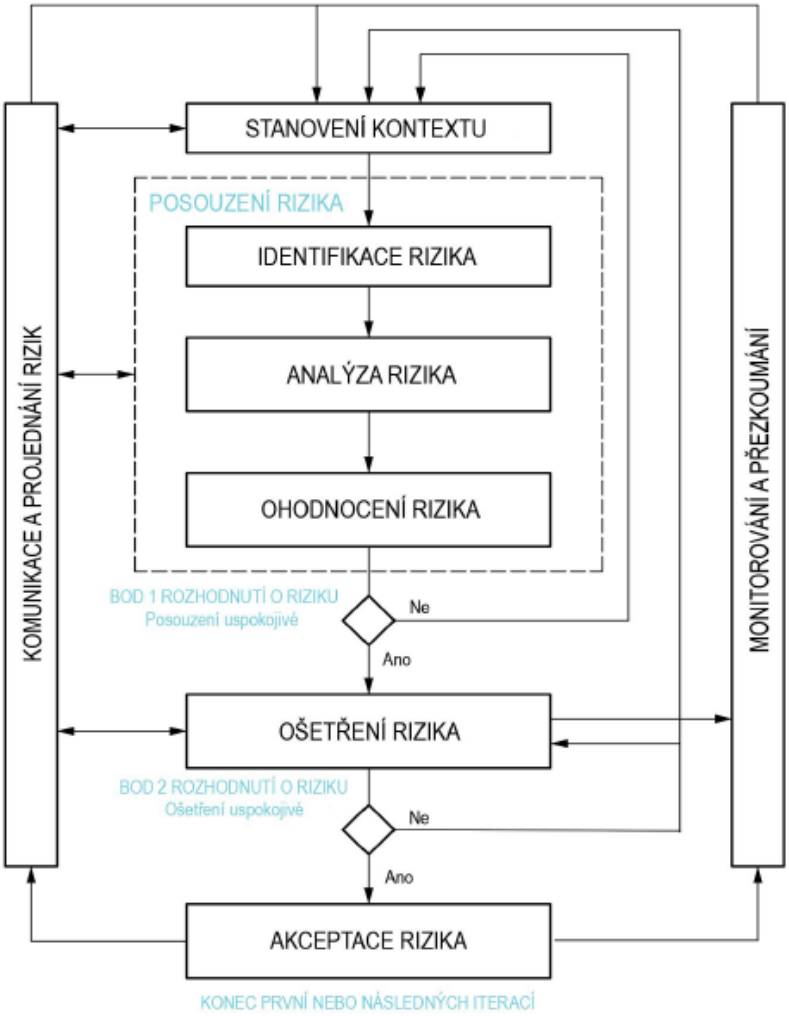
Podle kapitoly 0.4 „Vytváření vlastních směrnic normy“ (ISO 27002, 2014) je tato norma považována za výchozí bod pro vytváření směrnic pro informační bezpečnost, kdy ne všechna opatření musí být použita a současně mohou být zavedena opatření, která nejsou v této normě obsažena například v souvislosti s národní legislativou a nařízeními.

Podle ISO/IEC 27002 definuje příklad obsahu takové směrnice – politiky bezpečnosti IS:

- řízení přístupu (kap. 9);
- klasifikace informací a manipulace s informacemi (kap. 8.2);
- fyzickou bezpečnost a bezpečnost prostředí (kap. 11);
- opatření pro práci uživatelů:
    - přijatelné použití aktiv (kap. 8.1.3);
    - čistý stůl a čistý displej (kap. 11.2.9);
    - přenos informací (kap. 13.2.1);
    - mobilní zařízení a práce na dálku (kap. 6.2);
    - omezení týkající se instalací a použití software (kap. 12.6.2);
- zálohování (kap. 12.3);
- ochrana před malware (kap. 12.2);
- správa a řízení technických opatření (kap. 12.6);
- kryptografická opatření (kap. 10);
- bezpečnost komunikací (kap. 13);
- soukromí a ochrana osobních údajů (kap. 18.1.4);
- dodavatelské vztahy (kap. 15).

Bezpečnost informací v organizaci je součástí každé fáze životního cyklu informací a informačního systému, což jsou aktiva, která je nutno chránit.

Obrázek 8 Ilustrace procesu řízení rizik bezpečnosti informací



Zdroj: ISO 27005 (2019, s. 10)

ISO/IEC 27005

Poskytuje návod pro řízení rizik bezpečnosti informací, včetně doporučení v oblasti posuzování rizika, ošetření rizika, přijetí rizika, komunikace rizika, monitorování a přezkoumání rizika (ISO 27002, 2014, s. 7).Tato norma neposkytuje žádnou specifickou metodu pro řízení rizik bezpečnosti informací. Může být použita libovolná metoda pro analýzu rizik, která zakládá na metodě identifikace rizika, aktiv, hrozeb, zranitelností v souvislosti s touto normou. Pro pochopení této normy je nutné mít znalost konceptů, modelů, procesů a terminologie popsané v ISO/IEC 27001 a ISO/IEC 27002. Struktura normy obsahuje popis procesu řízení rizik bezpečnosti informací a jeho činností obecně

uvedený v ISO/IEC 27005, kapitole 6. Všechny činnosti řízení rizik bezpečnosti informací jsou rozděleny (ISO 27005, 2019):

- stanovení rámce (kap.7);
- posouzení rizika (kap.8);
- ošetření rizika (kap.9);
- akceptace rizika (kap.10);
- komunikace rizika (kap.11);
- monitorování a přezkoumání rizika (kap. 12);

Samotný proces analýzy rizik je zachycen na obrázku 8.

ISO IEC 27799

Tato norma poskytuje pokyny zdravotnickým organizacím a jiným správcům osobních zdravotních informací, jak nejlépe ochránit důvěrnost, integritu a dostupnost takových informací. Je založená na a rozšiřuje obecné pokyny stanovené v ISO/IEC 27002. Zaměřuje se na specifické potřeby řízení bezpečnosti informací v resortu zdravotnictví. Nenahrazuje výše uvedenou normu. Cílem této normy je:

- umožnit implementaci ISO/IEC 27002 a pomáhá zdravotnickým organizacím zajistit dodržování důvěrnosti a integrity dat v jejich péči, zachování dostupnosti kritických zdravotnických IS a prosazování odpovědnosti za zdravotnické informace;
- zavedení a udržování informační bezpečnosti se vztahuje na zdravotnické informace ve všech jejich souvislostech, bez ohledu na to, jakou má informace formu slovní a číselnou, zvukové nahrávky, kresby, video a lékařské snímky na prostředky k jejich ukládání tisk, zápis na papíře nebo elektronické uložení a na prostředky využívané k jejich přenosu ručně, faxem, přes počítačové sítě nebo poštou.

Informace, které mají být pomocí této normy (ISO 27799, 2019) chráněny:

- osobní zdravotní dokumentace;
- pseudonymizovaná data z osobní zdravotní informace;
- statistické a výzkumné údaje;
- lékařské znalosti, které nesouvisí se subjektem péče;
- údaje o odborných pracovnících ve zdravotnictví a zaměstnancích;
- informace týkající se veřejného dohledu nad zdravotnictvím;
- data auditních záznamů vytvářených zdravotnickými informačními systémy;

- systémová bezpečnostní data pro zdravotnické informační systémy, včetně dat řízení přístupu a dat souvisících s bezpečnostní konfigurací systému pro zdravotnické IS.

Cíle a opatření k informační bezpečnosti v ISO/IEC 27799 odkazují na související opatření v kapitolách 5 až 18 ISO/IEC 27002.

3.4 Porovnání vybraných bezpečnostních standardů

COBIT, ITIL a ISO 27001 jsou metody pro správu a řízení IT. Každá z těchto metod má své specifické zaměření a oblast na kterou se specializuje. Metody se svým zaměřením překrývají a organizace mohou využít všech tří metod k dosažení řízení IS (ITC) v našem případě správy informační bezpečnosti.

3.4.1 Porovnání ISMS, ITIL, COBIT

ISMS – je systém řízení informační bezpečnosti je založen na rodině norem ISO/IEC 27000. Metodika ISMS je popsána v kapitole 3.2 a legislativní rámec je objasněn na obrázku 7. Životní cyklus je založen na metodě PDCA – plánuj, dělej, kontroluj a jednej, zachycené na obrázku 5, kdy každá fáze obsahuje stanovené oblasti a aplikuje příslušná opatření informační bezpečnosti dle ISO/IEC 27002. Metodika navrhuje postupy k implementaci a opatření k nastavení informační bezpečnosti v organizaci. Norma nesvazuje, nenařizuje, ale doporučuje organizaci, libovolné velikosti, nastavit a řídit informační bezpečnost dle finančních, organizačních, technických či procesních možností organizace.

ITIL – IT Infrastructure Library podle společnosti Tayllorcox (2023) není to norma, ale agilní metodika, která obsahuje doporučení, nejlepší praktiky a zaměřuje se především na uživatele než na procesy.

ITIL 4 je charakterizován jako rámec pro řízení služeb, založený na „best practices“ obsahující 34 postupů rozdělených do tří kategorií (řídící postupy, postupy správa služeb a technického řízení) k dosažení cíle řízení IT. Základem je Service Value System – systém správy a řízení cílů hodnot služeb, obsahující (Danby, 2023):

- guiding principles – hlavní zásady;
- governance – správa;
- service value chain – hodnotový řetězec služeb;
- management practices – řídící postupy;
- continual improvement – kontinuální zlepšování.

Zaměřuje se na propojení IT služeb a obchodních zájmů organizace, *„podporuje plnění strategických a obchodních cílů organizace "* (Tayllorcox, 2023), kdy umožnuje postupné zavádění jednotlivých části řízení a správy IT služeb. Metodika je orientovaná na IT služby a obsahuje konceptuální referenční modely. Aktuální verze ITIL 4 podporuje komplexní přístup k řízení, kdy pokrývá 4 dimenze, které jsou klíčové pro každou organizaci, která chce systematicky řídit služby (Škrabánek, 2020):

- organizace a lidé;
- informace a technologie;
- partneři a dodavatelé;
- informační toky a procesy.

Klíčovými principy ITIL 4 pro úspěšné řízení IT služeb v organizaci jsou (Rance, 2019):

- soustředit se na hodnotu – nejen v kontextu financí, ale také zamýšlet se nad přínosem pro uživatele, zákazníky a dodavatele;
- začít tam, kde jste – není nutné začínat budovat IT od začátku, ale případně zachovat procesy které fungují dobře a jiné změnit, vylepšit nebo pozastavit;
- postupovat iterativně se zpětnou vazbou – tento princip zdůrazňuje důležitost zpětné vazby při postupném vylepšení;
- spolupracovat a podporovat viditelnost – podporuje týmovou práci a transparentnost;
- myslet a pracovat holisticky – tento princip zdůrazňuje důležitost uvažování o celkovém dopadu;
- udržet to jednoduché a praktické – zdůrazňuje důležitost jednoduchosti a praktičnosti při řešení problémů;
- optimalizovat a automatizovat – tento princip zdůrazňuje důležitost optimalizace a automatizace procesů tam, kde je to možné.

COBIT – Control Objectives for Information and related Technology dle Vitouše (2013) COBIT poskytuje komplexní rámec, který napomáhá firmám dosáhnout jejich cílů v rámci směrování, řízení IT a napomáhá vytvořit optimální hodnotu získanou pomocí přínosů při optimálním riziku a využití IT zdrojů.

COBIT 2019 je rámec pro správu a řízení podnikových informací a technologií zaměřený na celý podnik (ISACA, 2018):

- podnikové IT znamená veškerou technologii a zpracování informací, které podnik zavádí k dosažení svých cílů, bez ohledu na to, kde se to v podniku děje;

- podnikové IT není omezeno na IT oddělení organizace, ale rozhodně je zahrnuje.

Rámec COBIT 2019 poskytuje opatření, ukazatele, procesy a sbírku nejlepších postupů, které pomáhají společnostem optimalizovat řízení informačních technologií a vyvíjet řízení informačních technologií, které je pro organizaci vhodné. (Kusumaningrum, 2021)

COBIT 2019 podle Thomas (2021) v procesním modelu rozlišuje principy systému řízení (Governance System Principles) a rámcové zásady řízení (Governance framework principles). Definuje 40 cílů správy a řízení procesů rozdělených do 5 klíčových domén:

- vyhodnocovat, řídit a monitorovat (EDM);
- stanovit, plánovat a organizovat (APO);
- vytvořit, získat a implementovat (BAI);
- poskytovat, servis a podpora (DSS);
- monitorovat, hodnotit a vyhodnocovat (MEA).

Principy systému řízení COBIT 2019 jsou (Thomas, 2021):

- poskytovat hodnotu pro zúčastněné strany – vytvářet hodnotu z používání IT. Hodnota odráží rovnováhu mezi přínosy, riziky a zdroji, které jsou součástí systému řízení;
- holistický přístup – celostní přístup k systému řízení různých komponent systému;
- dynamický systém řízení – při změně strategie /technologie je nutné vzít v úvahu dopad těchto změn na systém;
- zásady správného řízení – rozlišovat mezi činnostmi v systému správy a systému řízení;
- přizpůsobovat se potřebám organizace – užívat množinu stanovených faktorů (parametrů) pro přizpůsobení a stanovení priorit zásad správného systému řízení;
- komplexní systém řízení – zaměřit se na IT, veškeré technologie a zpracování informací, které podnik používá k dosažení svých cílů.

Porovnání ISMS, ITIL, COBIT

Všechny tři rámce řízení informačních systémů jsou komplexní a robustní postupy, které zakládají na životním cyklu provozu IT, a to na podobnosti životního cyklu řízení PDCA (kap. 3.2.3). Každý z těchto rámců má specifické zaměření, všechny spolu souvisí a doplňují se. Některé způsoby, kterými jsou rámce propojeny, zahrnují (vlastní):

- COBIT nastavuje procesy pro správu IT služeb v celé společnosti. ITIL můžeme použít pro nastavení jednotlivých IT služeb v organizaci. Pro obecnou správu a řízení cílů

ITIL4 používá Service Value Systém a COBIT užívá COBIT Core. COBIT zakládá na období PDCA, kdežto ITIL4 proces opatření pomocí životního cyklu nevyžaduje;

- COBIT a ISO 27001 se zabývají řízením rizik provozovaných IT. COBIT poskytuje sadu kontrol a procesů pro řízení IT rizik, zatímco pomocí ISO 27001 navrhujeme rozsah opatření pro nastavení ISMS vedoucích k řízení rizik. Obě metodiky užívají obdoby životního cyklu PDCA;
- ITIL a ISO 27001 se zabývají řízením informačních služeb v organizaci, kdy ITIL poskytuje „best practices" postupy pro správu IT služeb, zatímco ISO 27001 doporučuje jednotlivá opatření k splnění cílů ISMS a zachování důvěrnosti, integrity a dostupnosti informačních aktiv.

Pro potřeby práce, rozšíření teoretických znalostí autora o řízení IT byla na základní teoretické úrovni analyzována metodika MBI.

3.4.2 MBI model

Pro řízení informatiky v mikropodniku můžeme využít vlastnosti a principy Management of Business Informatics neboli MBI. Model je vyvinutý na katedře informačních technologií, VŠE v Praze. Smyslem použití tohoto referenčního modelu je zobecnění řešení v řízení provozu a rozvoje informačních technologií nasazených v podniku. Model MBI byl navržen na základě několika průzkumů provedených mezi českými organizacemi v období let 2010–2012. (Voříšek, 2015)

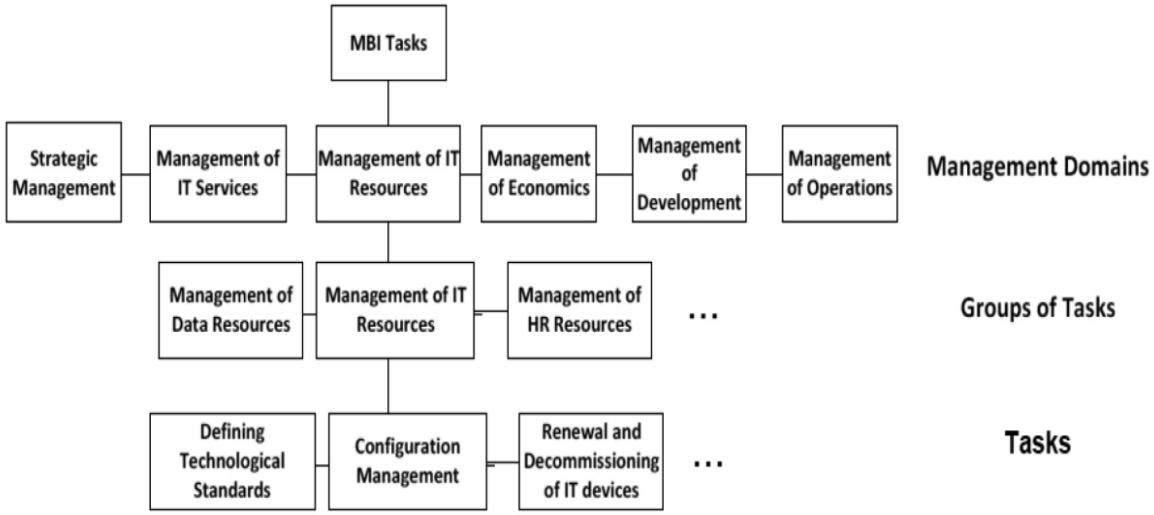
Základní charakteristika modelu

Cílem řešení modelu MBI je prezentovat doporučené postupy, řešení a dosud získané zkušenosti při poskytování informatických služeb a zvyšování jejich kvality a výkonosti. Pro řešení modelu MBI bylo definováno několik **klíčových principů** vycházejících jak z dostupných teoretických zdrojů, tak ze zkušeností praxi (Pour, 2012):

- model je schopen v prvé řadě respektovat podnikatelský záměr a strategii podniku;
- model je schopen rychle reagovat na měnící se potřeby a podmínky podnikové informatiky, jeho funkcionalita musí být snadno rozšiřitelná a aktualizovatelná;
- nasazení modelu v praxi musí nabídnout vysokou flexibilitu, může být implementován po jednotlivých částech (úlohách) a nikoli nutně jako celek;
- model má schopnost efektivního nasazení v různých velikostech a typech podniků respektující jejich zvláštnosti a specifické potřeby;

- metriky řízení jsou chápány jako systém ukazatelů provázaných na dimenze pro jejich identifikaci a analýzy;
- model nabízí různou úroveň podrobnosti (granulity) úloh řízení i sledovaných metrik odpovídající potřebám různých typů podniků a jejich disponibilním datovým zdrojům a musí pak umožnit efektivní customizaci celého řešení vzhledem ke konkrétnímu podnikovému prostředí;
- model zahrnuje u většiny svých komponent tzv. faktor úspěšnosti, které shrnují nejpodstatnější zkušenosti a doporučení z praxe.

Obrázek 9 Tříúrovňová hierarchie modelu MBI



Zdroj: Voříšek (2015)

Koncept modelu

Model MBI na obrázku 9 je organizován do hierarchii tří úrovní (Voříšek, 2015):

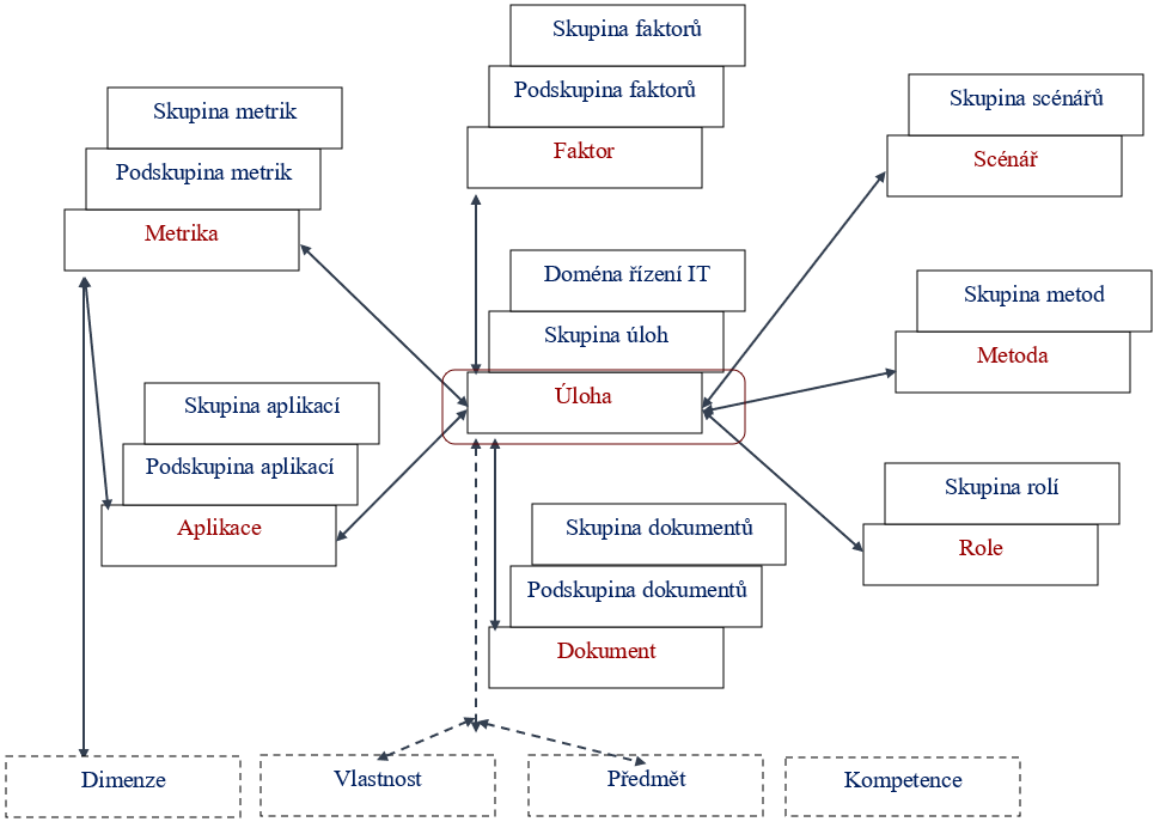
- správa domén;
- skupina úloh;
- úlohy.

Podle Buchalcevové (2016) a Voříška (2015) je hlavním prvkem úloha, která popisuje, jak postupovat při řešení konkrétního problému správy IT. Úloha popisuje, jak postupovat při řešení řízení specifického problému. Příkladem úloh jsou návrh na zajištění podnikového IT, implementace IT služby, aktivace služby, implementace bezpečnostního auditu atd. Rámec

MBI definuje velké množství úloh, které jsou seskupeny do skupin úloh, které tvoří domény řízení. Úlohy MBI naplňují zejména požadavek na flexibilitu při praktickém uplatňování modelu, neboť umožňují použít např. pouze jednu z úloh, nebo jejich různé vybrané kombinace.

Na obrázku 10 jsou vidět vazby objektu úloha s ostatními objekty. Každý z objektů má vlastní hierarchickou strukturu, mezi objekty jsou definovány vazby, např. Úloha – Metoda.

Obrázek 10 Přehled objektů a jejich hierarchická struktura a vazby



Zdroj: VŠE (2015)

Dalšími objekty jsou (Voříšek, 2015):

- **scénáře** – definují různé situace, problém, otázky v řízení informatiky v organizaci;
- **faktory** – definují existující prostředí informatiky a udržují MBI v souladu s vývojovými trendy, souhrnné vyjádření pro cíle, organizační, technické a další podmínky řízení IT;
- **role** – určují, jaké pracovní pozice se v podniku vyskytují, jak se podílejí na provozu a rozvoji informatiky v organizaci;

- **dokumenty** – jsou jakékoliv datová struktura, která představuje vstup nebo výstup úloh, může být v papírové, elektronické formě, databáze, report, tabulka, graf;
- **metriky** – slouží pro řízení kvality a výkonnosti informatiky, podnikových aktivit, kdy pro metriky jsou definovány analytické dimenze a související metriky;
- **aplikace** – analytické, plánovací a další aplikace a nástroje pro podporu řízení IT;
- **metody** – souhrnné označení pro manažerské, analytické, plánovací metodiky, metody, normy a rámce aplikovatelné v MBI;
- **dimenze –** slouží jako analytická hlediska při práci s jednotlivými metrikami;
- **vlastnosti –** definuje základní vlastnosti informatiky (např. flexibilita, výkonnost, aj.);
- **předměty –** představují hlavní předměty řízení (podnikové procesy, podniková pravidla, aj.);
- **kompetence –** představují přehled standardních kompetencí pracovníků podniku ve vztahu k informatice i podnikovému řízení.

Na základě pochopení teoretického základu MBI autor vybral úlohu, kterou se pokusil na teoretickém základu popsat v následující kapitole.

Příklad úlohy MBI

Úloha: Analýza a řízení rizik (vlastní zpracování).

Algoritmus analýzy rizik je znázorněn na obrázku 8 a datový model na obrázku 11.

Vstupy:

- normy řady ISO/IEC 27000;
- legislativní rámec organizace;
- bezpečnostní politika IS a role v ISMS;
- metodika hodnocení aktiv dle CIA a hodnocení hrozeb, zranitelností;
- metodika hodnocení rizik a dopadů na aktiva;
- kontext organizace a analýza činnosti organizace v prostředí ISMS;
- prohlášení o aplikovatelosti opatření ISO 27002;
- registr primární a podpůrných aktiv, znalost jejich souvislostí;
- registr hrozeb a zranitelnostní.

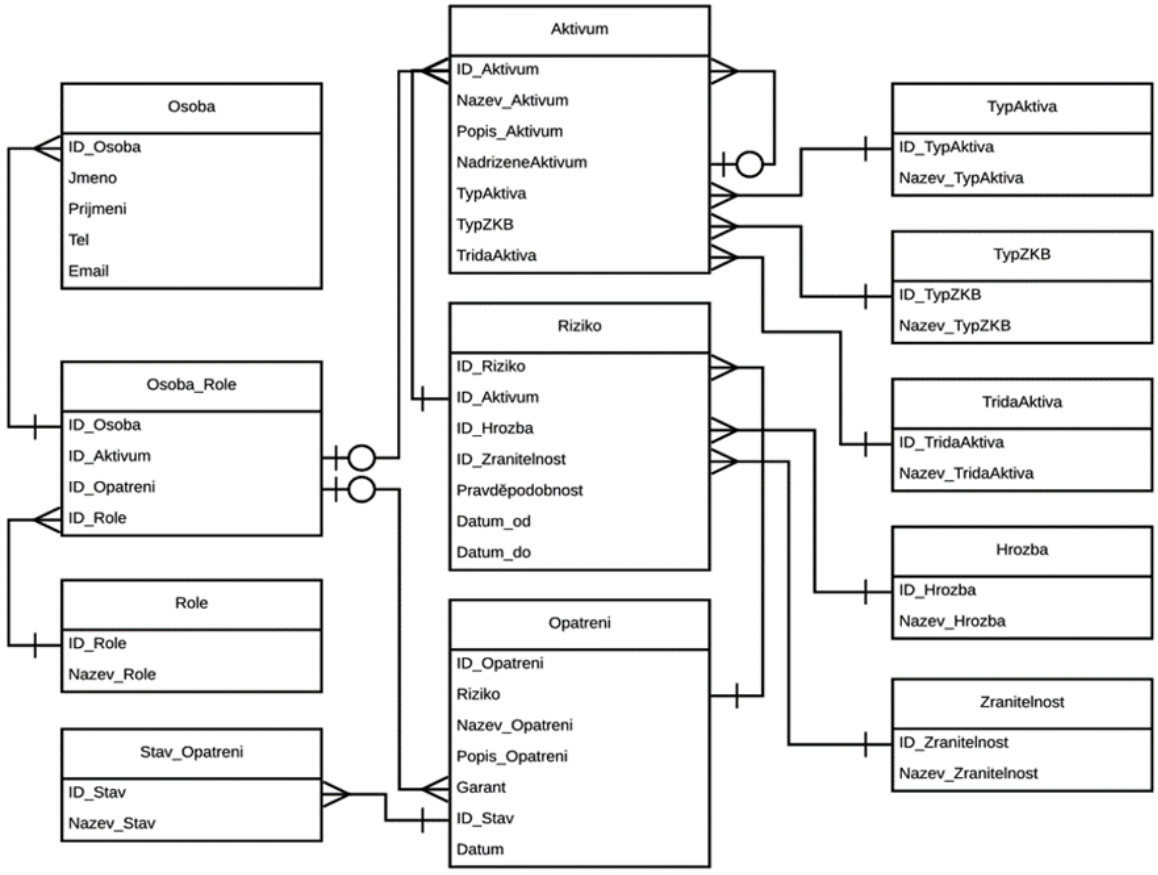
Klíčové aktivity:

- nalezení souvislostí mezi hrozbami a zranitelnostmi;
- identifikace možných rizik;
- matice rizika – výpočet rizika dopadů uskutečnitelné hrozby a souvisejí zranitelnosti, identifikace kritických a vysokých rizik;
- registr rizik, ohodnocení míry dopadu na aktiva;
- vytvoření plánu zvládání rizik – posouzení finanční, technické a organizační náročnosti zavedení opatření k akceptaci, snížení nebo modifikaci rizika působící na cíle informační bezpečnosti dle ISMS.

Výstup:

- identifikované rizika a hodnota dopadů na aktiva;
- plán zvládání rizik;
- zavedený systém řízení bezpečnosti informací.

Obrázek 11 Datový model pro analýzu rizik



Zdroj: Bezouška (2020)

4 Praktická část práce

4.1 Realizace ISMS ve zdravotnickém zařízení

Cílem realizace ISMS ve zdravotnickém zařízení je implementovat informační bezpečnost a získat kontrolu nad bezpečností informací v elektronické, tištěné a myšlenkové podobě zaměstnanců. Celý systém ISO/IEC 27000 je byrokratický způsob řízení, kdy základem je identifikace činností, procesů organizace, do kterých je nutné implementovat pravidla pro řízení informační bezpečnosti s praktickým dopadem na tyto činnosti a procesy.

Základní dokumenty pro zavedení ISMS do zdravotnického zařízení autor popisuje v kapitole 3, jsou především tyto:

- ISO/IEC 27001 – systémy řízení bezpečnosti informací – požadavky;
- ISO/IEC 27002 – soubor postupů pro opatření bezpečnosti informací;
- ISO/IEC 27005 – řízení rizik bezpečnosti informací identifikovaných aktiv;
- ISO/IEC 27799 – pokyny k implementace ISO/IEC 27002 ve zdravotnictví.

Ochrana a bezpečnost zdravotních informací souvisí s klasifikací informací dle ISO/IEC 27002, kap. 8.2.1 s upřesňujícím vysvětlením ISO/IEC 27799 „*Kromě tradiční klasifikace dat, na základě jejich citlivosti vůči prozrazení je také třeba klasifikovat kritičnosti informací, míru dostupnosti a integritu informací, které jsou důležité pro pokračující poskytování zdravotní péče. Časové faktory v klinických procesech často hrají klíčovou roli při určování požadavků na dostupnost osobních zdravotních informací. Klasifikace s ohledem na dostupnost, integritu a kritičnost (důvěrnost) musí být také aplikována na procesy, zařízení IT, software, umístnění a personál*.“ (ISO 27799, 2019)

Tento druh informací je považován za nejdůvěrnější ze všech druhů osobních informací, kdy ochrana (ISO 27799, 2019):

- důvěrnosti je nezbytná, pokud má být zajištěno soukromí subjektů péče;
- integrita zdravotnických informací musí být chráněna, aby bylo zajištěno bezpečí pacientů, a důležitou součástí této ochrany je zajištění auditovatelnosti celého životního cyklu informací;
- dostupnost zdravotnických informací je také rozhodující z hlediska efektivity výkonu zdravotní péče. Zdravotnické informační systémy musí splňovat zvláštní požadavky, aby byly akceschopné při přírodních katastrofách, selháních systému a při útocích typu odmítnutí služby.

Přístup k rozsahu dokumentace ISMS je v ISO/IEC 27001 rozsáhlý. Pro účely této diplomové práci byly vybrány klíčové dokumenty:

- **kontext organizace** (ISO/IEC 27001, kap.4) – je dokument zpracovaný v kapitole 4.3, který vystihuje hlavní činnosti, procesy, aktiva a informace v souvislosti s požadavkem na formulování informační bezpečnosti, kdy rozsah je definován v kapitole 3.2.2 jako interpretace přístupu k ISMS dle NÚKIB a základní rámec zdravotní péče je uveden v úvody kapitoly 4 jako právní rámec poskytování zdravotní péče dle obrázku 12;
- **prohlášení o aplikovatelnosti PoA** (ISO/IEC 27001, příloha A) – forma dokumentu specifikuje rozsah opatření ISMS organizace (rozsah normy A.5 – A.18 v kapitole 2.5), která mají rozhodující význam v souvskilpislosti s kontextem organizace a rámcem hlavní činnosti organizce je uvedeno v příloze 12 PoA s popisem vlastních navrhnutých opatření);
- **politika ISMS** (ISO/IEC 27001, kap.5) – obsahuje stanovené základy organizace informační bezpečnosti v mikropodniku, návrh je zpracován v příloze 13 této práce.

Na základě definovaného rámce činnosti organizace, kdy identifikujeme hlavní ekonomické činnosti a související aktiva organizace, zjistíme primární a podpůrná aktiva organizace. S tím souvisí dokumenty:

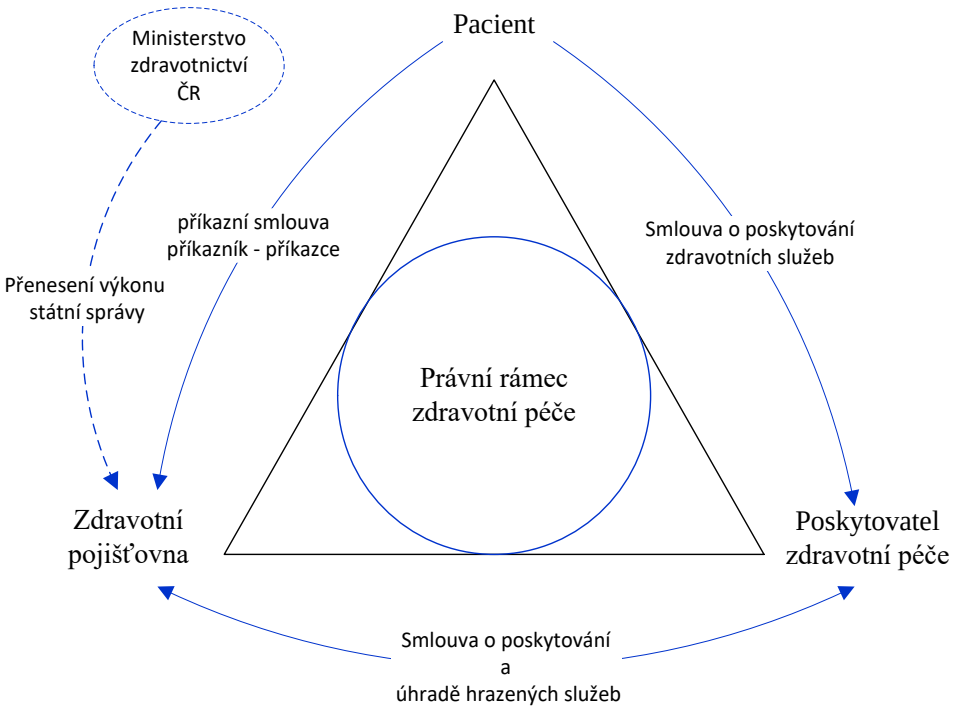
- rejstřík aktiv (primárních a podpůrných) a rejstřík hrozeb a zranitelností (kapitola 4);
- analýza rizik (podle ISO/IEC 27005 a příloha č. 1, 2, 3 VKB), matice rizik (příloha 10, příloha 11) s identifikovanými riziky v registru rizik (tabulka 10), s plánem zvládání rizik (registr rizik s terminem splnění opatření). Celý proces zavedení ISMS do mikropodniku probíhá postupně v jednotlivých krocích ISO/IEC 27002. Výsledkem je bezpečnostní politika organizace, která „*... v ideálním případě se bude přezkoumání této politiky řídit závěry zjištěnými při posuzování rizik organizace, ačkoliv politika samotná potřebuje pouze nastavit směr, stanovit zásady a označit další normy, kde se nacházejí (často se měnící) specifika.“* (ISO 27799, 2019, s. 19)

Podle kap. B.4.4 ISO/IEC 27799 základní princip realizace ISMS ve zdravotnictví je souvislost výše míry rizika s výší míry informační bezpečnosti, kdy snížení míry rizika znamená zvýšení míry bezpečnosti IS a naopak.

4.2 Rámec hlavního aktiva organizace

Pro zahájení analýzy ISMS v ambulanci praktického lékaře je vhodné stanovit rámec výkonu zdravotní péče, která je hlavní podnikatelskou činností organizace. Zdravotní péče je stanovena zákonem č. 372/2011 Sb., Zákon o zdravotních službách a podmínkách jejich poskytování. Zdravotní péče je podle §5 Druhy zdravotní péče definována podle naléhavosti její ho poskytnutí – neodkladná, akutní, nezbytná a plánovaná. Druhy zdravotní péče podle účelu jejího poskytnutí jsou – preventivní péče, diagnostická péče, dispenzární péče, léčebná péče, posudková péče, ošetřovatelská péče, paliativní péče. Podle §6 Formy zdravotní péče jsou pro výkon činnosti ambulance praktického lékaře stanoveny formy ambulantní péče a péče poskytovaná ve vlastním sociálním prostředí pacienta (návštěvní služba).
Ambulantní péče (podle §7) je zdravotní péčí, při níž se nevyžaduje hospitalizace pacienta a je poskytována jako primární ambulantní péče, jejímž účelem je poskytování preventivní, diagnostické, léčebné a posudkové péče a konzultací, dále koordinace a návaznost poskytovaných zdravotních služeb jinými poskytovateli. Tuto zdravotní péči pacientovi poskytuje registrující poskytovatel.

Obrázek 12 Právní rámec poskytování zdravotní péče



Zdroj: vlastní zpracování

Významnou částí oblasti informační bezpečnosti jsou osobní a zdravotnické informace osoby. Pacient do procesu ambulantní zdravotní péče vstupuje s požadavkem na poskytnutí zdravotních služeb včetně své registrace u příslušného poskytovatele zdravotní péče, kdy pacient uzavírá smlouvu o poskytování zdravotních služeb s poskytovatelem zdravotní péče (zájmový mikropodnik). Poskytovatel zdravotní péče má zpravidla uzavřenou smlouvu o poskytování a úhradě hrazených služeb se zdravotní pojišťovnou v rámci tzv. úhradové vyhlášky, kdy MZČR stanovuje hodnotu bodu, výše úhrad za hrazené služby a regulační omezení pro rok 2023 vyhláškou č.315/2022 Sb. Zdravotní pojišťovna na základě příkazní smlouvy mezi pacientem a zdravotní pojišťovnou pacientovi zabezpečuje smluvního praktického lékaře a hradí provedené zdravotní výkony pacientovi lékařem, a to poskytovateli zdravotní péče. Na obrázku 12 je znázorněn právní rámec zdravotní péče s přenesením výkonu státní správy v oblasti veřejného zdravotního pojištění.

4.3 Kontext modelu zdravotnického zařízení

Pro porozumění organizaci dle ISO/IEC 27001(2014) kap. 4 musí organizace určit externí a interní aspekty, které jsou významné pro její záměry a které ovlivňují její schopnost dosáhnout zamýšleného výstupu v souvislosti se systémem řízení bezpečnosti informací. Dle ISO/IEC 27005 (příloha A) s tímto souvisí definování rozsahu a mezních hodnot procesu řízení rizik bezpečnosti informací a to:

- analýza organizace;
- seznam omezení ovlivňující organizaci;
- seznam omezení ovlivňující rozsah působnosti.

Analýza těchto záležitostí má tři účely (ISO 27003, 2018, s. 8):

- porozumění kontextu, aby bylo možné rozhodnout o rozsahu ISMS;
- analýza kontextu s cílem určit rizika a příležitosti;
- zajistit, aby byl ISMS přizpůsoben měnícím se vnějším a vnitřním záležitostem.

Základní informace organizace

Předmět podnikání:

Organizace poskytuje zdravotní služby v rozsahu specializace kód 001 tzn. ambulance všeobecného praktického lékaře. Právní forma je s.r.o., počet zaměstnanců 4.

Výkon činnosti je v souladu s legislativou:

- zákonem č. 372/2011 Sb., Zákon o zdravotních službách a podmínkách jejich poskytování;
- vyhláškou č. 92/2012 Sb., o požadavcích na minimální technické a věcné vybavení zdravotnických zařízení a kontaktních pracovišť domácí péče;
- vyhláškou č. 98/2012 Sb., o zdravotnické dokumentaci;
- vyhláškou č. 70/2012 Sb. o preventivních prohlídkách;
- zákonem č. 373/ 2011 Sb. o specifických zdravotních službách;
- zákonem č. 101/2000 Sb., o ochraně osobních údajů;
- nařízení Evropského Parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Interní dokumenty organizace:

- politika ISMS (není zpracována);
- organizační řád organizace;
- směrnice bezpečnosti IS (není zpracována);
- prohlášení GDPR a o ochraně osobních údajů pacienta (obecná směrnice bez analýzy);
- směrnice BOZP na pracovišti;
- operační postup pro nakládání s léčivy.

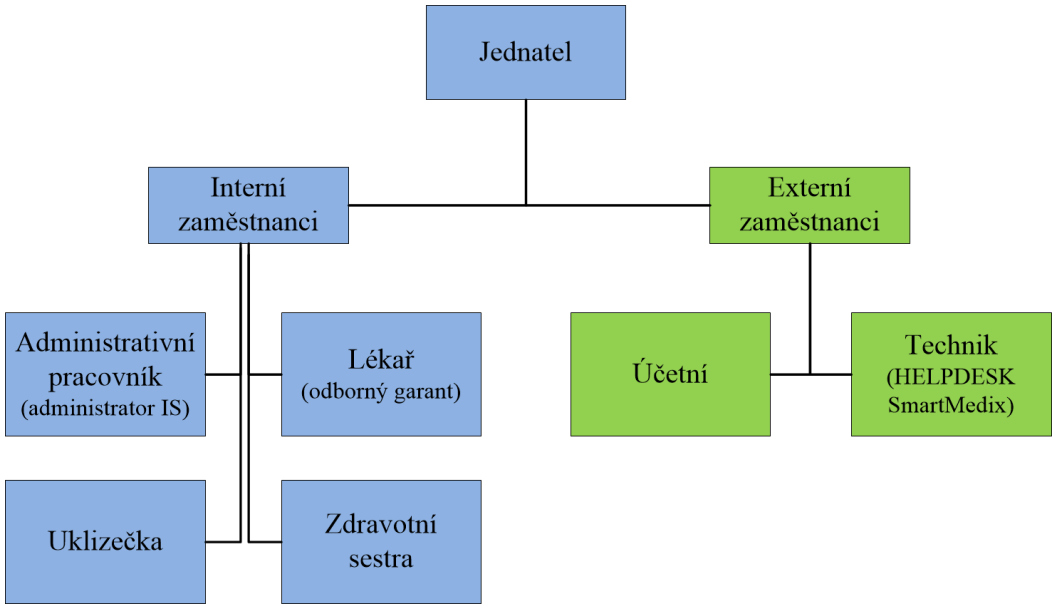
Smlouvy s obchodními partnery:

- smlouvy se zdravotními pojišťovnami a souvisejícími dodatky;
- smlouvy s dodavateli diagnostických zdravotnických zařízení;
- smlouvy s dodavateli zdravotnického materiálu;
- smlouvy o likvidaci odpadů (infekční a komunální odpad);
- smlouvy se zaměstnavateli, kterým je poskytována služba závodního lékaře;
- smlouvy s poskytovateli telekomunikačních služeb a internetu;
- smlouva s dodavatelem aplikačního SW SMARTMEDIX.

Organizační struktura

Organizace využívá interní a externí zaměstnance. Majitelem organizace je jednatelka společnosti. Organizační struktura mikropodniku je uvedena na obrázku 13.

Obrázek 13 Organizační struktura mikropodniku



Zdroj: vlastní zpracování

Účastníci kontextu organizace a jejich požadavky

Poskytovatel zdravotní péče (jednatel s.r.o.) organizaci řídí a předpokládá:

- lékař a zdravotní sestra budou poskytovat zdravotní péči podle platné legislativy ČR;
- podnikání při výkonu zdravotní péče povede k ekonomickému zisku;
- kontinuitu zachování důvěrnosti, integrity a dostupnosti zdravotní péče, dokumentace, účtování provedených zdravotních výkonů a provoz aplikačního IS;

Pacient ze zdravotního pojištění má nárok na:

- zdravotní péče bude poskytnuta minimálně z rozsahu zdravotního pojištění;
- diagnostiku a léčbu bude provádět atestovaný lékař a specialisté ve zdravotnictví s využitím schválených postupů a diagnostický přístrojů;
- informace o zdravotním stavu a osobní údaje jsou zpracovávány na základě platného souhlasu GDPR a principu CIA.

Zdravotní pojišťovna plní a vyžaduje:

- změny provozu ambulance, zaměstnanců a žádostí o nasmlouvání nových výkonů budou formou smluvní dodatků ze strany jednatele verifikovány cestou portálu zdravotní pojišťovny nebo datovou schránkou;

- zdravotní péče a provedené zdravotní výkony budou účtovány dle vyhlášky č. 134/1998 Sb., seznam zdravotních výkonů s bodovými hodnotami.

Dodavatelé a odběratelé plní a vyžadují:

- dodržování uzavřených smluv a souvisejících povinnosti např. pro poskytování pracovních lékařských prohlídek, posudků, kontroly pracovního prostředí zaměstnanců odběru očkovacích látek, nákupu diagnostických přístrojů či zdravotnického materiálu;
- nedodržování smluvních vztahů související např. s finančním plněním, dodávkami, poskytováním služeb v oblasti IT a správy IS, zajištěním personálu nebo porušením bezpečnosti práce, je nutné vždy smluvně ošetřit, aby nedošlo k přímému či nepřímému dopadu na činnost organizace;
- zpracování informací a osobních údajů, které souvisejí s dodavateli / odběrateli, podléhá zpracování a ochraně osobních údajů (GDPR).

Ostatní zainteresované strany:

- externí poskytovatelé zdravotní péče;
- Česká správa sociálního zabezpečení;
- veřejně spolky a organizace sociální péče;
- orgány, úřady a instituce statní správy, Policie ČR a soudy České republiky.

ISMS a související rizika

Příkladem rizik je vznik nového poskytovatele ambulantní zdravotní péče, kdy dochází k odregistrování stávajících pacientům k novému poskytovateli což vede k snížení kapitační platby, tedy snížení zisku organizace. Současně ambulance potřebuje v okolí jinou ambulanci pro zabezpečení zastupovaní v období dovolené a nemoci lékaře, aby byla zabezpečena dostupnost zdravotní péče.

Významná rizika:

- rizika ISMS obecně:
    - důvěrnost – informace je uchovávána a sdělena pouze oprávněné osobě;
    - integrita – informace není bez vědomí oprávněné osoby změněna;
    - dostupnost – informace je přístupná po identifikaci oprávněné osoby.
- rizika zpracování a ochrany osobních údajů (GDPR):
    - udržování principu odpovědnosti správce a vedení záznamů o zpracování osobních údajů – v organizaci výkon správce zabezpečuje jednatel;

- dodržování bezpečnostních opatření zpracovateli osobních údajů – určenými zpracovateli jsou lékař a zdravotní sestra;
- vyžadování a udržovaní informovaného souhlasu GDPR od pacientů;

- rizika bezpečnosti práce:
  - nedodržení pracovních postupů;
  - neprovedení revizí elektrických spotřebičů a diagnostických přístrojů;
  - nedodržení pravidelného školení BOZP, PO, ekologie, infekční odpad;
  - nedodržení dezinfekčního plánu.
- finanční rizika:
  - zamítnutí proplacení výkonů zdravotní péče zdravotní pojišťovanou;
  - chybné ohodnocení výkonu zdravotní péče nebo chyby v měsíčních výkazech účtování kapitačních plateb a výkonů zdravotní pojišťovně;
  - porušení pravidel neoprávněného předepisování léčiv ze strany lékaře, vymáhání ze strany zdravotní pojišťovny;
  - pozdní reakce pojišťovny k nasmlouvání výkonů dle úhradové vyhlášky č. 315/2022 Sb.;
- ostatní rizika:
  - organizační rizika v souvislosti s nedostupností odborného personálu pro výkon všeobecného lékaře a sestry;
  - technická rizika – nedostupnost informačního systému a komunikačních služeb, dodávek energií;
  - narušení fyzického objektu organizace – krádež, požár, přírodní živel.

4.4 Analýza vstupního stavu ISMS mikropodniku

Pro potřeby této práce je vhodným nástrojem základní audit pro vstupní hodnocení ISMS v mikropodniku pomocí SWOT analýzy a následným hodnocením porovnání analýzou GAP aktuálního stavu bezpečnosti informací v mikropodniku, které jsou provedeny na základě rozhovoru a pozorování.

SWOT analýza dle metodiky ISO/IEC 27001 není povinná, ale pro potřeby této práce vhodná. GAP analýza je užita pro porovnání aktuálního stavu opatření „kde se nacházíme“ a cílového stavu „kam se chceme dostat“. Výsledkem analýzy jsou identifikovaná opatření k dosažení cílového stavu PoA (příloha 12) ISMS mikropodniku.

4.4.1 SWOT analýza

SWOT analýza je analytický nástroj, pomocí kterého byla provedena analýza činnosti organizace v souvislosti s ISMS. Na základě provedené analýzy lze vyhodnotit počáteční stav systému řízení bezpečnosti informací. Analýza byla provedena na základě pozorování a provedeného rozhovoru č.1 (kap. 2) s jednatelem organizace a správcem informačního systému. Na základě pozorování a rozhovoru byl identifikován stav plnění jednotlivých opatření A.5 - A.18. Jednotlivé části SWOT analýzy jsou uvedeny v tabulce 1:

- silné stránky – identifikují již užívaná opatření, která odpovídají minimálnímu rozsahu implementace bezpečnosti informací v interním prostředí;
- slabé stránky – charakterizují nedostatky neboli interní zranitelnosti v podobě nedostatečných technických, objektových, personálních, komunikačních nebo informačních opatření, která je nutné aktualizovat a zlepšit;
- příležitosti – identifikují opatření v informační bezpečnosti související s činnostmi organizace směřující ke zlepšení bezpečnosti informací díky implementaci ISMS a zvýší standardu pro opatření zpracování osobních údajů GDPR, která mohou být konkurenční výhodou či garancí zavedeného ISMS pro pacienty a partnery;
- hrozby – jsou identifikovány v souvislosti s činností organizace definovaného rámce podnikání, kdy hrozí narušení důvěrnosti, integrity a dostupnosti primárního aktiva především z důvodu nezavedených opatření ISMS, která mají vliv na externí faktory ovlivňující kontinuitu poskytování zdravotní péče.

Hrozby souvisí s rizikem zneužití zranitelnosti, porušení CIA na primárních aktivech, které v ambulanci VPL souvisí s posykováním zdravotní péče a ochranou aktiv. Seznam identifikovaný hrozeb Hx pro analýzu rizik je uveden v kapitole 4.8.1.

Slabé stránky jsou zdrojem k identifikaci zranitelností organizace (příklady jsou uvedeny v ISO/IEC 27003 příloha D.1). Dále v práci jsou použity vlastní identifikované zranitelnosti Zx uvedené v kapitole 4.8.2.

Poznámka: v analýze rizik s hrozbami Hx a zranitelnostmi Zx autor dále pracuje za předpokladu neaplikovaných opatření ISMS dle PoA.

Tabulka 1 SWOT analýza

Silné	Slabé
A.6.1 Interní organizace	A.5 Politiky bezpečnosti informací
A.7.1 Před vznikem pracovního vztahu	A.6.2 Mobilní zařízení a práce na dálku
A.9.1 Požadavky organizace na řízení přístupu	A.7.2 Během pracovního vztahu
A.9.2 Řízení přístupu uživatelů	A.8.1 Odpovědnost a aktiva
A.11.1 Bezpečné oblasti	A.10.1 Kryptografické opatření
A.12.2 Ochrana proti malware	A.12.4 Zaznamenání logů a monitorování
A.12.6 Řízení technických zranitelností	A.12.5 Správa provozního software
A.15 Dodavatelské vztahy	A.13.1 Správa bezpečnosti sítí
A.18.1 Soulad s právními a smluvními požadavky	A.17.2 Redundance
Příležitosti	**Hrozby**
A.8.2 Klasifikace informací	A.8.3 Manipulace s médii
A.9.3 Odpovědnosti uživatelů	A.12.1 Provozní postupy a odpovědnosti
A.9.4 Řízení přístupu k systému a aplikacím	A.12.3 Zálohování
A.11.2 Zařízení	A.16 Řízení incidentů bezpečnosti
A.12.7 Hlediska auditu informačních systémů	A.17.1 Kontinuita informační bezpečnosti
A.13.2 Přenos informací	
A 14.1 Bezpečnostní požadavky IS	
A.18.2 Přezkoumání informační bezpečnosti	

Zdroj: vlastní zpracování

4.4.2 GAP analýza

S předcházející SWOT analýzy autor identifikoval kapitoly bezpečnostních opatření, které jsou užita pro aktuální nastavení bezpečnosti informací. Pro hodnocení aktuálního stavu pomocí analýzy GAP, porovnání stávajícího stavu nastavených pravidel bezpečnosti informací a cílového stavu ISMS PoA, je zpracováno hodnocení ve sloupci *počáteční stav* tabulky PoA v příloze 12.

Pro hodnocení úrovně nastavení opatření byla zvolena klasifikace:

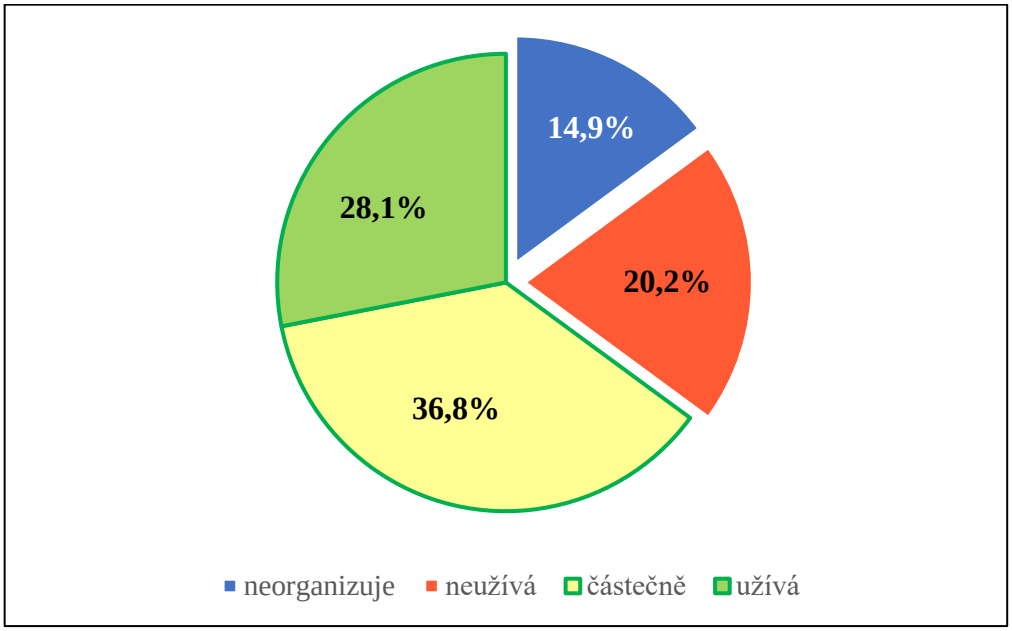
- užívá – opatření jsou aplikována s minimální potřebou adaptace na cílový stav;
- částečné – opatření jsou parciálně splněna a je nutné rozšíření opatření na cílový stav;

- neužívá – opatření nejsou splněna nebo chybí dokumentace, která dané opatření řídí;
- neorganizuje – opatření jsou outsourcing nebo nerelevantní.

Vyhodnocení počátečního stavu celkového užívání opatření ISMS dle grafu 1 je:

- z 28 % opatření jsou zavedena;
- z 20 % opatření nejsou zavedena vůbec;
- z 15% opatření organizace neplánuje, nebo jsou řešena jako outsourcing;
- z 65 % opatření klasifikovaná jako „užívá“ nebo užívá „částečně“ organizace řešila při implementaci nastavení minimálního rozsahu ochrany osobních údajů GDPR.

Graf 1 Počáteční stav plnění opatření ISMS



Zdroj: vlastní zpracování

Vyhodnocení rozdílu užívání opatření ve sloupci *počáteční stav* proti cílovému stavu aplikovatelných opatření dle PoA pomocí GAP analýzy (graf 2) autor analyzoval (vlastní):

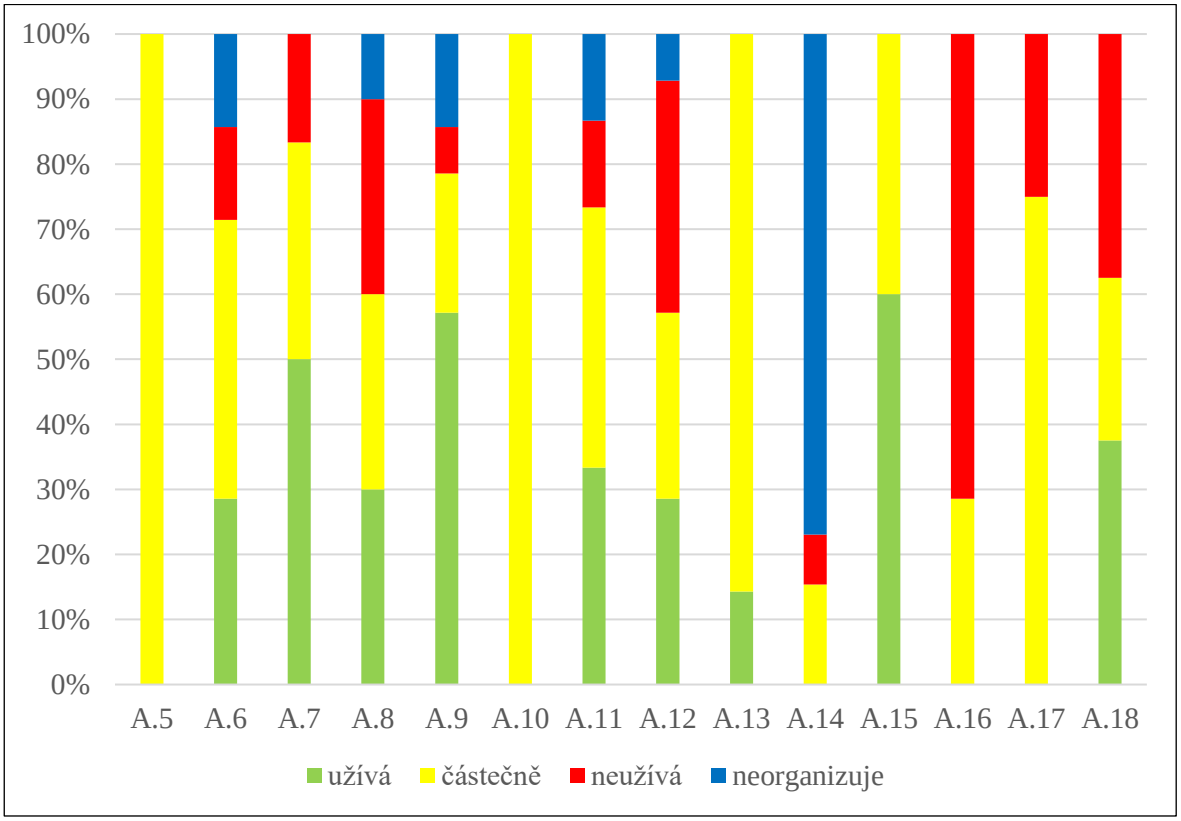
- organizace má zavedená základní opatření ochrany a manipulace osobních údajů GDPR. Podle PoA nejsou vytvořeny a schváleny politiky bezpečnosti informací. Hodnocení plnění opatření kapitoly **A.5 politiky bezpečnosti informací** (2 opatření / 2 částečně) - užívá částečně. Pro splnění opatření je nutné vytvořit politiku ISMS, politiku bezpečnosti IS a prohlášení o aplikovatelnosti PoA;
- opatření kapitoly **A.12 bezpečnost provozu** (14 opatření / 4 užívá / 4 částečně / 5 neužívá / 1 neorganizuje) jsou v organizaci zavedena z 29 %. Tato opatření souvisí

především se zavedenou minimální politikou GDPR. Opatření A.12.1.4 není organizováno. Pro splnění je nutné dokumentovat proces hlavní činnosti organizace (poskytování zdravotní péče) a provozní postupy, zálohování, zaznamenávání logů a provádění auditu. Ostatní opatření je nutné aktualizovat a zlepšit.

- autor zjistil, že opatření kapitoly **A.16 řízení incidentů bezpečnosti** (7 opatření / 2 částečně / 5 neužívá) organizace neužívá a není aplikováno řízení zvládání incidentů bezpečnosti informací. Cílem je provést analýzu rizik, identifikovat rizika a nastavit opatření ke snížení rizik. Je nutné stanovit plán kontinuity IS (ISMS).

Stav plnění opatření ostatních kapitol PoA lze odvodit z grafu 2 GAP analýzy a návrhu vlastník opatření k splnění cíle v příloze 12.

Graf 2 GAP analýza – porovnání počátečního stav ISMS k cílovému stavu PoA



Zdroj: vlastní zpracování

4.5 Model zdravotní péče v mikropodniku

Vytvoření základního modelu hlavní činnosti organizace vychází z požadavku ISO/IEC 27001 kap.8, kdy „*organizace musí plánovat, implementovat a řídit procesy potřebné ke splnění požadavků bezpečnosti informací*“ a podle ISO/IEC 27001, tabulka A.1, opatření A17.1.2 „organizace *musí ustanovit, dokumentovat, implementovat a udržovat procesy, postupy a opatření k zajištění požadované úrovně kontinuity pro bezpečnost informací… „*, tedy model zdravotní péče je součást opatření k dosažení cílů ISMS.

4.5.1 Model zdravotní péče

Rámec služby zdravotní péče je popsán v kapitole 4.2, z kterého vychází potřebnost základního principu implementace systémů řízení bezpečnosti informací v prostředí mikropodniku ambulance VPL. Legislativa a analyzované souvislosti jsou popsány v kapitole 3.3. Bezpečnost informací při poskytování zdravotní péče je v této práci postavena na aktivech, která jsou následně identifikována v kapitole 4.7.

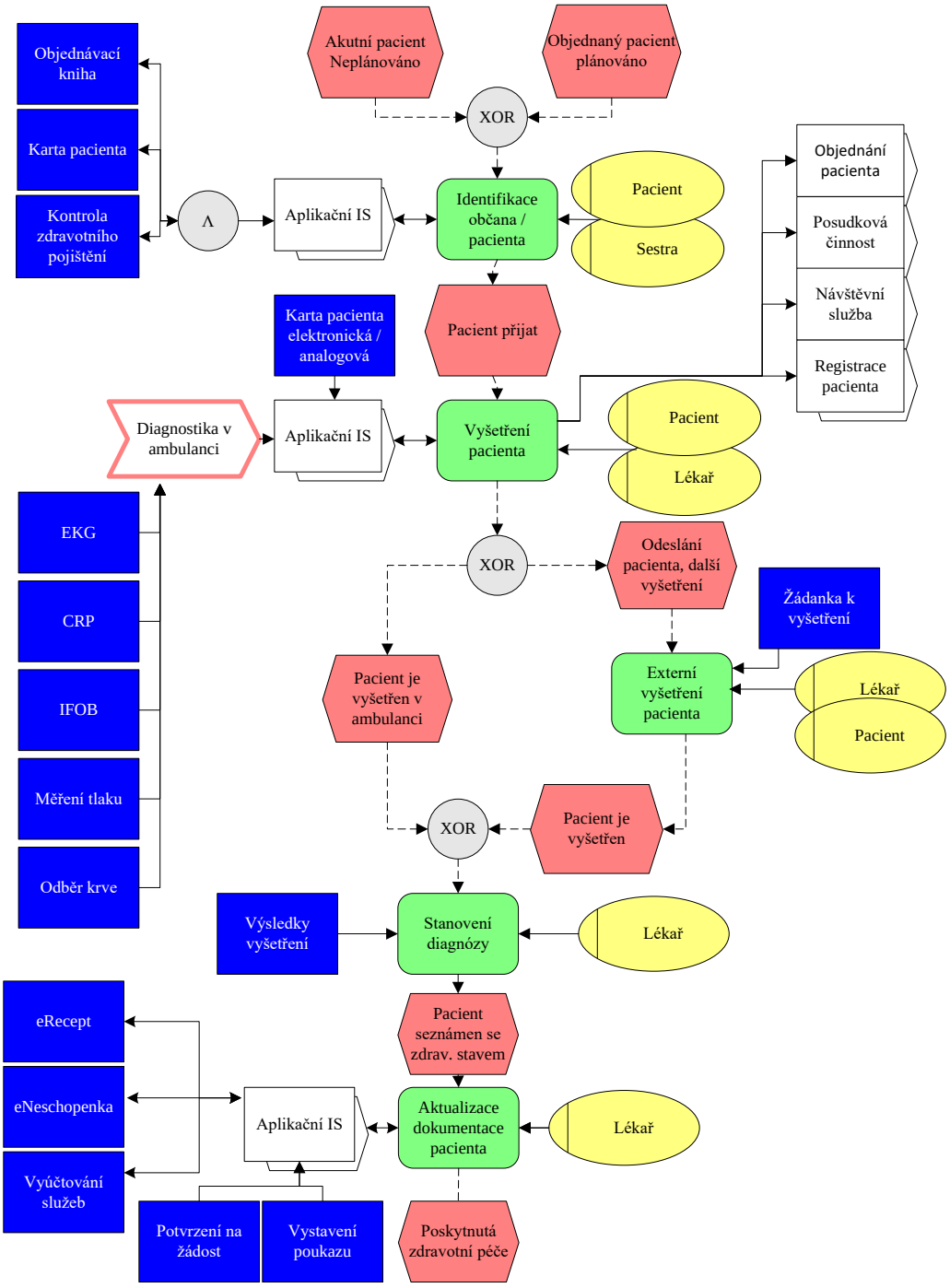
Aktivum zdravotní péče je hlavní službou (primárním aktivem), které autor identifikoval na základě legislativy a je zachyceno na modelu EPC na obrázku 14. Poskytování zdravotní péče je hlavním proces. Stěžejní pro porozumění organizaci (mikropodniku) jsou hlavní procesy. V organizaci autor z běžné činnosti organizace, legislativního rámce a v souvislosti s rozhovory (kapitola 2) identifikoval vybrané procesy:

- **poskytnutí ambulantní zdravotní péče** (hlavní proces) – zpracování osobních informací, manipulace se zdravotní dokumentací při zpracování informaci o zdravotním stavu. Hlavní proces užívá všech opatření PoA;
- **aplikační IS** (řídící proces, schéma na obrázku 15, informační tok na obrázku 16) – informační systém pro zabezpečení správy a řízení informačních procesů a aktiv zdravotnického zařízení. Součástí je také komunikační rozhraní s nastavenými požadavky bezpečného připojení k externím informačním systémům. Pro IS by měla být aplikována opatření dle PoA v souvislosti s politikou bezpečnosti IS;
- **objednání pacienta** (podpůrný proces, model v příloze 2) – bezpečnost informací při komunikaci s pacientem osobní nebo telefonický kontakt. V souvislosti s ISO/IEC 27001 identifikujeme opatření, např.:
    - kap. A.9.2.2, správa uživatelský přístupů, kdy zdravotní sestra musí mít přístup v aplikačním IS k elektronickým kartám a kalendáři objednání;

- kap. A.18.1.4, soukromí a ochrana osobních údajů s ohledem na informační bezpečnost a GDPR;

- **registrace nového pacienta** (podpůrný proces, model v příloze 3) – zpracování osobních informací pacienta, a to souhlas pacienta (GDPR), převzetí zdravotní dokumentace z jiného poskytovatele zdravotní péče, registrace na zdravotní pojišťovně.

Obrázek 14 EPC model zdravotní péče v ambulanci praktického lékaře



Zdroj: vlastní zpracování

V souvislosti s ISO/IEC 27001 identifikujeme opatření, např.:

- kap. A.13.2.3, elektronické předávání zpráv – opatření k bezpečnému přenosu zdravotnických informací mezi poskytovateli zdravotní péče;
- kap. A.18.1.3, ochrana záznamů – opatření k splnění dle CIA;

- **posudková činnost** (podpůrný proces, model v příloze 1) – informační bezpečnost v komunikačním prostředí s třetí stranou, vystavení posudku k zdravotnímu stavu pacienta, smlouva s třetí stranou, fakturace, operace s informacemi. V souvislosti s ISO/IEC 27001 identifikujeme opatření, např.:
  - kapitola A.13, bezpečnost komunikací je nutné zajistit bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty;
  - kapitola A.18, soulad s právními a smluvními požadavky nebo povinnostmi plnění se smlouvy v souvislosti s ochranou osobních údajů.

4.5.2 Aplikační IS

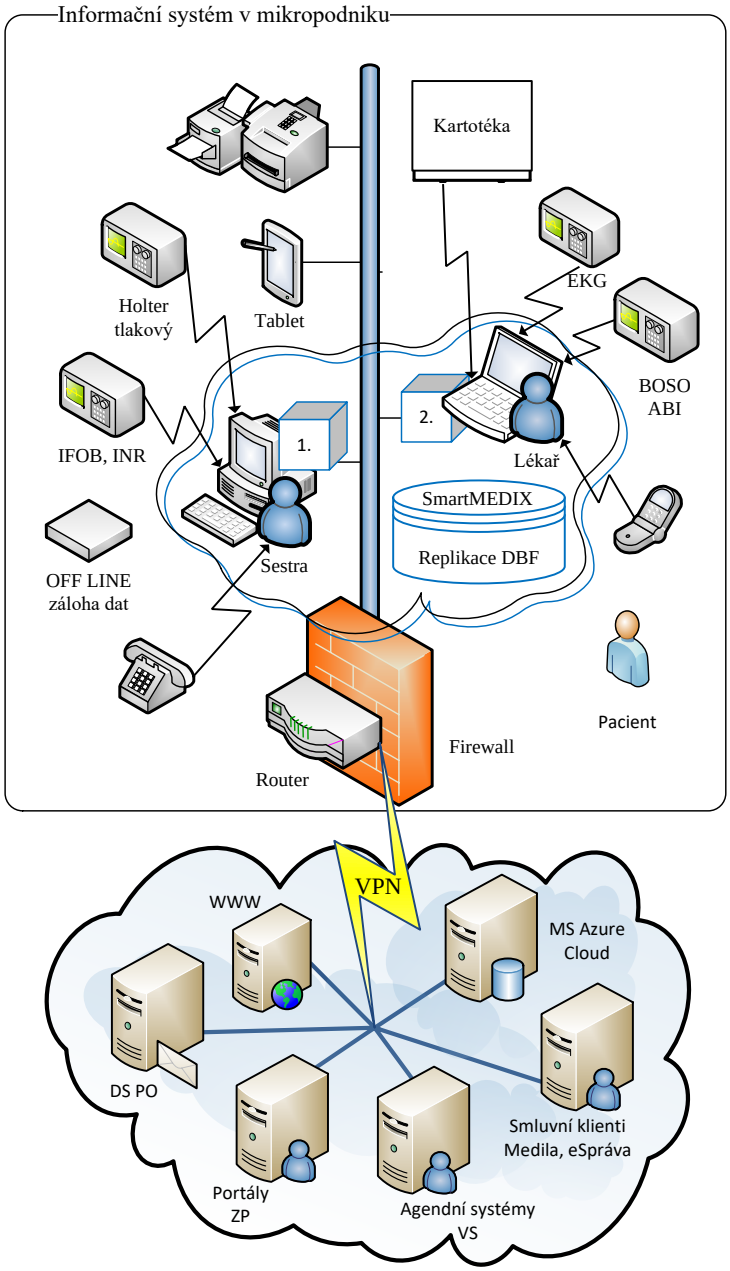
Informační systém je vybudován za účelem podpory hlavního procesu v mikropodniku, a to poskytování ambulantní zdravotní péče. Informační systém poskytuje:

- správu a vedení zdravotnické dokumentace pacientů v elektronické a analogové (listinné) formě;
- účtování výkonů zdravotní péče pacientů zdravotním pojišťovnám;
- přenos dat z diagnostických přístrojů ambulance do aplikačního IS po vyšetření pacientů k dalšímu zpracování;
- propojení jednotlivých počítačů, periferních zařízení a přístrojů v lokální síti LAN;
- provoz aplikačního software SmartMEDIX, který poskytuje řízení toku informací;
- užívá komunikačního prostředí internetu k výměně dat s jinými IS, agendními systémy, poštovními elektronickými službami a ostatními poskytovateli zdravotní péče.

Rozsah plnění opatření bezpečnosti informací provozu aplikačního IS dle ISO/IEC 27001 odpovídá prohlášení o aplikovatelnosti PoA (příloha 12).

Schéma informačního systému mikropodniku je zachyceno ve formě IS ambulance praktického lékaře na obrázku 15, kde identifikujeme potřebu aplikace nutných opatření informační, komunikační, technologické, fyzické, personální a kryptografické bezpečnosti. Tato opatření budou popsána v návrhu metodiky bezpečnosti IS.

Obrázek 15 Schéma platformy IS mikropodniku

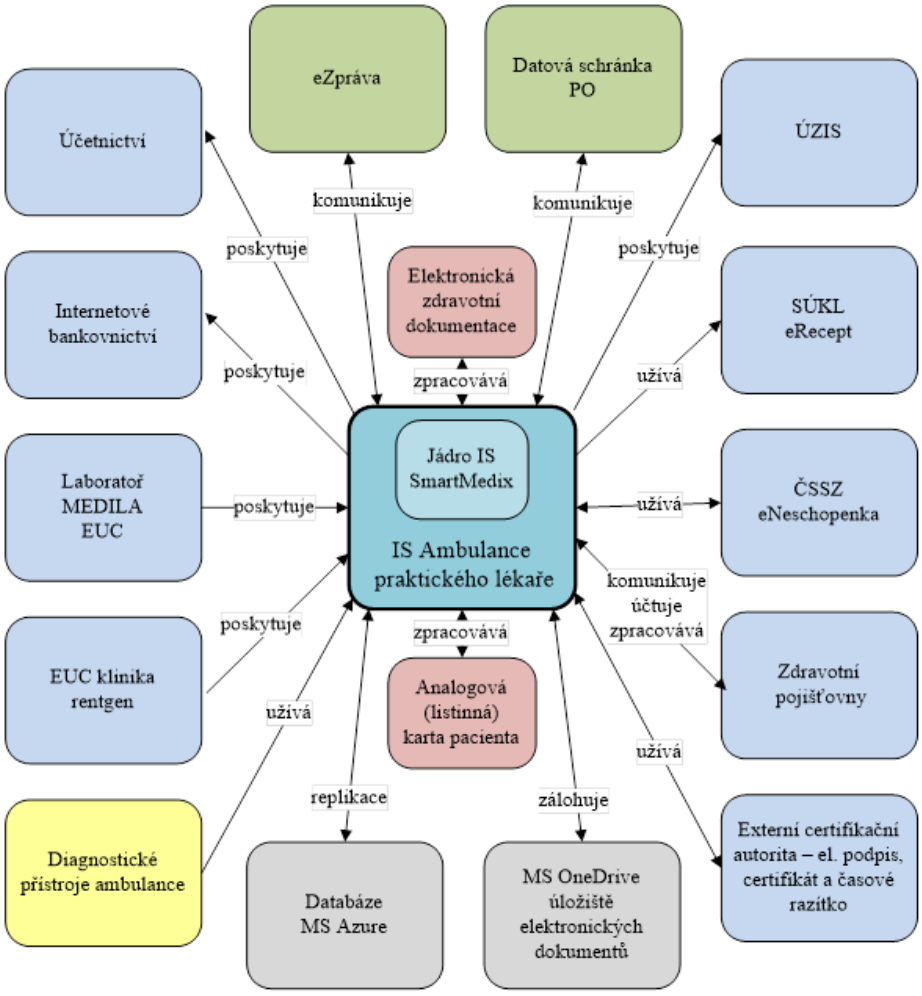


Zdroj: vlastní zpracování

IS mikropodniku je provozován na 2 počítačích (stolní a přenosný) s nainstalovaným operačním systémem Windows 10, potřebným podpůrným softwarem, ovladači periferních zařízení, diagnostických přístrojů a aplikačním softwarem SmartMEDIX. V počítačích je naistalován SW pro ochranu proti škodlivému kódu. Počítače a zařízení jsou propojeny v intranetu v zabezpečené WLAN s WPA2, kdy výměna informací mezi počítači se uskutečňuje pomocí replikace databáze, kterou zabezpečuje SW SmartMEDIX. Pro připojení k externím informačním systémům se užívá připojení do internetu přes router

s aplikovaným firewallem a zabezpečeným přenosem v komunikačním prostředí pomocí VPN. Informace v informačním systému se ukládají a zpracovávají v šifrované databázi. Tato databáze je zálohována v cloudu (MS Azure) a mezi počítači probíhá komunikace pomocí replikace databáze pomocí SW SmartMEDIX, protože notebook je využíván lékařem pro práci mimo ambulanci a k vyšetření pacientů při návštěvách.

Obrázek 16 Informační tok v IS



Zdroj: vlastní zpracování

4.5.3 Řízení zpracování informací

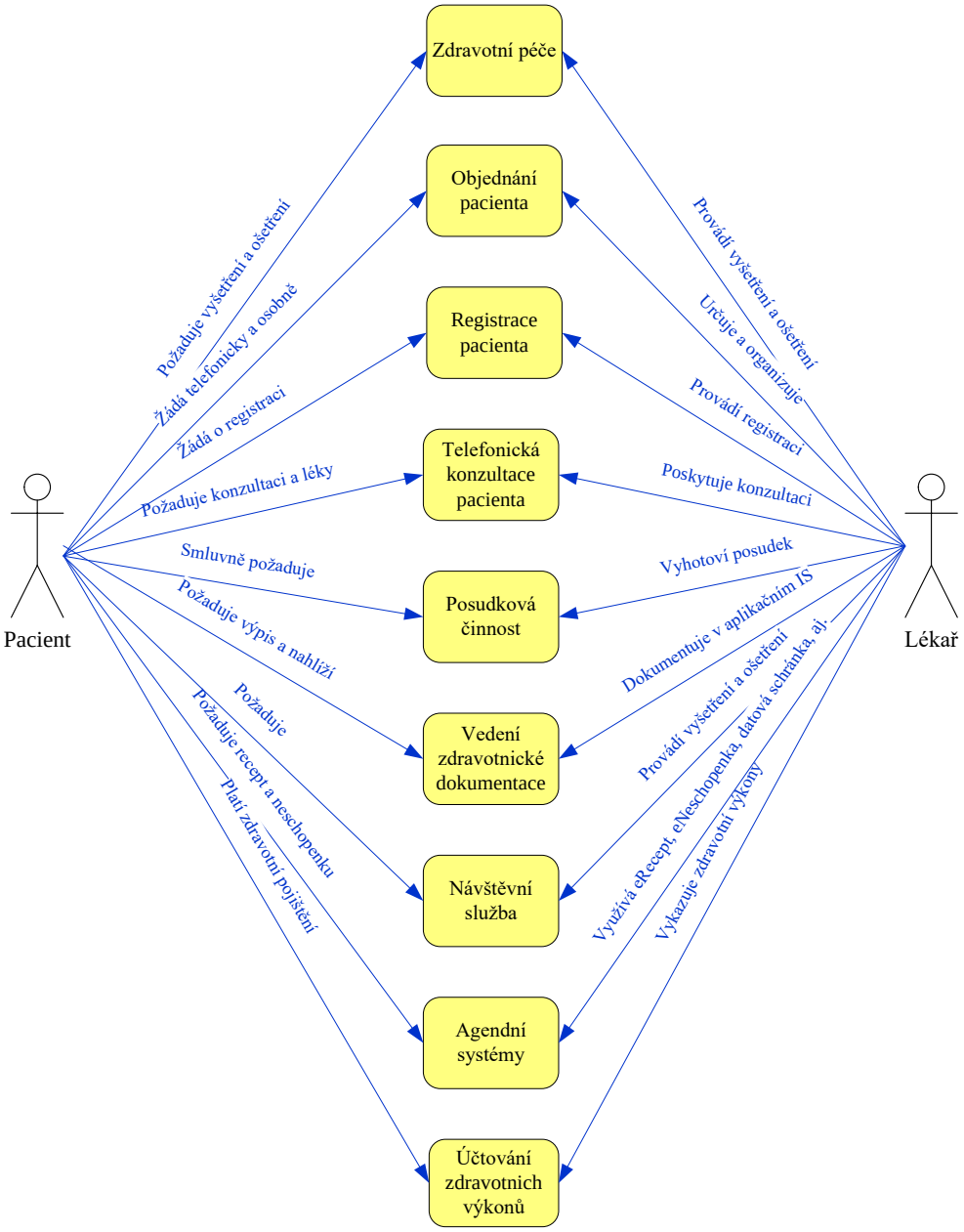
Organizace dle ISO/IEC 27001, kapitola 7.4 má povinnost v systému řízení bezpečnosti informací určit potřebu pro interní a externí komunikace, které zahrnuje:

- kdo musí komunikovat;
- kdy komunikovat;

- s kým komunikovat;
- o čem komunikovat;
- procesy, kterými musí být komunikace realizována.

Pro řízení dokumentovaných informací dle kapitoly 7.5.3 je nutné identifikovat tok informací z důvodu realizace nutných opatření dle PoA jako např. kap. A.13.2.3, elektronické předávání zpráv – opatření k bezpečnému přenosu zdravotnických informací mezi poskytovateli zdravotní péče.

Obrázek 17 Use case (lékař – pacient)



Zdroj: vlastní zpracování

V souvislosti s kapitolou 4.5.1 a 4.5.2 této práce se v hlavním procesu podnikatelské činnosti organizace zpracovávají informace, které jsou součástí informačního prostředí poskytovatele zdravotní péče. V informačním prostředí autor identifikoval jednotlivé činnosti, při kterých se uskutečňuje manipulace s informacemi. Způsob řízení interní a externí komunikace zachycuje informační tok v IS, který je znázorněn na obrázku 16. Autor dále analyzoval komunikaci mezi pacientem a lékaře, která se opírá o povinnosti poskytovatele zdravotních služeb. Na základě identifikovaných procesů a požadavků na informace mezi lékařem a pacientem byl vypracován use case diagram na obrázku 17.

Pro potřeby práce klasifikujeme informace v ambulanci VPL podle potřeby nastavení ochrany bezpečnosti informací na (vlastní):

- veřejné – veřejně publikovatelné dokumenty, které obsahují veřejně přístupné informace (ceník služeb nehrazených z veřejného zdravotního pojištění, informační webový portál, ambulantní doba, informace pro pacienty o možnosti očkování aj.);
- citlivé – informace a dokumenty obsahující neveřejné informace organizace, účetnictví organizace, smlouvy se zaměstnanci, obchodních partnerů, které mohou vyžadovat smluvní či právní ochranu;
- důvěrné – zdravotnická dokumentace pacientů, citlivé osobní údaje, obchodní tajemství.

Dále pro elektronické a listinné dokumenty v mikropodniku vniká potřeba řízené distribuce dokumentů:

- nastavit toky informací a manipulace listinných dokumentů;
- digitalizovat dokumenty pro usnadnění manipulace (sdílení);
- organizovat zabezpečený přístup k souborům digitalizovaných dokumentů;
- archivovat listinné originály dokumentů a zálohovat digitalizované dokumenty.

Tabulka 2 obsahuje vybraný přehled činností organizace a identifikovaných manipulací s informacemi, pro potřeby interního a externího toku informací stanovených na základě:

- právního rámce poskytování zdravotní péče (kapitola 4.2);
- kontextu činnosti modelu zdravotnického zařízení (kapitola 4.3);
- modelu hlavního procesu na obrázku 14;
- modelu informačních toků IS viz. obrázek 16;
- use case diagramu interakce aktéra (lékař, pacient) a systému na obrázku 17;
- rozhovoru č.2 uvedeného v metodice diplomové práce kapitola 2;

Tabulka 2 Manipulace (operace) s informacemi v ambulanci VPL

		informace získané od		informace odeslané k			
Činnost v organizaci	**Příklad manipulace**	**pacienta**	**externí subjekt**	**pacienovi**	**externí subjekt**	**fyzická listina**	**Klasifikace informace**
Archivace zdravotnické dokumentace	Uzavření dokumentce pacienta a uložení na 10let do archivu lékaře	X	X			X	důvěrné
Dopis registrovanému pacientovi	Odeslání pozvánky, informací VPL			X		X	citlivé
Doporučení k hospitalizaci	Vystavení dokumentu a zápis, sdílení			X	X	X	důvěrné
Hlášení infekčního onemocnění	Zaslání hlášení a zápis, sdílení	X			X	X	důvěrné
Hlášení reakce po očkování	Zaslání hlášení a zápis, sdílení	X			X		důvěrné
Hlášení ÚZIS, SÚKL	Odeslání souhrnného hlášení				X		citlivé
Komunikace datovou schránkou, eSprávou	Sdílení informací, ukládání, zpracování zdravotní dokumentace		X		X		citlivé
Komunikace mailem	Sdílení informací veřejného charakteru	X	X	X	X		veřejné
Komunikace telefonem	Výměna informací hlasem, zápis do dokumentace, vystavení receptu	X	X	X	X		citlivé
Kontrola dokumentace posudkovým lékařem	Sdílení, zpracování informací a manipulace s fyzickou kartou pacienta		X	X	X	X	důvěrné
Kontrola dokumentace pracovníkem hygienické služby	Nahlédnutí do dokumentace, hygienická služba vydává zprávu o kontrole				X	X	citlivé
Kontrola dokumentace revizním lékařem	sdílení, čtení, zápis revizní lékař vydává zprávu o kontrole	X	X	X	X	X	důvěrné
Nahlédnutí do dokumentace oprávněnou osobou	Čtení a zápis do dokumentace, sdílení			X	X	X	důvěrné
Návštěvní služba	Zápis do dokumentace, vystavení zprávy, eRecetu, eNeschopenky	X		X		X	důvěrné
Nepravidelná péče	Zápis do dokumentace, vystavení zprávy, eRecetu, eNeschopenky	X		X		X	důvěrné
Posudková činnost	Vystavení dokumentu, zápis, sdílení	X	X	X	X	X	citlivé
Potvrzení na žádost	Vystavení dokumentu a zápis	X		X		X	citlivé
Zdravotní péče (prohlídka v ambulaci)	Zrpacování informací a dokumentů, zápis do dokumentace, eRecept, eNeschopenka	X		X			důvěrné
Registrace nového pacienta	Založení dokumentace, kontrola osobních údajů, odeslání informace ZP	X			X	X	citlivé
Smlouvy s dodavateli a 3-tími stranami	Zpracování citlivých osobních informací, vystavení dokumentu a zápis		X		X	X	citlivé
Vyplnění povinného dotazníku	Zápis a založení do dokumentace	X				X	citlivé
Vyřazení z péče (přeregistrace, úmrtí)	Zápis do dokumentace, výpis z zdravotnické dokumentace, archivace	X	X		X	X	důvěrné
Vystavení neschopenky	Zápis do dokumentace, eNeschopenka	X		X	X		důvěrné
Vystavení OČR	Vystavení dokumentu a zápis	X		X			důvěrné
Vystavení pojistky	Vyplnění pojistky a zápis, sdílení	X	X	X	X	X	citlivé
Vystavení poukazu na léčebnou a ortopedickou pomůcku	Vystavení dokumentu a zápis	X		X		X	důvěrné
Vystavení receptu/žádanky	Zápis, eRecept, dokument	X		X		X	důvěrné
Vystavení žádosti o lázně	Vystavení poukazu, výpis zdravotnické dokumentace a zápis	X		X		X	citlivé
Vyúčtování služeb	Vyúčtování provedených zdravotních výkonů a kapitace pojišťovnám			X	X		citlivé
Vyžádání dokumentace policií / soudem	Předání dokumentace na základě řádné žádosti a zápisu, sdílení		X		X	X	důvěrné
Žádanka - laboratoř	Vystavení dokumentu a zápis, sdílení	X		X	X	X	důvěrné
Žádanka - vyšetření specialistou	Vystavení dokumentu, výpis zdravotnické dokumnetace a zápis		X	X			citlivé
Informace na webovém portále organizace	Informace nezdravotnického charkteru pro veřejnost			X	X		veřejné
Personální dokumentce	Vystavení pracovních smluv, přijetí a ukládání citlivých osobních infromací	X				X	citlivé
Účetní dokumentace	Přijetí a odesílání faktur, účtování, převážně interní dokumentace pro vedení	X	X		X	X	citlivé
Smlouvy se zdravotními pojišťovnami	Zrpacovní , uložení a sdílení dokumentů		X		X	X	důvěrné
Interní dokumentace / politiky pro provoz ambulance	Předpisy, revize, skladové hospodářství, politiky - zpracování ,uložení					X	citlivé

Zdroj: vlastní zpracování, Těšitelová a kol. (2018, s. 15)

4.6 Organizace bezpečnosti informací

4.6.1 Základní řešení bezpečnosti informací v mikropodniku

Počáteční stav informační bezpečnosti v organizaci by měl být nastaven politikou bezpečnosti informací, která je schválena management organizace, zveřejněna a dána na vědomí zaměstnancům a případně relevantním externím stranám. (ISO 27002, 2014, s. 10) Tato zavedená politika by měla být porovnána se skutečným stavem v mikropodniku. Toto porovnání nazýváme stav implementace opatření bezpečnosti informací, které autor provedl v kapitole 4.4.2. V souvislosti s modelovým mikropodnikem (ambulance VPL) pro další práci předpokládáme, že v organizaci není zavedena politika ISMS, a proto je potřeba vytvořit metodiku bezpečnosti IS, která mj. politiku bezpečnosti IS bude užívat, zavede ji.

4.6.2 Rozsah systému řízení bezpečnosti informací

ISMS je založeno na principu řízení rizik a neustálém zlepšování. V případě, kdy je rozsah stanoven pouze na vybranou část organizace (dílčí část IS), je důležité do rozsahu systému řízení informací zahrnout vše podstatné pro zajištění bezpečnosti informací regulovaného IS. Rozsah ISMS je vhodné v organizaci vymezit na všechny služby a informace, které mají být zabezpečeny v souvislosti s primárními a podpůrnými aktivy IS, tedy může být zahrnuta celá organizace. Tento rozsah musí být dokumentačně popsán například formou funkčního schématu, procesním modelem, topologií, organizačním řádem či prohlášením o aplikovatelnosti ISMS viz. tabulka 3. Celý rozsah prohlášení o aplikovatelnosti je uveden v příloze 12.

Tabulka 3 Ukázka zpracování „Prohlášení o aplikovatelnosti ISMS“

Kapitola normy	Cíle opatření	Aplikovatelnost	Vlastní opatření k splnění cíle
A.5	**Politiky bezpečnosti informací**		
A.5.1	**Směřování bezpečnosti informací vedením organizace**		
Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicemi.			
A.5.1.1	Politiky pro bezpečnost informací	Ano	Vytvoření politiky ISMS, politiky bezpečnosti IS.
A.5.1.2	Přezkoumání politik pro bezpečnost informací	Ano	Hodnocení aktuálního stavu dle navrhnuté politiky ISMS pomocí GAP analýzy.

Zdroj: vlastní zpracování, ISO 27002 (2014)

4.6.3 Fyzická bezpečnost

Cílem opatření fyzické bezpečnosti je stanovit a aplikovat základní opatření fyzické bezpečnosti v prostorech výkonu činnosti organizace, která budou předcházet poškození, zneužití, krádeži aktiv či majetku, které mají vliv na řízení kontinuity činností a CIA.
Analýza fyzické bezpečnosti organizace objektu ambulance praktického lékaře dle ISO/IEC 27002 kap.11 – fyzická bezpečnost a bezpečnost prostředí (vlastní zpracování):

- objekt organizace je zabezpečen proti neautorizovanému fyzickému přístupu;
- instalovány dveře a zámky třídy RC3 dle ČSN EN 1627;
- instalovány plastová okna s kovovou výztuží třídy RC2N dle ČSN EN 1627-30;
- ve vnitřním prostoru jsou dveře třídy RC2 jsou zamykatelné se zámkem třídy 3;
- fyzický bezpečnostní perimetr je zastřežen EZS s osobním kódem zaměstnance a heslem pro dohled, v objektu jsou instalovány pohybová čidla a proti požárním čidlo, kdy EZC je napojeno na pult ostrahy fa Jablotron s dozorem bezpečnostní agentury určené pro případný výjezd a kontaktování policie při incidentu;
- rozvodová skříň elektrické energie s pojistkami a uzávěr vody je v bezpečnostním perimetru objektu;
- kabelové rozvody telefonní VDSL sítě jsou vedeny v objektu ordinace, slaboproudé rozvody LAN nejsou realizovány, užívá se WLAN s WPA2 a fixní IP adresou;
- v objektu není centrální rozvod zálohovaní elektrické energie, u PC a notebooku nejsou instalovány žádné záložní zdroje;
- objekt prošel v roce 2022 kontrolou BOZP včetně povinných revizí.

Výsledek porovnání GAP analýzou (kap. 4.4.2) pro opatření A.11.1.1 – A.11.2.9 je uvedeno v tabulce PoA v příloze 12 ve sloupci *Počáteční stav:*

- 5 opatření plní v plném rozsahu:
    - A.11.1.2 Fyzické kontroly vstupu;
    - A.11.1.3 Zabezpečení kanceláří, místností a vybavení;
    - A.11.2.4 Údržba zařízení;
    - A.11.2.5 Přemístění aktiv;
    - A.11.2.8 Uživatelská zařízení bez obsluhy;
- 6 opatření je splněno částečně:
    - A11.1.1. Fyzický bezpečnostní perimetr – chybí dokumentace řešení fyzické bezpečnosti perimetru, přehled informačních aktiv;

- A.11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí – chybí zabezpečení okenních otvorů v přízemí budovy mřížemi;
- A.11.2.1 Umístnění zařízení a jeho ochrana– chybí dokumentované politiky bezpečnosti a postupy kontinuity;
- A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace – není dokumentováno politikou bezpečnosti IS;
- A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení – zabezpečit nákup SW pro bezpečný výmaz záznamových medií;
- A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru – chybí pravidelná edukace personálu a politika bezpečnosti IS;

- 2 opatření nesplňuje:
  - A.11.2.2 Podpůrné služby – chybí UPS (záložní elektrické napájení);
  - A.11.2.3 Bezpečnost kabelových rozvodů – je nutná rekonstrukce LAN;
- 2 opatření nejsou součástí POA:
  - A.12.1.1 Práce v bezpečných oblastech;
  - A.12.1.2 Oblasti pro nakládku a vykládku;

Komparací autor identifikoval nutnost zavedení a zlepšení 8 opatření dle PoA.

4.6.4 Role v ISMS organizace

Cílem opatření je stanovit bezpečnostní správu. Povinnou rolí je vrcholové vedení zastoupené jednatelem společnosti, které nese odpovědnost za bezpečnost informací a zajištění odpovídajících podmínek pro klíčové role, které se na ISMS aktivně podílejí. Role podle ISO/IEC 27001 kap. 5.3. jsou stanoveny *„Vrcholové vedení organizace musí zajistit, že odpovědnost a pravomoci pro role relevantní bezpečnosti informací jsou přiřazeny a komunikovány.“* (ISO 27001, 2014) Autor navrhuje povinnost určit role, odpovědnost a pravomoci delegovat, ale norma již striktně nenařizuje, jakým způsobem. S ohledem na velikost mikropodniku a zkušenost autora s provozem informačních systémů, navrhne strukturu a rozsah rolí.

Návrh stanovení rolí ISMS v mikropodniku organizovat (vlastní zpracování)**:**

INTERNÍ ROLE (výkonné role)

- gestor aktiv (jednatel)
    - je nejvýše postavený vedoucí pracovník organizace;
    - rozhoduje o nastavení požadavků nutných pro zajištění bezpečnosti aktiv;
    - stanovuje garanta aktiv;
- vlastník aktiv (lékař, odborný garant)
    - má odpovědnost za zajištění rozvoje, použití a bezpečnosti aktiva;
    - spolupracuje s ostatními osobami zastávajícími bezpečnostní role;
- administrátor (správce IS)
    - výkonná role správce IS a KS;
    - může být poradcem pro garanta aktiv v oblasti rozvoje, použití a bezpečnosti;
- uživatel (zaměstnanci)
    - mají přidělena uživatelská práva;
    - výkonná role osoby nakládající s informačními aktivy při běžné činnosti mikropodniku (poskytování zdravotní péče).

Tabulka 4 Role ISMS návrh části RACI matice

Popis činnosti	**bezpečnostní role ISMS** EXTERNÍ			**výkonné role ISMS** INTERNÍ			
	Manažer ISMS	**Architekt ISMS**	**Auditor ISMS**	**Jednatel**	**Vlastník aktiv**	**Administrátor**	**Uživatel**
Identifikace aktiv							
Identifikace aktiv	**R**	**C, I**		**A**	**I**		
Stanovení vlastnictví aktiv	**R**	**C, I**		**A**	**I**		
Klasifikace aktiv							
Klasifikace aktiv	**R**	**C, I**		**A**	**I**		

Zdroj: vlastní zpracování, Bezouška (2022)

EXTERNÍ ROLE (bezpečnostní role)

Pro nastavení bezpečnostní politiky ISMS v organizací je jednateli mikropodniku doporučeno nasmlouvat poskytovatele služby oblasti návrhů bezpečnosti informací, informačních systému v souladu s IMSS a KB pro analýzu stavu informační bezpečnosti, návrhu a prvotního zavedení opatřeni k plnění ISMS včetně systému řízení informační bezpečnosti v souladu s plánem řízení rizik. Je vhodné, aby jedenkrát ročně došlo k přezkoumání legislativních, informačních, technických, a organizačních změn včetně posouzení rizik s cílem udržení kontinuity bezpečnosti informací v mikropodniku. Jednateli je doporučeno zabezpečit outsourcing rolí:

- manažer / architekt ISMS
    - role manažera a architekta mohou být sloučeny z důvod obdobné odbornosti;
    - většinou jednorázový smluvní vztah
- auditor ISMS
    - měla by být vybrána osoba nezávisle na manažeru / architektu ISMS, aby bylo dosaženo maximalizace užitku a úrovně kontroly a komparace nastavených opatření;
    - provádí audit stavu ISMS jedenkrát ročně.

Vzor zpracování návrhu rolí formou RACI matice je uveden v tabulce 4.

4.7 Identifikace a správa informačních aktiv

Vhodným úvodem jsou otázky k identifikaci aktiv podle dokumentu NÚKIB (2022b) „Průvodce řízení aktiv a rizik dle vyhlášky o kybernetické bezpečnosti“ k hledání primárních aktiv, na které autor odpoví na základě rozhovoru č.1 s jednatelem a lékařem organizace poskytující primární zdravotní péči, z kterého byl pořízen tento upravený záznam (vlastní zpracování, kapitola 2, rozhovor č.1):

- Jaký je účel této organizace, agendy či IS?
  Poskytování ambulantní zdravotní péče a vedení zdravotnické dokumentace, provoz aplikačního informačního systému s programem SmartMEDIX.
- Jaké jsou v rámci této organizace, agendy či IS klíčové procesy?
  Vedení elektronické a dokumentové podoby zdravotních karet pacientů, registrace pacientů, posudková činnost, návštěvní služba, očkování, účtování zdravotnických

výkonů poskytnutých pacientům a práce v informačním systému s programovým vybavením SmartMEDIX.

- Jací jsou klíčoví zákazníci či uživatelé této organizace, agendy či IS?
  Ambulanci navštěvují registrovaní a neregistrování pacienti; objednávají se telefonicky nebo osobně; pacienti telefonicky volají a informují se o zdravotním stavu, potřebují recept na léky, neschopenku; zaměstnanci nasmlouvaných organizací, kterým ambulance poskytuje pracovně-lékařskou posudkovou činnost; ČSSZ požaduje lékařské posudky pro osoby se zdravotním omezením.
- Bez jakých informací nemůžete vykonávat svoji práci?
  Lékařské správy a výpisy o zdravotním stavu pacientů od jiných poskytovatelů zdravotní péče; zdravotní dokumentaci (papírovou); informace ukládané a vedené v informačním systému; výsledky vyšetření z diagnostických přístrojů v ambulanci; informace o registraci nového pacienta; informace o úhradách za provedení zdravotnických výkonů.
- Jaké činnosti jsou potřeba k vykonávání běžné agendy?
  Zpracovávání zdravotních a osobních informací; posílání výpisů ze zdravotní dokumentace; odesílání a přijímání emailů, datových zpráv, výsledků z vyžádaných vyšetření; telefonický kontakt s pacientem, osobní kontakt s pacientem, nákup zdravotnického materiálu, léků a očkovacích látek; odesílání měsíčních výkazů o poskytnuté léčbě a kapitačních platbách nasmlouvaným zdravotním pojišťovnám; vedení účetnictví, užívání kvalifikovaného a komerčního elektronického certifikátu, práce v aplikaci SmartMEDIX.
- Jakou pro mě má agenda či IS hodnotu (z pohledu významu/smyslu) a co je v něm to důležité?
  Zdravotní dokumentace a to papírová (uložená v kartotéce) a elektronická (uložená v informačním systému) jsou nejcennější pro lékaře a pacienta; v počítači je přístup do různých systémů a portálů (WebLIMS, eSpráva, eRecept, eNeschopenka, zdravotní pojišťovny, ÚZIS).
- Jsou součástí této organizace, agendy či IS osobní údaje, citlivé osobní údaje nebo obchodní tajemství?
  Operace s důvěrnými zdravotnickými informacemi pacientů, citlivé osobní informace (GDPR), interní firemní dokumenty jako jsou smlouvy, vnitřní směrnice; zveřejňovaní informací na internetu – webu; smlouvy ze zdravotními pojišťovnami, účetnictví.

- Jsou s existencí této organizace, agendy či IS spojeny nějaké zákonné nebo smluvní požadavky?

  Ano, zákonem č. 372/2011 Sb., Zákon o zdravotních službách a podmínkách jejich poskytování; vyhláškou č. 92/2012 Sb., o požadavcích na minimální technické a věcné vybavení zdravotnických zařízení a kontaktních pracovišť domácí péče; vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci; vyhláška č. 70/2012 Sb. o preventivních prohlídkách; zákon č. 373/ 2011 Sb. o specifických zdravotních službách; zákon č. 101/2000 Sb., o ochraně osobních údajů; nařízení k GDPR EU č. 2016/679.
- Zahrnuje vaše práce mezinárodní spolupráci?

  Ne.
- Může dojít k poškození pověsti při narušení bezpečnosti informací?

  Ano, především pokud by došlo úniku zdravotnické dokumentace; citlivých dat s ohledem na GDPR; sdělení informací o zdravotním stavu neoprávněné osobě; způsobené chybě lékaři při nedodržení léčebných postupů; krádeži nezabezpečených zdravotnických informací; nevhodném technickém a diagnostickém vybavení ambulance.
- Může mít narušení bezpečnosti informací vliv na bezpečnost či zdraví osob?

  Fatální následky na souvislosti o zdravotním stavu, předepsaných lécích, ztráty informací z důležitých nákladných vyšetření, neoprávněné změna osobních dat, smazaní zdravotních informací o pacientech; pokud není zdravotní dokumentace dostupná nelze vykonávat zdravotní péči; hackerský útok na informační systém, zavirování počítačů.
- Hrozí v nějaké situaci možnost finanční ztráty či nutnost nahrazovat škody (pokuty/sankce)?

  Ano hrozí; finanční postih hrozí za nedodržení plnění nařízení GDPR v souvislosti o nakládání s osobními informacemi a zdravotní dokumentací pacientů, která je důvěrná; při prokázané chybné léčbě pacienta, nedodržení hygienických norem aj.
- S jakými dalšími systémy pracujete v rámci výkonu běžné pracovní činnosti?

  Datová schránka, eSpráva, WebLIMS, Portál zdravotních pojišťoven, eNeschopenka, eRecept, eOčkování, Portál ČSSZ, SÚKL, elektronické bankovnictví.

Z uvedeného rozhovoru plyne, že důvěrné informace (zdravotní informace o pacientech) se zpracovávají v informačním systému organizace, (aplikační IS), kde jádrem je aplikační software SmartMEDIX, (aplikační SW) který vymezuje službu (hlavní proces) poskytování

zdravotní péče. V této souvislosti NÚKIB v dokumentu „*Systém a rozsah ISMS“* klasifikuje informační systém jako službu, pro kterou existuje, tedy pro službu zdravotní péče. *Informační nebo komunikační systém je tvořen aktivy, tedy jak technickým a programovým vybavením, komunikačními prostředky, objekty, zaměstnanci a dodavateli, stejně tak jako informacemi, které zpracovává a službami (procesy), které tento informační nebo komunikační systém poskytuje. Tato aktiva podporují výkon předmětné služby v daném rozsahu a kvalitě, přičemž se nezohledňuje důležitost daného aktiva pro její zajištění – všechna, i ta nejméně důležitá aktiva, jsou součástí informačního nebo komunikačního systému, pokud slouží k zajištění jeho funkčnosti a poskytování předmětné služby v požadované kvalitě*. (NÚKIB, 2022a)

Identifikace informačních aktiv a jejich následná analýza podle Bezouška (2022) je základním předpokladem pro možnost efektivního řízení jejích bezpečnosti. Informační aktiva jsou řazena v hierarchické struktuře, počínaje samotnými informacemi, přes informační systémy, které data a informace zpracovávají, až po konkrétní technologie a komponenty, které provoz těchto informačních systémů zajišťují. Aby byla identifikace a analýza aktiv informačního systému úplná, je proto nutné široké zapojení celého týmu odborníků ze všech oblastí správy IS/ICT.

4.7.1 Identifikace aktiv

Identifikace aktiv dle Bezouška (2022) je proces, kde je nutné vymezit hranice a rozsah zkoumaného informačního systému. V rámci těchto hranic je provedeno systematické rozdělení na jednotlivé aktiva. Každé aktivum je přesně popsáno, identifikováno, určena jeho úloha v informačním systému včetně garanta (vlastníka), který plně odpovídá za dané aktivum (jeho stav, funkčnost, údržbu, bezpečnost). Kompetence a odpovědnost za identifikaci aktiv mají manažer KB/BI, garanti za primární a podpůrná aktiva a administrátor. Přiměřenost dekompozice aktiv je otázkou nezbytné úrovně dekompozice aktiv pro identifikaci aktiv. Příliš detailní dekompozice by byla nejen pracná, ale i zbytečná. Bez dekompozice aktiv by bezpečnost informací nemusela být prakticky řiditelná.

Pro identifikaci aktiv dle (ISO 27005, 2019), kapitola B.1.2, potřebuje organizace nejprve identifikovat svá aktiva na příslušné úrovni a to:

- **primární aktiva** – klíčové procesy a informace o předmětu příslušné činnosti organizace v našem případě zdravotnického zařízení:

    - **podnikatelské procesy a činnosti** – jsou to procesy bez, kterých nelze uskutečnit poslání organizace a jsou nezbytné, aby splnila aplikovatelné smluvní či právní požadavky vyplívající z činnosti organizace a modifikace procesu by značně ovlivnila její poslání;
    - **informace** – důležité pro uskutečnění podnikatelské činnosti organizace; osobní informace uvedené ve zdravotní dokumentaci pacientů a s tím související náročnost shromažďovaní, ukládání, zpracovávání a přenášení těchto zdravotnických informací;
- **podpůrná aktiva** – mají zranitelnosti, které jsou zneužitelné hrozbami, snažícími se narušit primární aktiva procesy a informace (technická aktiva):
    - **hardware** (sestává se ze všech procesů podporujících fyzické prvky) a **software** (skládá se ze všech programů podílejících se na provozu a zpracování dat ve specifické podnikatelské aplikaci);
    - **síť** (všechna telekomunikační zařízení použitá k propojení několika fyzicky vzdálených počítačů nebo prvků informačního systému);
    - **zaměstnanci** (pro jednotlivá aktiva jsou identifikování klíčový zaměstnanci, kteří jsou zapojeni do správy nebo užívání informačního systému);
    - **lokalita** (obsahuje všechna místa zahrnující prostor nebo části prostoru a fyzické prostředky požadované pro jejich fungování);
    - **organizace** (typ organizace popisuje organizační rámec, obsahující všechny personální struktury přiřazené k úkolům a postupům. Které tyto struktury řídí).

Na základě právního rámce poskytování zdravotné péče (kapitola 4.2) do aktiv zahrnujeme hlavní podnikatelský proces službu poskytování zdravotní péče, protože to je hlavní činnost, která vede k zisku a je ukotvena v zákoně č.372/2011 Sb. Zákon o zdravotních službách, a tedy danou činnost můžeme jako celek považovat za kritickou činnost. Mezi aktiva z této činnosti uvažujeme části, které nakládají s osobními informacemi, zdravotnickou dokumentací v rámci informačního systému a zařadíme zde informace, data, diagnostické přístroje s rozhraním do IS, komunikační rozhraní a fyzické prvky IS. Tyto aktiva, pak řadíme mezi kritická aktiva, která je nutno chránit.

Pro další práci chápeme PAx jako x-té primární aktivum a POAx jako x-té podpůrné aktivum. Na základě předchozí analýzy, pozorování a výzkumných šetření (rozhovorů) autor identifikoval primární a podpůrná aktiva. Tato aktiva podporuje:

- rámce hlavního aktiva organizace kapitola 4.2;
- kontextu modelu zdravotnické organizace kapitola 4.3;
- analýzy v kapitole 4.4;
- modelu zdravotní péče v mikropodniku kapitola 4.5;
- rozhovoru č.1 v úvodu kapitola 4.7.

PRIMÁRNÍ AKTIVA

PA1 – Zdravotní péče (služba);

PA2 – Zdravotnická dokumentace (informace);

PA3 – Účtování zdravotních služeb (informace);

PA4 – Aplikační IS (informace).

Registr primárních aktiv je zpracován do tabulky, kde jsou určené specifikace, vlastník a lokalizace aktiva. Registr aktiv je uveden v tabulce 7.

Obrázek 18 Primárních aktiva a jejich souvislost

Zdroj: vlastní zpracování.

Autor vypracoval podle dokumentu NÚKIB (2022c) „Struktura podpůrných aktiv“ souhrn a grupování identifikovaných podpůrných aktiv (výběr je uveden v příloze 4).

Grupování podpůrných aktiv znamená slučování podpůrných aktiv do kategorií, kde jednotlivá aktiva mají podobný rámec určení, funkce, souvislostí s hlavními aktivy. Souvislosti primárních aktiv a podpůrných aktiv ukazuje tabulka 6.

Grupování podpůrných aktiv bylo provedeno podle:

- typu podpůrného aktiva;
- skupiny podpůrného aktiva;
- kategorie podpůrného aktiva.

PODPŮRNÁ AKITVA:

POA1 – Systémový HW;

POA2 – Systémový SW;

POA3 – Dokumenty;

POA4 – Diagnostické přístroje;

POA5 – Komunikační prostředky;

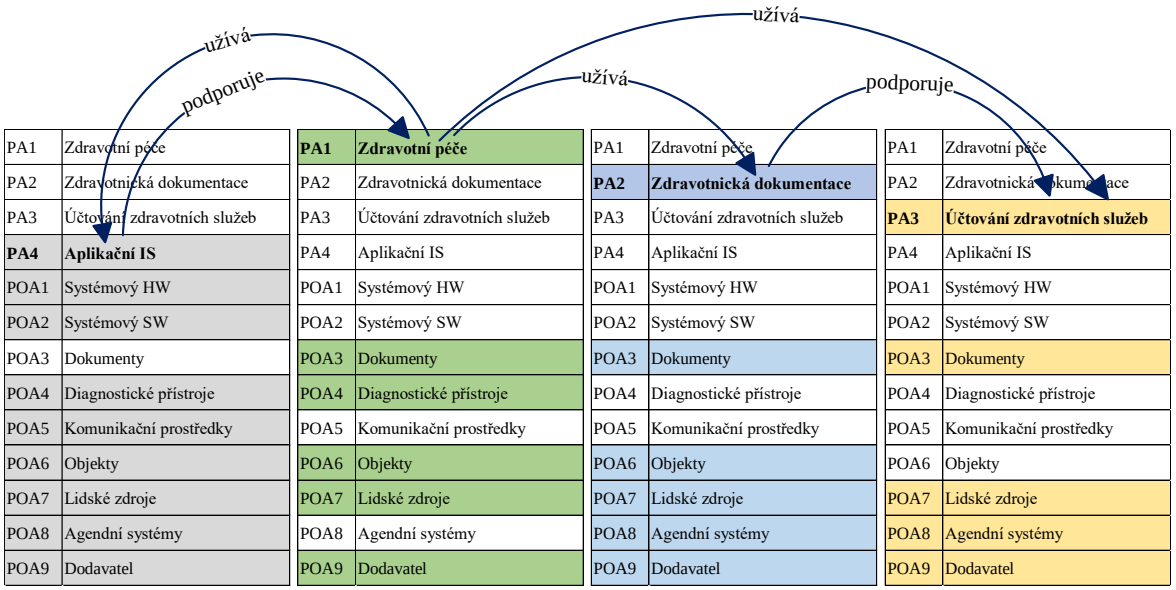
POA6 – Objekty;

POA7 – Lidské zdroje;

POA8 – Agendní systémy;

POA9 – Dodavatel.

Tabulka 5 Přehled souvislostí primárních a podpůrných aktiv



PA1	Zdravotní péče
PA2	Zdravotnická dokumentace
PA3	Účtování zdravotních služeb
PA4	**Aplikační IS**
POA1	Systémový HW
POA2	Systémový SW
POA3	Dokumenty
POA4	Diagnostické přístroje
POA5	Komunikační prostředky
POA6	Objekty
POA7	Lidské zdroje
POA8	Agendní systémy
POA9	Dodavatel

PA1	**Zdravotní péče**
PA2	Zdravotnická dokumentace
PA3	Účtování zdravotních služeb
PA4	Aplikační IS
POA1	Systémový HW
POA2	Systémový SW
POA3	Dokumenty
POA4	Diagnostické přístroje
POA5	Komunikační prostředky
POA6	Objekty
POA7	Lidské zdroje
POA8	Agendní systémy
POA9	Dodavatel

PA1	Zdravotní péče
PA2	**Zdravotnická dokumentace**
PA3	Účtování zdravotních služeb
PA4	Aplikační IS
POA1	Systémový HW
POA2	Systémový SW
POA3	Dokumenty
POA4	Diagnostické přístroje
POA5	Komunikační prostředky
POA6	Objekty
POA7	Lidské zdroje
POA8	Agendní systémy
POA9	Dodavatel

PA1	Zdravotní péče
PA2	Zdravotnická dokumentace
PA3	**Účtování zdravotních služeb**
PA4	Aplikační IS
POA1	Systémový HW
POA2	Systémový SW
POA3	Dokumenty
POA4	Diagnostické přístroje
POA5	Komunikační prostředky
POA6	Objekty
POA7	Lidské zdroje
POA8	Agendní systémy
POA9	Dodavatel

Zdroj: Vlastní zpracování.

Příklad souvislostí aktiv z tabulky 5 pro PA4 a POAx:

PA4 – Aplikační IS *je podporováno* POA1 – Systémový HW, POA2 – Systémový SW, POA4 – Diagnostické přístroje, POA5 – Komunikační prostředky, POA6 – Objekty, POA7 – Lidské zdroje, POA8 – Agendní systémy, POA9 – Dodavatel.

4.7.2 Hodnocení aktiv

Hodnocení aktiv dle CIA vychází z přílohy č. 1, VKB.
Hodnocení identifikovaných aktiv je prováděno řízeným a dokumentovaným postupem tak, že vezme výsledky prvního kroku dekompozice aktiv a na tomto rozsahu se provede hodnocení pro všechny 3 oblasti (důvěrnost, integrita, dostupnost) ve škále určeného hodnocení. Prvotní hodnocení aktiv provede manažer ISMS ve spolupráci s jednatelem organizace, revize hodnocení a případné změny je vhodné provádět ve spolupráci s vlastníkem příslušného aktiva. Pro potřebu diplomové práce hodnocení provedl autor na základě rozhovoru č.4 uvedeného v metodice práce.

Tabulka 6 Registr primárních aktiv ambulance VPL

ID aktiva	Název primárního aktiva	Kategorie	Specifikace	Vlastník aktiva	Osobní údaje GDPR	Legislativa	Lokalizace aktiva	Důvěrnost (C)	Integritu (I)	Dostupnost (A)	DO PAx aktiva
PA1	Zdravotní péče	služba	Zajištění poskytování zákonné a smluvní zdravotní služby občanům. Zákonné posouzení zdravotního stavu občana pro potřeby veřejné správy, ze smluvní povinnosti pro zaměstnavatele občanů, PČR, pojišťovny, soudy aj.. Zabezpečení návštěvní služby.	Lékař	ano	Zákon č. 372/2011 Sb.	Ambulance PL	4	4	4	**4**
PA2	Zdravotnická dokumentace	infromace	Bezpečné zpracovávání, ukládání a distribuce zdravotické dokumentace s dodržením GDPR. Operace s citlivými, důvěrnými infromacemi se uskutečňuje elektronicky a dokomentovou formou (analogově)	Lékař	ano	Zákon č. 372/2011 Sb. Vyhláška č. 98/2012 Sb Nařízení EU 2016/679	Ambulance PL	4	4	3	**4**
PA3	Účtování zdravotních služeb	informace	Měsíční vyučtování kapitačních plateb a zdravotnický výkonů registrovaných / neregistrovaných pacientů. Fakturace za posudkovou činnost a smluvní služby.	Lékař	ano	Vyhláška č. 134/1998 Sb.	Ambulance PL (Zdravotní pojišťovna)	2	3	2	**3**
PA4	Aplikační IS	informace	Jádrem aplikačního IS je HW, periferní zařázení, diagnostické přístroje a SW SmartMEDIX. Zpracovává zdravotnické informace. Je propojen s agendními IS přes komunikační prostředí. Ukládá, replikuje elektronickou dbf. s zdravotnickou dokumentací pacienta.	Lékař	ano	ISO 2700x ZKB a VKB Zákon č. 365/2000 Sb.	Ambulance PL (Objekty agendních systémů)	3	4	4	**4**

Zdroj: vlastní zpracování.

Identifikovaná aktiva budou pro účely řádného postupu v následně prováděné analýze rizik ohodnocena z pohledu jejich významu pro organizaci a jí poskytované služby. Hodnocení bude provedeno na škále od 1 do 4 bodů, kdy nejzávažnější KRITICKÝ dopad je hodnocen 4 body, nejméně závažný NÍZKÝ dopad 1 bodem. Stupnice vychází z přílohy č. 1 VKB. Použitá stupnice je uvedena v příloze 5 musí být aplikována na všechna primární a podpůrná aktiva organizace jednotně.

Autor pro potřeby práce zavádí hodnotu dopadu DO x-tého primárního aktiva PAx.

Pro další část práci je uvedeno vysvětlení stanovení přejímání hodnoty primárního aktiva PAx podpůrným aktivem POAx na příkladu:

Primární aktivum PA1 – Zdravotní péče má hodnotu CIA dopadu DO PA1 = 4, kdy podporujícími aktivy podle tabulka 5 jsou:

POA3 – Dokumenty;

POA4 – Diagnostické přístroje;

POA6 – Objekty;

POA7 – Lidské zdroje;

POA9 – Dodavatel;

Pro tyto podpůrná aktiva je přejata hodnotu CIA, kdy můžeme uvažovat tak, že pokud primární aktivum má hodnocen dopadu „kritický“ DO PA1=4, tak i podpůrná aktiva by měla převzít tuto hodnotu od primárního aktiva, aby nedošlo k oslabení nastavení potřebných opatření. Z toho vyplývá, že není nutné analyzovat riziko pro každé podpůrné aktivum zvlášť. V práci v kapitole 4.8.3 jsou vytvořeny „univerzální“ matice rizik s identifikovanými a ohodnocenými hrozbami Hx a zranitelnostmi Zx pro hodnoty dopadu aktiva DO = 4 a DO = 3, viz. také:

- příloha 10 - Matice rizik pro primární aktiva s hodnocením CIA DO = 4;
- příloha 11 - Matice rizik pro primární aktiva s hodnocením CIA DO = 3;
- tabulka 5 - Přehled souvislostí primárních a podpůrných aktiv.

Komparace provedené analýzy aktiv organizace pro účely bezpečnosti informací podle doporučených opatření dle ISO/IEC 27001, A.8 a PoA:

- identifikovat aktiva organizace (A.8.1) a definovat odpovědnost k jejich přiměřené ochraně – registr primárních aktiv (tabulka 6), registr podpůrných aktiv (příloha 4) a popis vztahů mezi aktivy (tabulka 5).
- klasifikovat informace a aktiva (A.8.2) v souvislosti s jejich důležitostí a s požadovanou ochranou – klasifikace aktiv dle CIA (příloha 5), manipulace a klasifikace informace dle tabulky 2 v souvislosti s GDPR.
- popsat manipulaci s médii (A.8.3), kdy manipulace (operace) s informacemi jsou uvedeny v tabulce *2*, souvislosti jsou odvoditelné z modelu zdravotní péče (obrázek 14) a schématu platformy IS (obrázek 15) a informačního toku v IS (obrázek 16)

Základní doporučená opatření normy kapitoly A.8, ISO/IEC 27001 byla komparací porovnána, splněna.

4.8 Analýza a řízení rizik

Kontext procesu managmentu rizik má být stanoven na základě porozumění externími a internímu prostředí, ve kterém organizace provozuje své činnosti, a má odpovídat specifickému prostředí činností, pro které je management rizik aplikován. Pochopení kontextu je důležité protože (ISO 31000, 2018, s. 22):

- management rizik probíhá v kontextu cílů a činností organizace;
- organizační faktory mohou být zdrojem rizika;
- účel a rozsah procesů managementu rizik může být propojen s cíli organizace jako celku.

Definice rizika podle ISO 27000 (2018), definice 3.61 – riziko je účinek nejistoty na dosažení cíle; v souvislosti s ISMS mohou být rizika bezpečnosti informací vyjádřena jako účinek nejistoty na cíle bezpečnosti informací; riziko bezpečnosti informací je spojeno s možností, že hrozby využijí zranitelnosti informačního aktiva nebo skupiny informačních aktiv, a tak způsobí organizaci škodu.

ISO/IEC 27001 specifikuje, že opatření implementovaná v rámci rozsahu, mezních hodnot a rámce ISMS je třeba založit na riziku. Aplikace procesu řízení rizik bezpečnosti informací může tento požadavek splnit. Existuje mnoho přístupů, pomocí kterých mohou být stanovena opatření k implementaci vybraných ošetření rizika (ISO 27005, 2019).

Pro přístup k analýze a řízení rizik autor zvolil metodiku MZČR a to *„Metodický pokyn poskytovatelům zdravotních služeb ke kybernetické bezpečnosti, příloha č. 9, Metodika analýzy a řízení rizik“.*(Bezouška, 2020). Dokument je součásti úložiště MZČR „Metodika kybernetické bezpečnosti“ (MZČR, 2022). Celý proces analýzy a řízení rizik je precizně graficky zachycen na obrázku 8 v teoretické části diplomové práce.

Pro řízení bezpečnosti informací je důležité stanovit výchozí rozsah systému ISMS organizace a to (Bezouška, 2020):

- rozsah ISMS je shodný s rozsahem celé organizace, kdy zahrnuje všechny procesy kontextu malé až střední velikosti organizace;
- ISMS se aplikuje pouze na určitý proces nebo informační systém, kdy zahrnujeme pouze oblast chráněného zájmu organizace a je vhodnější pro velké organizace.

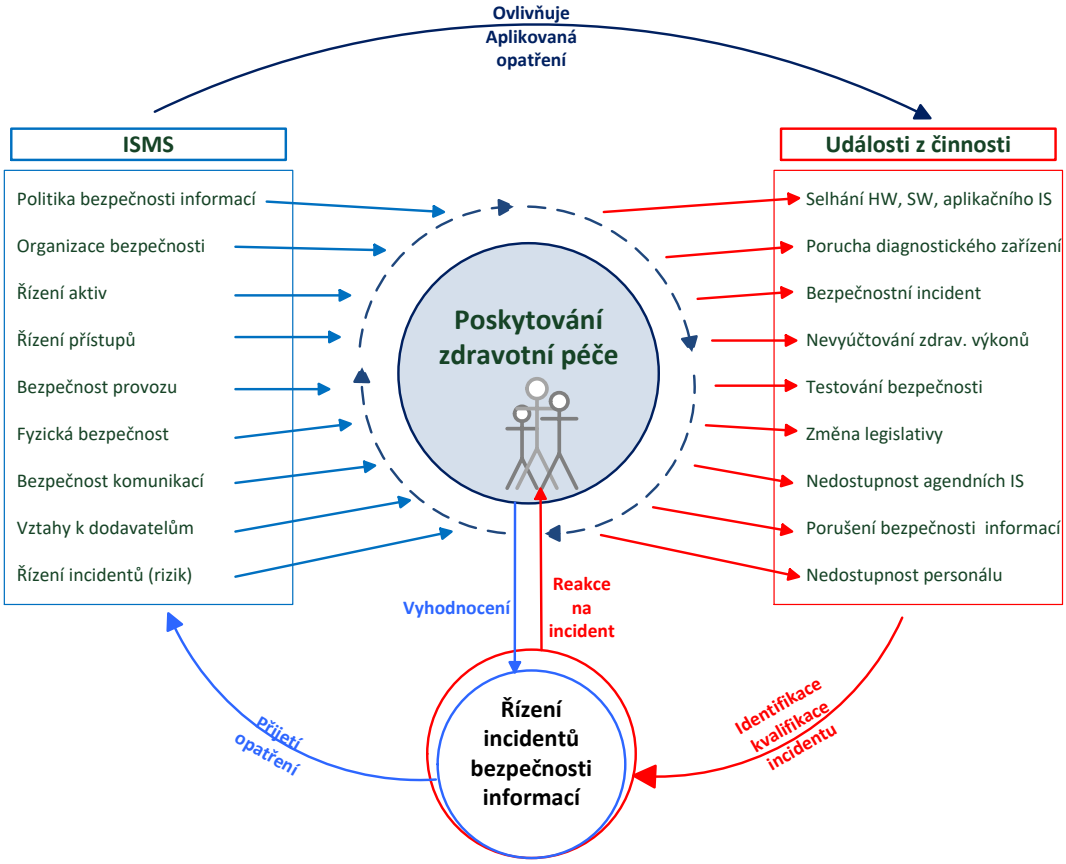
Autor pro práci vybral variantu řízení bezpečnosti informací v rozsahu celé organizace, protože v mikropodniku je provozován jeden aplikační IS s aplikačním SW a jedná se

o systematické řízení bezpečnosti informací, ochrany informací a dat zdravotnické dokumentace v elektronické a analogové podobě.

Teoreticky může být ISO/IEC 27002 aplikována i na velkou organizaci. Rozsáhlá vzájemná závislost funkcí ve zdravotnictví indikuje problematickou definici rozsahu ISMS. Ve velkých organizacích se spíše volí druhý typ, tedy parciální postupu implementace. Dosažení shody v rozsahu ISMS je vhodné zvolit jako přírůstkový a opakovaný proces, aby byla postupně aplikována norma na celou organizaci. Cílem je zajistit rovnováhu mezi „dosažitelností“ shody a přínosem pro organizaci, tedy určit počáteční minimální rozsah bezpečného poskytování služeb informační bezpečnosti.

Hodnocení rizik je mechanismus, kterým má být identifikován rámec opatření, která plní cíle opatřeními A.5 – A.18 dle ISO/IEC 27002. Tento proces analýzy rizik je rozepsán v ISO/IEC 27005.

Obrázek 19 Řízení rizik v mikropodniku



Zdroj: vlastní zpracování, ISO 27799 (2019).

Autor navrhuje řízení rizik na obrázku 19 v ambulanci jako činnost probíhající při běžné činnosti mikropodniku, kdy dochází k plnění jednotlivých opatření dle PoA, na základě

provedené analýzy rizik a stanoveného plánu zvládání rizik v souvislosti s registrem rizik. Je stanoven časový plán pro implementaci a akceptovaná výše finančních prostředku nutných k splnění opatření dle přílohy A, ISO/IEC 27001. Některá rizika s ohledem na jejich finanční, materiální, informační či organizační dopad jsou akceptovány bez aplikace bezpečnostních opatření, která by byla technicky a finančně nákladnější než újma z dopadu způsobená rizikem, podmíněná realizovanou hrozbou využívající určité zranitelnosti. V případě uskutečnění bezpečnostního incidentu, na základě reakce na incident a vyhodnocení dopadu, je realizováno navržené opatření z plánu zvládání rizik, které bylo naplánováno a akceptováno jednatelem organizace, a to neprodleně.

4.8.1 Hrozby

Hrozba má schopnost poškodit aktivum, kdy aktivem chápeme primární a podpůrná aktiva identifikované v kapitole 4.7.1. Hrozby autor analyzoval pomocí analýzy nad oblastí informační bezpečnosti kapitola 4.4, modelu zdravotní péče kapitola 4.5 a organizační bezpečnosti kapitola 4.6. Ukázka vytvořeného katalogu hrozeb je v tabulce 7. Celý katalog hrozeb je uveden v příloze 7. Hrozby byly ohodnoceny podle hodnotící stupnice uvedené v příloze 6, které jsou součástí VKB.

Tabulka 7 Ukázka katalogu identifikovaných hrozeb

Hx	Název hrozby	Hodnota Hx	Činnost, která hrozbu může naplnit
H01	Porušení bezpečnostní politiky IS.	3	Činnost uživatele a administrátora, která neodpovídá nastavenému způsobu užívání IS, operací s informací (manipulace s zdravotnickou dokumentací) a posyktování zdravotní péče. Provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administratorů.
H02	Poškození, selhání technického nebo HW vybavení.	3	Úmyslné, nezaviněné, náhodné selhání hardwarových součástí IS, diagnostických přístrojů (nevhodná manipulace, přepětí v el.síti, krádež a jiné).
H03	Poškození, selhání SW a OS.	3	Cílená snaha o narušení integrity SW, nevhodný update verze SW, chybná aktualizace OS nekompaktibilní s aplikačním SW (SmartMedix), Užívání SW třetích stran, které nejsou schváleny pro provoz v organizaci a nejsou uvedeny v bezpečnostní politice jako povolený SW může způsobit nedostupnost aplikačního IS.

Zdroj: vlastní zpracování

4.8.2 Zranitelnosti

Identifikovat zranitelnosti v rámci bezpečnosti informací znamená najít chyby a nedostatky podpůrných aktiv, ale také chybějící bezpečnostní opatření v systému řízení bezpečnosti informací uvedené v PoA. Právě opatření v prohlášení o aplikovatelnosti je vstupní informace pro identifikaci hrozeb, kdy autor pomocí analýzy (kapitola 4.4) identifikoval možné zranitelnosti v souvislosti s modelem zdravotní péče (kapitola 4.5) a organizační bezpečností (kapitola 4.6) v souvislosti s hrozbami (kapitola 4.8.2). V organizaci byly identifikovány zranitelnosti uvedené v příloze 8. Ukázka zranitelností je v tabulce 8.

Tabulka 8 Ukázka katalogu zranitelností

Zx	Název zranitelnosti	Hodnota Zx
Z01	Nedostatečné provádění a vyhodnocování auditů, preventivních a servisních kontrol.	2
Z02	Nedostatečné stanovení bezpečnostních pravidel, práv a povinností uživatelů, administrátorů a bezpečnostních rolí.	3
Z03	Nevhodné nastavení přístupových oprávnění.	3
Z04	Nedostatečná ochrana a správa aktiv.	3
Z05	Přístupnost papírové dokumentace na pracovišti.	3
Z06	Nedostatek identifikace a autentizace odesílatele a příjemce informací.	4

Zdroj: vlastní zpracování

4.8.3 Matice rizik

Matice rizik v tabulce 9 je výsledkem výpočtu míry rizika kvalitativní metodou. Pro potřeby práce hodnocení míry rizika autor stanovil hodnotící stupnici (stupnice hodnocení dopadu rizik), kdy podle intenzity rizika jsou definovány čtyři intervaly, a to úrovně (upraveno dle VKB, příloha 2, tabulka 3):

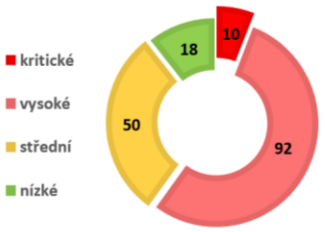
- nízké – intervalu míry 1-16, riziko je považováno za akceptovatelné;
- střední – intervalu míry 17-32, riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné;
- vysoké – intervalu míry 33-48, riziko je dlouhodobě nepřístupné a musí být zahájeny systematické kroky k jeho odstranění;

- kritické – intervalu míry 49–64, riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.

Tabulka 9 Matice rizik pro primární aktivum PA s dopadem DO = 4.

MATICE RIZIK PAx pro DO = 4

ROZLOŽENÍ HODNOCENÍ RIZIK



ID	Kategorie hrozeb	Hx /Zx	Z01 Nedostatečné provádění a vyhodnocování auditů, preventivních a servisních kontrol.	Z02 Nedostatečné stanovení bezpečnostních pravidel, práv a povinnosti uživatelů, administrátorů a bezpečnostních rolí.	Z03 Nevhodné nastavení přístupových oprávnění.	Z04 Nedostatečná ochrana a správa aktiv.	Z05 Přístupnost papírové dokumentace na pracovišti.	Z06 Nedostatek identifikace a autentizace odesílatele a příjemce informací.	Z07 Nedostatečná ochrana vnějšího perimetru.	Z08 Nevhodná fyzická ochrana budovy, prostorů ambulance, kontroly vstupů osob.	Z09 Nedostatek kontroly aktiv mimo objekt.
ID	Kategorie zranitelnosti		2	3	3	3	3	4	3	2	2
H07	Nedostupnost služby poskytované aplikačním IS.	3	24		36						
H08	Nedostupnost komunikačních služeb.	2	16			24			24	16	
H09	Neoprávněná modifikace informací v aplikačním IS.	2		24	24	24					16
H10	Ztráta, zneužití certifikátu s heslem.	2			24	24		32			16
H11	Zneužití, porucha přenosných nosičů dat.	3			36	36				24	24
H12	Nedostupnost technické a softwarové pomoci dodavatelů.	2					24		24		
H13	Nedostupnost agendních IS.	3						48			
H14	Ztráta, poškození, odcizení elektronické zdravotní dokumentace.	4	32	48	48	48		64	48		32
H15	Ztráta, poškození, odcizení papírové zdravotní dokumentace.	4	32			48	48	64	48	32	32

Zdroj: vlastní zpracování

Funkce výpočtu míry rizika v matici rizik

Pro výpočet hodnoty jednotlivých rizik je užita funkce podle VKB (2018, str. 1141), kde Riziko = Dopad × Hrozba × Zranitelnost. Pro potřeby diplomové práce definujeme:

- hodnotu dopadu DO jako hodnotu *k-tého* primárního aktiva PAk;
- hodnotu hrozby jako hodnotu *í-té* hrozby Hi;
- hodnotu zranitelnosti jako hodnotu *j-té* zranitelnosti Zj;

Výpočet hodnoty *x-tého* rizika $Rx_{i,j}$ definujeme funkcí:

$$Rx_{i,j} = PAk \times Hi \times Zj \text{ , kde} \qquad \text{(vzorec 1)}$$

i = 1,..,23 pro jednotlivá *Hi; j = 1,..,16* pro jednotlivá *Zj*; *k = 1,..,4* pro jednotlivá *PAk*.

Tabulka 9 je ukázkou matice rizik pro primární aktivum s hodnotami jednotlivých identifikovaných rizik $Rx_{i,j}$. Celá matice rizik pro DO = 4 je uvedena v příloze 10, kde výpočet míry rizika pro primární aktivum PA1 – zdravotní péče, PA2 – zdravotnická dokumentace a PA3 – aplikační IS, která mají stanoven kritický stupeň míry dopadu hodnocení dle CIA a to DO = 4. V tabulce je zobrazen graf ukazující celkový počet identifikovaných rizik, kdy 10 rizik je kritických a 92 rizik je zařazeno mezi rizika vysoká. Celkem bylo identifikováno 170 rizik s různou mírou intenzity. Matice rizik pro primární aktivum PA3 – účtování zdravotních služeb je uvedena v příloze 11.

4.8.4 Registr rizik

Registr rizik uvedený v tabulce 10 obsahuje 19 vybraných rizik identifikovaných na základě analýzy rizik. Pro orientaci autor uvádí interpretaci vytvořeného registru na riziku **R3 – Nedostupnost diagnostických přístrojů**:

- odpovědná osoba – jednatel;
- scénář rizika – nesplnění povinných kalibrací a revizí diagnostických zařízení, nenasmlouvání výkonů u zdravotních pojišťoven, neproškolený personál.
- CIA – porušení integrity a dostupnosti;
- aktivum – související aktivum, na které působí riziko (PA1 – zdravotní péče, PA – 4 aplikační IS);
- identifikovaná souvislost působení hrozby a zranitelnosti – H17 (CIA=2) – manipulace/operace s zdravotnickou dokumentací, Z12 (CIA=4) – nedostatek odborného personálu;
- hodnota dopadu – DO=4, hodnota dopadu je převzata z hodnoty PA1;
- významnost a hodnota rizika – výpočtem podle vzorce 1 je R3 = 48, což znamená vysoké riziko, které bude nutno posoudit, ošetřit opatřením a následné po opětovném posouzení modifikovat, zachovat riziko nebo akceptovat;
- opatření dle PoA – aplikovat opatření dle ISO/IEC 27002 č.A.8.1, A.11.2.1 - A.11.2.5;
- interpretace dopadu – z nedostatku nasmlouvaného revizního technika a propadnutí revize na diagnostickém přístroji, nelze využívat diagnostický přístroj pro poskytování zdravotní péče.

Tabulka 10 Registr rizik pro potřeby DP

Riziko	Odpovědná osoba	Název rizika	Scénář	CIA	Aktivum	Matice rizik		Hodnota dopadu	Významnost hodnota rizika	Opatření dle PoA	Interpretace dopadu Hx a Zx
						Hozba	Zranitelnost				
R1	Jednatel	Porušení integrity hardware.	Porušení integrity pracovních stanic, technického vybyvení a periferiních zařázení důsledkem poruchy, havárie, fyzického opotřebení, ztráty, krádeže.	integrita, dostupnost	PA1, PA4	H02=3	Z07=3	4	vysoké R1=36	A.5.1.1, A.6.1.1, A.7.1.1, A.7.2.2, A.11.1.1 - A.11.1.4, A.11.2.1	Z důvodu narušení fyzické bezpečnosti objektu došlo ke krádeži HW vybavení.
R2	Administrator	Porušení integrity software.	Selhání programového vybavení, neprovádění bezpečsnotních aktualizací OS a SW, užívání nelegální licence SW, kybermetický útok.	integrita, dostupnost	PA1, PA2, PA4	H01=3	Z03=3	4	vysoké R2=36	A.5.1.1, A.6.1.1, A.9.1.1, A.9.2.2, A.9.2.5, A.9.4.3, A.9.4.4, A.12.1.2, A.12.4.1, A.12.5.1, A.12.6.2	Z důvodu nevhoného nastavení práv uživatele, došlo k porušení bezpečnostní politiky a uživatel narušil integritu SW nebo SW odinstaloval / neschválený SW nainstaloval.
R3	Administrator	Nedostupnost informací v IS.	Porušení smlouvy outsorcingových služeb pro aplikační SW, výpadky elektrické energie, porucha nebo krádež HW (pracovní stanice, notebooku), chybně nastavená archivace dat, kybernetický útok.	důvěrnost, integrita, dostupnost	PA2, PA3, PA4	H05=4	Z12=4	4	kritické R3=64	A.6.1.1, A.6.2.1, A.6.2.2, A.8, A.9.1.1, A.9.2.1, A.9.2.2, A.9.4, A.10.1.1, A.11.1.1, A.12, A.13.2, A.15.1, A.17.1, A.18.1.2.	Z důvodu kybernetického útoku na aplikační IS došlo k nedostupnosti informací v IS. Je nutný zásah specialisty, který není zaměstnancem organizce.
R4	Jednatel	Nedostupnosti agendních IS.	Výpadek služeb eRecept, eNeschopenka, portálů ZP, ČSSZ, aj. může být způsobeno nedostupností připojen do internetu, neplatnám certifikátem poskytovatele zdravotní péče, výpadkem služby u provozovatele služby.	integrita, dostupnost	PA1, PA2, PA3, PA4	H07=3	Z03=3	4	vysoké R4=36	A.9.1, A.9.2.1, A.9.4.1, A.9.4.2, A.11.2.2, A.12.2.1, A.13.1, A.13.2,A.18.1.1,	Zdůvdu chybného nastavní přístupových oprávnění v aplikačním IS došlo k nedostupnosti agendních IS. Např. není možné vystavit eRecept.
R5	Jednatel	Nedostupnosti diagnostický přístojů.	Nesplnění povinných kalibrací a revizí diagnostických zařízení, nenasmlouvání výkonů u zdravotních pojišťoven, neproškolený personál.	integrity, dostupnosti	PA1, PA4	H17=2	Z12=4	4	střední R5=32	A.8.1, A.11.2.1 - A.11.2.5	Z nedostaku nasmlouvaného revizního technika a propadnutí revize na diagnostickém přístroji, nelze využívat diagnistický přístroj pro poskytování zdravotní péče.
R6	Administrátor	Narušení bezpečnosti komunikačního prostředí.	Ztráta či krádež identity elektronického certifikátu pro elektronickou komunikaci, kybernetický útok, malware, havárie síťového prvku firewalu, aj.	důvěrnost, integrita, dostupnost	PA2, PA3, PA4	H05=4	Z07=3	4	vysoké R6=48	A.5.1.1, A.6.1.1, A.7.2.1, A.9.4.2, A.9.4.3, A.10.1, A.12.2.1, A.12.4.1, A.12.6, A.13, A.14.1.	Z důvodu nedostatku nastavení fiirewalu a routeru, kybernetický útok vedl k porušení integrity nastavení a dostupnosti komunikačního prostředí.
R7	Administrator	Nedostupnosti konektivity.	Výpadek telefonní sítě, nedostupnost připojení k internetu, porucha interní LAN.	dostupnost	PA2, PA3, PA4	H21=2	Z07=3	4	střední R7=24	A.11.2.1 - A.11.2.5, A.13.1, A.15.1, A.16.1, A1.7.1.	Nedostatečná opatřeně k hrozbě výpadek elektrické energie způsobil vypnutí aktivních prvků zabezpečující komunikační připojení.
R8	Jednatel	Narušení fyzické bezpečnosti objeku.	Vloupání, požár, vytopení objektu, nezastřežení EZS, nezamčení objektu, ztráta hesla od EZS a klíčů do onjektu.	důvěrnost, integrita, dostupnost	PA1, PA2, PA4	H15=4	Z11=4	4	kritické R8=64	A.6.1.1, A.7.1, A.11.1, A.16.	Z důvodu neaktivování EZS došlo k úspěšnému vloupání a odcizení volně přístupných dat a dokumentů, které nebyly uloženy uzamykatelném objektu (kartotéce).
R9	Jednatel	Technické havárie.	Může být idikováno výpadkem elektrické energie, zdroje vody, vytápění. Havárie může byt způsobena zahořením, požárem, poškození vodou, elektrickým proudem.	integrita, dostupnost	PA1, PA2, PA4	H23=4	Z04=3	4	vysoké R9=48	A.7.2.2, A.11.1.1, A.11.2.2, A.12.1.1, A.16.1.5.	Technická havárie způsobila nedostupnost posyktování zdravotní péče v souvislosti s nedostupmostí aplikačního IS, diagnostických přístrojů a přístup k datům v IS.
R10	Jednatel	Porušení povinností uživatele IS.	Sdělení hesla k uživatelskému účtu neoprávněné osobě, provádění nevhodných technik vedoucích k narušení integrity aplikačního IS,zneužití identity jého uživatele, operace v IS vedoucí ke ztrátě zdravotnických informací či modifikaci aj.	důvěrnost, integrita, dostupnost	PA2, PA4	H14=4	Z14=3	4	vysoké R10=48	A.5.1.1, A.6.1.1, A.6.2.1, A.6.2.2, A.8.1.3, A.8.2, A.9.4.1, A.9.4.2, A.12.3.1, A.12.4.1, A.12.6.2, A.14.1.3, A.16.1.2, A18.1.4.	Uživatel se dopustil bezpečnostního incidetu, kdy se řádně neodhlásil z IS a umožnil neorávněné osobě operace s daty v aplikačním IS.

Riziko	Odpovědná osoba	Název rizika	Scénář	CIA	Aktivum	Matice rizik		Hodnota dopadu	Významnost hodnota rizika	Opatření dle PoA	Interpretace dopadu Hx a Zx
						Hozba	Zranitelnost				
R11	Administrátor	Bezpečnostní incidet v aplikačním IS.	Událost, která veden k porušení CIA v souvisloti s bezpečsnotní politikou IS organizace.	důvěrnost, integrita, dostupnost	PA4	H01=3	Z11=4	4	kritické R11=48	A.5.1.1, A.6.1.1, A.7.1.2, A.7.2, A.8, A.9.1.1, A.9.2, A.9.4, A.11, A.12, A.13, A.14.1, A.15.1,A.16, A.18.2.1.	Neopravněnou operací uživatele s daty (zdravotnickou dokumnetací) / internímí dokumenty došlo k úniku důvěrných / citlivých informací.
R12	Jednatel	Omezení poskytování zdravotní péče.	Souvisí se všemi činostmi hlavního aktiva zdravotní péče vedoucích s narušení integrity a dostupnosti poskytovaných služeb.	integrita, dostupnost	PA1, PA2	H13=3	Z06=4	4	kritické R12=48	A.5.1.1, A.6.1.1, A.6.1.3, A.6.1.3, A.7, A.8, A.9, A.10, A.11, A.12, A.13, A.14.1.3, A.16, A.17, A.18.	Lékař nemá platný kvalifikovaný certifikát, který způsobí nedostupnost služby eRecept a omezení poskytování zdravotní péče.
R13	Jednatel	Nedostupnost outsorcingu aplikačního SW.	Smluvně nezabezpečený vývoj, provoz a aktualizace aplikačního SW (SmartMEDIX) včetně nedostupnosti helpdesku pro pomoc lékaři a řešení technických problému.	důvěrnost, integrita, dostupnost	PA4	H05=4	Z16=2	4	vysoké R13=32	A.15.1, A.15.2, A.17.1.1, A.18.2.1.	IS po kybernetickém útoku je nedostupný. Smlouva poskytování outsocing smluvně neobsahuje řešení této události.
R14	Lékař	Ztráta, krádež zdravoních karet pacientů.	Porušení řádného vedení papírové dokumentace zdravotní karty pacienta, archivace, ztráta, krádež. Souvisí s manipulací dokumentace a opatření k zajištění zákonných povinností.	důvěrnost, integrita, dostupnost	PA1, PA2	H17=3	Z05=3	4	vysoké R14=36	A.5.1.1, A.6.1.1, A.7.1, A.7.2.2, A.8.1.2, A.8.1.3, A.8.2, A.9.1, A.11.1.1, A.11.1.3, A.11.2.9, A.12.1, A.16.1, A.17.1A.18.1.1.	Došlo ke ztratě zdravotní dokumentace, s kterou je v ordinační době v ambulanci manipulováno - riziko odcizení karty neoprávněnou osobou.
R15	Lékař	Porušení platné legislativy	Nedodržení zákonných , legislativních norem a bezpečnostní politiky organizace, které může způsobit porušení CIA, finanční strátu nebo incident v ISMS.	integrita, dostupnost	PA1, PA2, PA3, PA4	H14 =4	Z11=4	4	kritické R15=64	A.5.1.1, A.6.1.1, A.9.1, A.10.1.1, A.12.1, A.15, A.16.1, A.18.1, A.18.2	Nedodržení opatření ve smyslu GDPR a nastavených operací výměny dat zabezpečenou elektronickou komunikací.
R16	Lékař	Neoprávněného nakládání s elektronickou zdravotnickou dokumentací.	Porušení bezpečnostních opatření IS, při manipulaci související se zákonnými povinostmi (operace se zdravotní dokumentací) výkonu činnosti poskytovatele zdravotní péče.	důvěrnost, integrita, dostupnost	PA1, PA2, PA3, PA4	H04=3	Z06=4	4	vysoké R16=48	A.5.1.1, A.6.1.1, A.6.2.1, A.7.2.2, A.8.1.2, A.8.1.3, A.8.2, A.9.1, A.9.2, A.11.2.9, A.13.2, A.14.1.	Došlo k zneužití cízí elektronické indenty při výměně zdravotnických dat v souvislosti s neoprávněným sdělením zdravotních informací třetí osobě bez možnosti ověření identity.
R17	Jednatel	Ztráty elektronického certifikátu.	Ztráta osobního hesla k elektronickým certifikátům, ztráta elektronických klíčů, zneužití kvalifikovaného a komerčního certifikátu neoprávněnou osobou, aj.	důvěrnost, integrita	PA2, PA4	H11=3	Z11=4	4	vysoké R17=48	A.8.1,A.9.2.1, A.9.2.2., A.9.4.1 - A.9.4.3, A.10.1, A.13.2.2, A.13.2.3A.14.1.2.	Došlo k zneužití přenostného záznamového média, na kterém byl zálohován elektronický certifikát (certifikát), který byl kompromitován.
R18	Lékař	Integrity účtování zdravotních výkonů.	Chybně vykazované provedené zdravotnické výkony, neodeslání měsíčního vyučtování zravotním pojišťovnám, neuznání (neproplacení) účtovaných pateb zdravotní pojišťovnou, neuzavření smlouvy se zdravotní pojišťovnou.	integrita	PA3	H23=4	Z16=2	3	střední R18=24	A.8.1.1 - A.8.1.3, A.9.2.2, A.11.2.2, A.12.1, A.13.2, A.14.1, A.15.1.	Poskytovatel zdravotní péče neuzavřel (neaktualizoval) smlouvu se zdravotní pojišťovnou. Nelze vykazovat zdravotní výkony.
R19	Jednatel	Úniku interních informací.	Zaměstnanci z firmy vynesou smlouvy, interní postupy, know-how, dokumentaci o informační bezpečnosti, selhání účtování zdravotních služeb.	důvěrnost, integrita, dostupnost	PA4	HO1=3	Z15=2	4	střední R19=24	A.5.1.1, A.6.1.1, A.6.1.2, A.6.2.1, A.8.1.3, A.8.2.3, A.8.3.2, A.9.1.1, A.9.2, A.9.4, A.11.2.7, A.13.2. A.15.1.1.	Z důvodu neprovedení školení z bezpečnosti informací došlo k porušení bezpečsnotní politiky organizace.

Zdroj: vlastní zpracování

4.8.5 Posouzení dopadu

Podle ISO/IEC 27005, přílohy B.3 pro posouzení dopadu platí, že incident bezpečnosti informací může ovlivnit více než jedno aktivum nebo jenom část aktiva. Dopad může mít buďto okamžitý (provozní) účinek nebo budoucí (podnikatelský) účinek, který zahrnuje finanční a tržní následky. Autor v mikropodniku analyzoval **oblasti dopadu**(vlastní):

- **ochrana osobních údajů pacienta** – porušení CIA ochrany osobních a zdravotních informací pacientů, porušení politiky GDPR, náklady na obnovu a zálohování;
- **zákonné a smluvní povinnosti** – porušení smluvních vztahů dle právní rámec poskytování zdravotní péče (kapitola 4.2) může vést k uzavření ambulance VPL;
- **provoz aplikačního SW** – oblast dopadu porušení CIA aplikačního SW, které implikuje omezení na všechna primárních aktiv, náklady na instalaci a obnovení dat;
- **provoz HW** – nedostupnost elektrické energie, porucha, poškození či krádež HW vyžaduje aplikaci dalších opatření a finančních nákladů – vliv na primární aktiva;
- **dostupnost zdravotnických dat** – porušení CIA provozu IS, ochrany osobních údajů, komunikačního prostředí, kdy může mít vliv na poskytování zdravotní péče;
- **komunikační prostředí** – porušení CIA připojení do internetu, neplatný digitální certifikát, nedostupné agendové registri, porucha – kybernetický útok na síťový prvek;
- **narušení běžné činnosti** – nedostupnost personálu, IS, informací a technická havárie;
- **bezpečnost a zdraví občanů** – porušení CIA manipulace s důvěrnou informací;
- **finanční ztráty** – pokuta za porušení GDPR, náklady na odstranění kybernetického incidentu, nedostupnost účtování zdravotních výkonů v IS, porušení smluvních vztahů;
- **ztráta důvěrnosti APL** – špatná pověst mezi pacienty má vliv na odregistrování pacientů, a to vede k nižším finančním ziskům, ztrátě pověsti a důvěry u obchodních partnerů;
- **nedostupnost diagnostických přístrojů** – neprovádění pravidelných revizí a kalibrací, nenasmlouvání zdravotních výkonů a přístrojů u ZP;
- **personální zabezpečení ambulance** – nemoc personálu, výpověď zaměstnance, odborné znalosti a nedostatečné vzdělávání, lékař musí být členem ČLK;
- **fyzická bezpečnost prostoru organizace** – vloupání, požár, nefunkční EZS;
- **dopad na uživatele IS a KS** – kybernetický útok, blokace účtu, ztráta přihlašovacích údajů do IS, prolomení bezpečnosti IS, neplatnost uživatelského certifikátu.

4.8.6 Ošetření a akceptace rizik

Účelem ošetřování rizika je vybrat a implementovat možnosti opatření pro jeho řešení, tedy akceptaci rizika. Ošetřování rizik zahrnuje soustavně se opakující:

- formulování a výběru možností ošetřování rizika;
- plánování a implementování ošetřování rizika (rizik);
- posuzování efektivnosti tohoto ošetřování;
- rozhodování, zda je zbytkové riziko přijatelné;
- pokud není přijatelné, přijmutí dalšího ošetřování.

Volba nejvhodnější možnosti k ošetřování rizika zahrnuje vyvažování potenciálních přínosů odvozených v souvislosti s dosažením cílů proti nákladům, úsilí nebo nevýhodám implementace (ISO 31000, 2018, s. 24). Návrh opatření k ošetření rizik jednotlivých cílů PoA je uvedeno v příloze 12 s popisem vlastních navrhnutých opatření.

Aplikace opatření k ošetření rizika provedené podle plánu zvládání rizik vychází z registru rizik s určeným termínem splnění těchto opatření. Po aplikaci je nutné efektivitu opatření k snížení rizika znovu posoudit, jak ilustruje obrázek 8 - Proces řízení rizik bezpečnosti informací. Ošetření rizika obsahuje cyklický proces (ISO 27005, 2019, s. 10):

- posouzení ošetření rizika;
- rozhodnutí, zda jsou úrovně zbytkového rizika akceptovatelné;
- generování nového ošetřeného rizika v případě, že úroveň rizika nejsou akceptovatelné;
- posouzení efektivity tohoto ošetření.

Součástí **akceptace rizika** dle ISO 27005 (2019, kap. 9) je zachovávání rizika, akceptování zbytkového rizika, sdílení rizika nebo modifikace rizika, kdy úroveň rizika by měla být spravována zavedením, odstraněním nebo pozměněním opatření, aby zbytkové riziko mohlo být znovu posouzeno jako akceptovatelné. S výběrem opatření pro implementaci s cílem snížení rizika je potřeba brát v úvahu omezení např. časová, technická, finanční, provozní, personální aj.

4.8.7 Řízení rizika

Autor v mikropodniku navrhl řízení rizik na základě identifikace rizika, aplikace opatření a akceptace ošetření rizika, kdy pro vysvětlení je užito příkladu, který užívá znalostí z matice rizik v tabulce 9, zpracovaného registru rizik uvedený v tabulce 10 a opatření dle ISO/IEC 27002 v souvislosti s PoA uvedená v příloze 12.

Příklad interpretace řízení rizika R12 na primární aktivum PA1 způsobené hrozbou H13 a umožněné zranitelností Z06, a následné ošetření a akceptace.

Riziko

- *R12 – omezení poskytování zdravotní péče.*

Hodnota dopadu DO $R12_{13,6}$ = 48 pro PA1 – zdravotní péče (služba), CIA = 4;

- *hrozba H13* (nedostupnost agendních systémů) CIA=3;
- *zranitelnosti Z06* (nedostatek identifikace a autentizace odesílatele a příjemce informací) CIA=4.

Dopad

Oblasti dopadu:

- zákonné a smluvní povinnosti;
- provoz aplikačního SW;
- komunikační prostředí;
- narušení běžné činnosti.

Interpretace dopadu:

- nedostupnost (nevyužití) služby datové schránky neumožňuje řádně identifikovat odesílatele a příjemce zdravotní dokumentace pacienta v informačním toku s externím subjektem, využití jiného způsobu elektronické komunikace (běžný email) existuje riziko porušení důvěrnosti a integrity osobních údajů a porušení zákonných povinností.
- ukončení platnosti kvalifikované certifikátu lékaře, kde důsledkem je nemožnost ověření identity poskytovatele zdravotní péče, způsobí nedostupnost agendy eRecept pro vystavení předpis léků, je narušena integrita aplikačního SW, dostupnost a důvěrnost připojení do agendového registru.

Opatření k ošetření rizika

Doporučená opatření k snížení a akceptaci rizika podle ISO/IEC 27002 vycházející z tabulky 10 a návrhu vlastních opatření splnění PoA: A.5.1.1, A.6.1.1, A.6.2.1, A.6.2.2, A.7.2.1, A.8, A.9.1.1, A.9.2.1, A.9.2.2, A.9.2.5, A.9.4.1 - A.9.4.4, A.10.1, A.11.1.1, A.11.2.1 - A.11.2.5, A12.1.2, A.12.2.1, A.12.4.1, A.12.5.1, A.12.6, A.13, A.14.1, A.15.1, A.16.1, A.17.1, 18.1.1, A.18.1.2.

Zajištění kontinuity

Pro případ selhání opatření cílů PoA (incident bezpečnosti IS) je nutné zpracovat plán kontinuity IS řízení bezpečností informací. Vybrané návrhy jsou uvedeny v příloze 14. Zajištění kontinuity poskytování zdravotních služeb pro riziko R12 podporuje:

- implementovat postup, kdy elektronickou zdravotnickou dokumentaci lékař zašifruje šifrovacím certifikátem nebo verifikuje elektronickým certifikátem odesílajícího lékaře a zašle na ověřenou emailovou adresu příjemce nebo zašle vytištěnou a signifikovanou zdravotní dokumentaci formou doporučeného dopisu, kurýrem.
- do bezpečnostní dokumentace zavést povinnost vyžádat nový elektronický certifikát u certifikační autority měsíc před ukončením jeho platnosti; z důvodu nedostupnosti konektivity do agendního systému eRecept lékař vystaví předpis na léky na papírový formulář Recept.

Závěr příkladu

Ošetření rizika na základě aplikovaných opatření a nastavení kontinuity běžné činnosti, vede k snížení hodnoty dopadu rizika na přijatelnou úroveň. Hovoříme pak o akceptaci rizika nebo riziko jsme modifikovali (více v kapitola 4.8.6).

V provedené analýze rizik, autora zaujala souvislost mezi hodnotami dopadu rizik $Rx_{i,j}$ pro jednotlivé hrozby Hx_i. V této souvislosti byl proveden výpočet průměrů hodnot dopadů rizik pro jednotlivé hrozby. Výsledek je uveden v tabulce 12, kde jsou hrozby hodnoceny procentuální mírou. Hodnota znamená procentuální míru hodnocení dopadu rizik dané hrozby neboli míra vyjadřuje průměrný dopad uskutečněné hrozby.

Příklad: H23 – neposkytování zdravotní péče je hrozba s největší hodnotou dopadu rizika a to 75 %. Hrozba H23 využívá 6 typů zranitelností (matice rizik viz. příloha 10):

Z04 – nedostatečná ochrana a správa aktiv;

Z05 – přístupnost papírové dokumentace na pracovišti;

Z06 – nedostatek identifikace a autentizace odesílatele a příjemce informací;

Z10 – nedostatek procesů účtování výkonů zdravotní péče;

Z12 – nedostatek odborného personálu;

Z16 – nedostatek právní formulace uzavření dodavatelské smlouvy.

Maximální dosažitelná hodnota rizika je 64 tedy 100 % (stupnice hodnocení dopadů rizik). Hodnoty jednotlivých rizik sečteme 48+48+64+32+64+32 a vydělíme počtem zranitelností, které hrozba využívá a to 6. Výsledná hodnota rizika je 48, což je 75% hodnoty maximálního rizika. Výsledkem analýzy rizik v souvislosti s analyzovanými hrozbami autor analyzoval:

Hrozby související s hlavní činností mikropodniku – pro poskytování zdravotní péče (PA1 – zdravotní péče) je nutné přijmout opatření ke snížení účinků rizik plynoucích

z hrozeb, kdy je nutné pro rizika s mírou vyšších než 50 %, vysoká až kritická rizika, aplikovat opatření neodkladně.

Opatření k ošetření rizik (snížení dopadů rizik) jsou v této práci součástí registru rizik, kde jsou identifikovány související nutná popatření dle ISO/IEC 27001, příloha A. **Plán zvládání rizik** vychází z registru rizik. K plnění jednotlivých opatření k ošetření rizik je stanoven termín implementace v organizaci. Jednotlivá opatření ke splnění jednotlivých cílů ISO/IEC 27002 jsou uvedena v příloze 12 - PoA s popisem vlastních navrhnutých opatření dle metodiky ISO/IEC 27002 a související s uvedenými opatřeními ke snížení rizika v registru rizik v tabulce 10.

Tabulka 11 Míra rizika účinků hrozby působící na aktiva

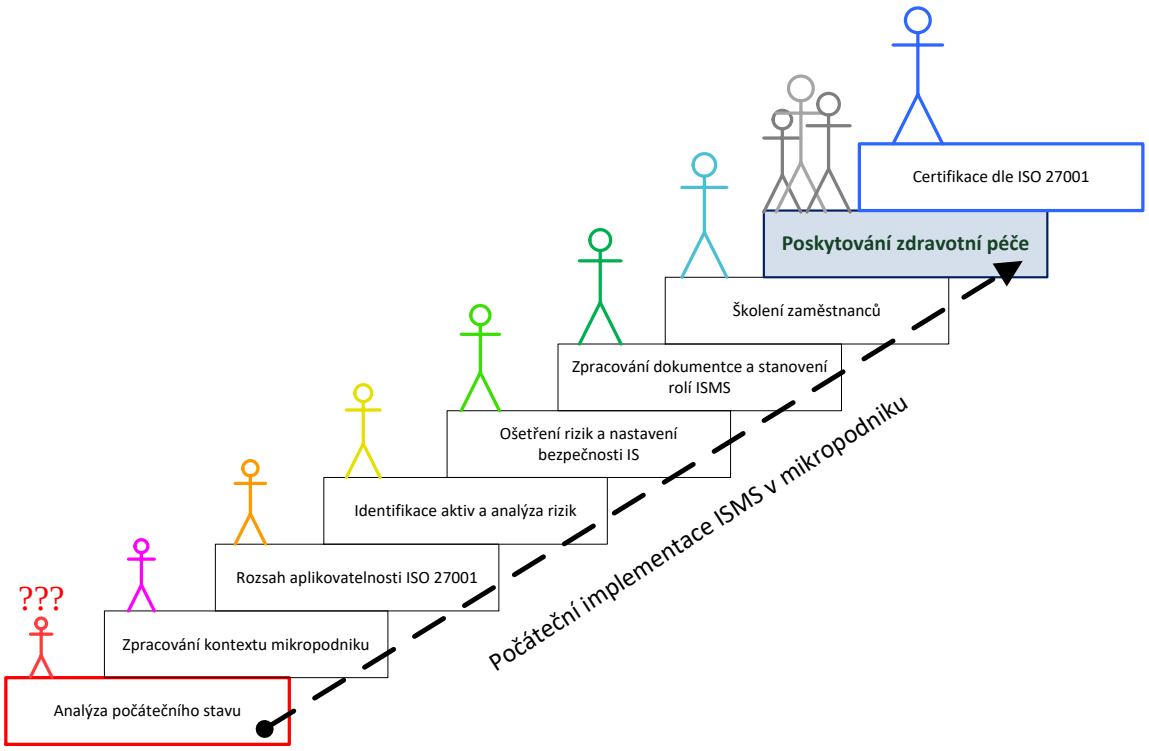
ID Hx	Kategorie hrozby	Míra rizika	Počet Zx
23	Neposkytování zdravotní péče	75,0%	6
5	Kybernetický útok z vnější komunikační sítě.	69,2%	13
15	Ztráta, poškození, odcizení papírové zdravotní dokumentace.	67,5%	10
14	Ztráta, poškození, odcizení elektronické zdravotní dokumentace.	67,3%	13
6	Škodlivý kód.	64,3%	7
4	Zneužití identity jiné fyzické osoby.	58,6%	8
13	Nedostupnost agendních IS.	56,3%	4
17	Manipulace / operace s zdravotnickou dokumentací.	56,3%	8
3	Poškození, selhání SW a OS.	51,6%	12
20	Porucha či nedostupnost tiskových a skenovacích zařízení.	51,6%	4
1	Porušení bezpečnostní politiky IS.	50,9%	14
11	Zneužití, porucha přenosných nosičů dat.	50,9%	7
7	Nedostupnost služby poskytované aplikačním IS.	48,8%	5
2	Poškození, selhání technického nebo HW vybavení.	47,9%	9
18	Narušení fyzické bezpečnosti.	43,8%	6
22	Nedostupnost replikace databáze aplikačního IS.	42,2%	4
12	Nedostupnost technické a softwarové pomoci dodavatelů.	37,5%	4
19	Nedostupnost služeb zdravotní pojišťovny.	37,5%	5
10	Ztráta, zneužití certifikátu s heslem.	34,4%	8
16	Neprovedení revize technických a diagnostických zařízení .	34,4%	4
9	Neoprávněná modifikace informací v aplikačním IS.	33,3%	9
21	Porucha dodávek elektrické energie,vody, vytápění.	33,3%	3
8	Nedostupnost komunikačních služeb.	32,1%	7

Zdroj: vlastní zpracování

4.9 Návrh metodiky bezpečnosti IS v mikropodniku

Základem metodiky je plán zavedení bezpečnosti informací dle ISO/IEC 27001 s vybranými opatřeními ISO/IEC 27002 a užitím opatření k plnění GDPR. Tato metodika poskytuje doporučení a navrhuje postup počáteční implementace ISMS v mikropodniku, který vidíme na obrázku 20, s cílem nastavit procesy řízení bezpečnosti a ošetření rizik informačního systému mikropodniku.

Obrázek 20 Návrh metodiky bezpečnosti IS v mikropodniku



Zdroj: vlastní zpracování

Metodika je navrhnuta ve formě postupných kroků, které byly v praktické části této práce analyzovány a interpretovány dle výše uvedených norem a legislativy. Vysvětlení jednotlivých kroků v metodice je realizováno odkazy do norem, jednotlivých kapitol této práce a konkrétními návrhy řešení. Metodika, je vlastní návrh autora k řešení bezpečnosti IS v mikropodniku – ambulanci všeobecného praktického lékaře.

4.9.1 Analýza počátečního stavu

- identifikovat data, informace a procesy mikropodniku;
- popsat stávající stav (způsob) zpracovávání informací v mikropodniku a manipulace s listinnou dokumentací;
- určit účel užívání počítačů, periferních zařízení, mobilních IT zařízení, diagnostických přístrojů, portálů veřejné správy, přístupů do agendových IS v mikropodniku;
- shromáždit dostupnou dokumentaci o zabezpečení objektu, revizích, personálu, smlouvách s dodavateli, nájemními smlouvami, o technologických zdrojích, dokumentace o plnění opatření souvisejících s GDRP, BOZP aj.;
- stanovit počáteční stav IS, kde zkoumáme – zastaralost HW, verze SW, provádění aktualizací, zálohování, funkčnost periferních zařízení, stav vnitřní LAN, připojení do internetu a nastavená opatření bezpečnosti informací.

4.9.2 Zpracování kontextu organizace

- porozumění vnitřním procesům organizace – model zdravotní péče (kap. 4.5.1);
- pochopení prostředí a okolí vykonávané činnosti organizace (kap. 4.3);
- zpracování základní analýzy organizace s ohledem na provoz IS a bezpečnost informací formou auditu (kap. 4.4);
- porozumět manipulaci (zpracování) informací v mikropodniku (kap. 4.5.3, tabulka 2).

4.9.3 Rozsah aplikovatelnosti ISO 27001

- nastavit rozsah aplikace normy ISO/IEC 27001 – PoA (kap.4.6.2) na základě kontextu organizace kap. 4.9.2;
- rozsah určit na základě reálné architektury IS v mikropodniku jako je na obrázku 15;
- vrcholové vedení musí projevit dostatečnou podporu a přidělit přiměřené zdroje (finanční, lidské, technické), které jsou potřebné k zavedení a udržování ISMS prohlášením – politika ISMS (příloha 13);
- stanovit role ISMS a to interní (výkonné v rámci běžné činnosti mikropodniku – lékař, sestra, smluvní správce IS) a externí (bezpečnostní role pro audit, nastavení ISMS, penetrační testování, certifikaci), (kap. 4.6.4).

4.9.4 Identifikace aktiv a analýza rizik

- odpovědět na otázky uvedené v úvodu kap. 4.7;
- provést identifikaci (kap. 4.7.1) a hodnocení primárních a podpůrných aktiv dle CIA (kap. 4.7.2), zkoumat vazby aktiv (analýza na obrázku 18, v tabulce 5), určit vlastníka aktiv, vytvořit registr primárních (tabulka 6) a podpůrných aktiv (příloha 4);
- provést analýzu rizik (kap. 4.8), vytvořit katalog identifikovaných hrozeb (příloha 7) a zranitelností (příloha 8), dopadů na aktiva a jejich hodnocení (kap. 4.8.5), matici souvislostí hrozeb využívající zranitelností (příloha 9), matice rizik (příloha 10);
- vytvořit registr identifikovaných rizik (kap. 4.8.4), který souvisí s prohlášením o aplikovatelnosti PoA;
- stanovit časový plán zvládání rizik k splnění jednotlivých opatření k ošetření rizik.

4.9.5 Ošetření rizik a nastavení bezpečnosti IS

Po splnění kroků předchozí části metodiky, autor navrhuje provést ošetření rizik s cílem snížení rizika působících hrozeb a dosáhnout míry přijatelného rizika, které je akceptovatelné pro jednatele / vedení mikropodniku v rámci politiky ISMS. Je nutné přijmout opatření **bezpečnostní politiky IS** v oblastech:

- **doporučený postup instalace aplikačního IS a nastavení základních informačních, technických a organizačních opatření:**
  - instalace dle schématu propojení aplikačního IS - uvedeno v kapitole 4.5.2;
  - počítač s moderním HW (min. 6-8 jádrový procesor AMD Ryzen 5.generace / Intel Core 11.generace, 2xSSD M.2 1TB, 16GB RAM a více, 1Gbit LAN karta, porty dle potřeby připojení diagnostických zdravotnich přístrojů a periferií (multifiunkční tiskárna, skener A4 duplex, tisk čárkových štítků ZEBRA system, myš, klávesnice, USB disk, zálohovací zažízení, čtečka karet a průkazů);
  - kontola pevné telefonní linky a aktivovaných GSM zařízení a služeb;
  - připojení do internetu symetrickou rychlostí 50-100Mbit (záložní připojení pomocí 4G/5G GSM), užít router s WAN a 4 – 8 ks portů RJ45 1Gb switche s možností konfigurace firewalu, DDoS ochrany, konfigurace VPN a komunikačních portů, užítvat v objektu mikropodniku strukturovanou kabeláž a provozovat WI-FI s šifrováním;

- instalované záložní zdroje UPS s dostatečnou kapacitou baterie na 20 - 30 minut provozu pro počítače, aktivního prvku intranetu a ostaních technických prostředků ambulance;
- instalace OS WINDOWS 10/11 Profesional na zformatovaný systémový disk souborovým systémem NTFS s nastavením potřebných instancí OS včetně provedení aktualizace a instalace ovladačů zařízení OS dle potřeb aplikačního SW;
- aktivace a nastavenní cloudových služeb (MS OneDrive) pro automatické ukládání elektronických dokumentů a zálohování;
- instalace SW pro ochranu proti škodlivému kódu (ESET, MS Defender);
- instalace a konfigurace aplikačního SW prostředí IS (SmartMedix) s nasatavením replikace mezi jednotlivými uzly (stolní počítač – notebook) a připojení / konfigurace diagnostických zdravotnických přístrojů;
- kontrola přístupu do portálu eNeschopenka, eRecept, eSpráva, datová schránka PO, ČSSZ, ZP, ISIN, ÚZIS, laboratoří (Medila, EUC) a bankovnictví;
- kontrola funkčnosti skenování dokumentů, tisku štítků, tisku dokumentů;
- vytvoření uživatelských účtů s možností biometrického přihlášení, nastaveni hesel a kontrola funkčnosti v IS;
- vytvoření zálohy systémových disků PC a notebooku jako bitové kopie;

- **řízení přístupu (ISO 27002, kap. 9):**
  - vlastníci aktiv řídí přístupová práva uživatelů s předpokladem „Obecně je vše zakázáno, pokud to není výslovně povoleno“;
  - politika uživatelských účtů a hesel OS, SW a IS:
    - administrátorský účet – určen pouze pro správu IS;
    - uživatelský účet – určen pro běžnou pracovní činnost lékaře a sestry;
  - systém tvorby, ukládání a chránění hesel:
    - nastavení pravidla délky a složitosti hesla se zásadou „každý systém jiné (jedinečné) heslo“;
    - vyžadovat změnu hesla uživatele alespoň 1x za 90 dní;
    - hesla archivovat v chráněné podobě (mimo ambulanci);
  - mít kontrolu nad přístupovými právy uživatelů k informacím v IS a k souborům v adresářích „kdo má právo číst, zapisovat, vytvářet, mazat či editovat data“;
  - mít kontrolu nad uživatelským přístupem k jednotlivým aplikacím, částem IS, portálům veřejné správy, datové schránce, eRecept/eNeschopenka, aj.;

- mít kontrolu nad přístupem k lokálním úložištím, cloudovým službám, síťovým službám a užívání bezdrátových sítí;
- mít kontrolu nad přístupem k listinné zdravotnické dokumentaci v kartotéce – zavírat šuplíky v přítomnosti pacientů, zamykat kartotéku mimo pracovní dobu, řídit fyzický vstup osob do archivu zdravotních karet ambulance;
- kontrolovaný přístup vzdálené správy k aplikačnímu IS samostatným obslužným programem po autentizaci a autorizaci například TeamViewer;
- nastavit auditování provozu OS MS Windows, aplikačního SW a provoz v sítovém prostředí na aktivním prvku (router, switch) – ukládat auditní záznamy pro případnou analýzu dokumentovaných informací o provozu a událostech v OS a IS, jako důkaz o výsledcích monitorování provozu (1xměsíčně);
- kontrola přístupových práv vlastníkem IS – provádění změn přístupových práv, případně úplné zablokování či odstranění práv a účtu uživatele;

- **klasifikace informací a manipulace s informacemi (ISO 27002, kap. 8.2):**
  - znát typ s rozsah informací podléhajících ochraně osobních údajů;
  - definovat správu informací v souladu s GDPR;
  - znát způsob manipulace (distribuce, přístup, použití, ukládání, řízení změn, uchování, likvidace) dokumentovaných informací v komunikačním prostředí (ISO 27001, kap. 7.5.3);
  - užívání datové schránky k přijímání a odesílání elektronických dokumentů obsahující zdravotnické informace při komunikaci s ostatními poskytovateli zdravotní péče a veřejnou správou;
  - užívat bezpečné přihlášení kvalifikovaným certifikátem do portálů zdravotních pojišťoven, ČSSZ a ÚZIS pro autorizovanou manipulaci s informacemi;
  - udržovat přehled manipulace s informacemi (uveden v tabulce 2 a v kap. 4.5.3);
- **fyzickou bezpečnost a bezpečnost prostředí (ISO 27002, kap. 11):**
  - definovat fyzický perimetr k ochraně oblasti zpracování zdravotnických informací, ukládání zdravotních karet pacientů, provozu informačních aktiv HW, SW a diagnostických přístrojů;
  - mimo pracovní dobu uzamykat dveře a prostory perimetru zabezpečit užíváním EZS s možností identifikace vstupu zaměstnanců a připojením na pult ochrany majetku bezpečnostní agentury;
  - doporučení instalovat požární hlásiče a hlásiče úniku plynu a vody;

- doporučení mít rozvodovou skříň elektrické energie s pojistkami a uzávěr vody v bezpečnostním perimetru objektu;
- instalovat klimatizaci pro zabezpečení udržení tepelných podmínek poskytování zdravotní péče, uchovávání léčiv a zdravotnického materiálu;
- provozovat slaboproudé rozvody dle platných norem;
- popis opatření v ambulanci praktického lékaře je rozepsáno v kap. 4.6.3;

- **opatření pro práci uživatelů:**
  - přijatelné použití aktiv (ISO 27002, kap. 8.1.3) souvisí s užíváním aktiv dle určeného účelu:
    - užívání stolního počítače zapojeného do IS ordinace pouze k užívání s předem nainstalovaného softwarového vybavení k výkonu zdravotní péče;
    - manipulace s analogovou (listinou) zdravotní kartou pacienta pro potřeby ošetřujícího lékaře či náhledu pacientem;
    - užívání externích záznamových medií pouze v počítačích k tomu určených;
  - čistý stůl a čistý displej (ISO 27002, kap. 11.2.9):
    - nezanechávat na pracovním stole otevřenou zdravotní kartu (dokumentaci) jiného pacienta, který není aktuálně ošetřován, aby nedošlo k neoprávněnému seznámení se s informacemi;
    - dbát na minimalizaci pracovního okna aplikačního software (SmartMedix) v přítomnosti jiné osoby, aby nedošlo k neoprávněnému seznámení se s informacemi, případně odhlášení uživatele (personálu) z dané aplikace či OS při nepřítomnosti uživatele;
    - při přerušení práce na počítači provést uzamknutí/odhlášení uživatele;
  - přenos informací (ISO 27002, kap. 13.2.1):
    - pro potřebu interní a externí komunikace (přenosu informací) potřebujeme znát „o čem, kdy, s kým, kdo musí komunikovat a způsob (proces) realizace komunikace (kap. 4.5.3);
    - nastavení komunikační ochrany důvěrnosti, integrity a autenticity z a do externího prostředí IS užitím VPN, šifrováním dokumentů a užíváním kvalifikovaných certifikátů;
    - nastavení postupů pro sdělování zdravotních informací po telefonu hlasem, otevřenou formou emailem, oprávněné osobě při rozhovoru v ambulanci, užití písemné formy dopisu a přenosu informací na CD, DVD, USB disku;

        - nastavit smlouvy o přenosu informací užíváním kurýra, datové schránky PO, eSprávy;
    - mobilní zařízení (notebook) a práce na dálku (ISO 27002, kap. 6.2):
        - instalovaný aplikační SW (SmartMedix) s nastavením replikace aplikační databáze (prostředí MS Azure) s řízením jednotlivých uzlů replikace (hlavní – počítač v ambulanci, podřízený – notebook) – výhodou je rychlost práce v IS, pro zápis vyšetření (dekurs) není vyžadováno připojení k internetu, kdy zpracovaná data se mezi uzly replikují po připojení do intranetu/internetu;
        - pro vystavení eReceptu, eNeschopenka, načtení výsledků z laboratoře při práci na dálku je nutné připojení do internetu;
    - omezení týkající se instalací a použití software (ISO 27002, kap. 12.6.2):
        - právo instalace SW vybaveni má správce IS s právem administrátora, uživateli je zakázáno spouštět a instalovat neschválený SW;
        - aktualizace aplikačního IS provádí dodavatel SW (SmartMedix) na základě smlouvy o poskytování podpory;
        - aktualizace antivirového SW se provádí automaticky poskytovatelem licence;
        - aktualizace operačního systému, ostatního programového vybavení a ovladačů HW zařízení provádí výhradně administrátor IS, aby nedošlo k instalaci nevhodné verze ovladače či nežádoucího updatu OS;
- **zálohování (ISO 27002, kap. 12.3):**
    - nasazení zálohování a replikace databáze elektronické zdravotní dokumentace mezi hlavním (stolním počítačem) v ambulanci a přenosným notebookem pro práci v a mimo ambulanci v MS Azure;
    - užití cloudu MS OneDrive pro automatické zálohování elektronických dokumentů v stolním počítači a notebooku v prostředí MS Windows 10/11 pro – dvě samostatné nezávislé úložiště;
    - 1x měsíčně vytvoření obrazu off-line bitové kopie systému;
    - bezpečné uložení osobních, komerčních a kvalifikovaných certifikátů s hesly;
    - uložení administrátorských hesel mimo mikropodnik;
- **ochrana před škodlivým kódem (ISO 27002, kap. 12.2):**
    - užívat SW pro ochranu před škodlivým kódem – antivir např. ESET, MS Defender aj. na všech zařízeních s OS a nastavenou automatickou kontrolou všech vyměnitelných médií, emailů a systémového provozu;

- zakázání spouštění maker v dokumentech MS OFFICE;
- na routeru aktivovat:
  - funkce ochrany sítě například s integrovaným nástrojem Trend Micro, který poskytuje prevenci proti hrozbám zneužití sítě, ochranu proti škodlivým adresám URL a chrání připojená zařízení před kybernetickými hrozbami;
  - užívání firewallu s ochranou proti DDoS útokům, s řízením komunikačních portů, s možností filtru URL a síťových služeb;
  - užívat VPN s možností konfigurace přímo v routeru (primární řešení) nebo užití software v OS u všech počítačů a notebooků (sekundární řešení) – opatření pro bezpečnost v komunikačním prostředí internetu;
- pro komunikaci PC, tabletů, periferií, diagnostických přístrojů přednostně užívat vnitřní sítě (intranetu);

- **správa a řízení technických opatření (ISO 27002, kap. 12.6.1):**
  - vést a aktualizovat seznam aktiv;
  - pro HW, SW aktiva a diagnostické přístroje určit informační zdroje pro identifikaci zranitelností a možností aplikace příslušných opatření dané zranitelnosti;
  - opatření aplikovat v podobě instalace nového ovladače zařazení, firmwaru, verze software, bezpečnostní systémové záplaty a síťové konfigurace po ověření účinku na dané aktivum;
  - nastavení parametrů BIOS počítače:
    - přístup pro konfiguraci pouze po zadání hesla oprávněné osoby;
    - nastavit bootování pouze ze systémového disku počítače;
    - deaktivovat volbu bootování LAN, USB, CD/DVD a jiných paměťových nosičů;
    - deaktivovat neužívaná komunikační rozhraní;
    - zakázat automatický update firmware BIOS;
- **kryptografická opatření (ISO 27002, kap. 10):**
  - nastavení a užívání VPN pro komunikační rozhraní do internetu;
  - šifrování paměťových medií a disků v PC a NB SW BitLocker;
  - provést bezpečný výmaz neužívaných paměťových nosičů při výměně v IS;
  - nastavení životního cyklu kryptografických klíčů jako je užívání osobních, komerčních a kvalifikovaných certifikátů;
  - aplikovat SSL certifikát pro zabezpečení webové domény protokolu https.

4.9.6 Zpracování dokumentace a stanovení rolí ISMS

- zpracování politiky ISMS (příloha 13);
- prohlášení o aplikovatelnosti PoA (příloha 12);
- stanovení rolí bezpečnostní správy IS (ISMS) mikropodniku (kap. 4.6.4);
- bezpečnostní politika IS (kap. 4.9.5);
- plán kontinuity IS – zpracováno pro vybrané incidenty (příloha 14);
- směrnice uživatele IS (příloha 15);
- vedení záznamů o činnostech, kontrolách a auditech IS – provozní deník;
- dodavatelské vztahy (ISO 27002, kap. 15) – návrh smluvních vztahů (kap.4.3);
- dokumentovat výstupy analýzy rizik (kap. 4.9.4).

4.9.7 Školení zaměstnanců

- zabezpečit školení vedoucích zaměstnanců a odborných pracovníků určených do role bezpečnostní správy IS;
- provést prvotní a provádět pravidelná školení zaměstnanců z ISMS;
- realizovat hodnocení zaměstnanců a lessons learned z incidentů a událostí v IS.

4.9.8 Poskytování zdravotní péče

- jsou zavedena opatření ochrany bezpečnosti informací primárních a podpůrných aktiv;
- je nastaven systém řízení ISMS (obrázek 19);
- provoz informačního systém ambulance podporuje výkon poskytování zdravotní péče v autorem navrhnutém prostoru ISMS (obrázek 7);

4.9.9 Audit a certifikace

- přezkoumání IS a porovnání s počátečním stavem (interní audit dle kap. 4.4);
- provést penetrační testování a nezávislý bezpečnostní audit od nezávislého subjektu;
- aktualizovat a akceptovat potřebná rozšiřujících opatření zavedeného ISMS;
- provedení certifikace akreditovanou identitou.

5 Zhodnocení výsledků

Diplomová práce je rozdělena na dvě části, a to teoretickou a praktickou část. V teoretické části v kapitole 3 autor provedl rešerši základního teoretického popisu IS, exploraci legislativního prostoru ISMS mikropodniku a popis metodik řízení IT. V praktické částí v kapitole 4 autor provedl analýzu reálného prostředí poskytovatele zdravotní péče a navrhnul implementaci bezpečnostních opatření ISMS dle ISO 27001 do prostředí IS mikropodniku ambulance VPL. Zdrojem informací pro diplomovou práci byl kvalitativní výzkum metodou nestrukturovaných a polostrukturovaných rozhovorů, metoda pozorování, explorace, komparace a praktická zkušenost administrace IS v mikropodniku.

Zhodnocení výsledků diplomové práce

Cíl diplomové práce byl realizován návrhem metodiky bezpečnosti IS (kap. 4.9).

Autor pro realizaci hlavního cíle diplomové práce:

- navrhnul legislativní prostor ISMS v mikropodniku (kap. 3.3 obrázek 7);
- identifikoval primární aktiva (kap. 4.7 tabulka 6) na základě právního rámce (kap. 4.2 obrázek 12), kontextu zdravotní péče (kap. 4.3) a hlavního procesu (kap. 4.5.1);
- analyzoval vztah mezi primárními a podpůrnými aktivy (kap. 4.7.1 tabulka 5);
- navrhnul stanovení rolí ISMS v mikropodniku (kap. 4.6.4);
- navrhnul způsob komparace stávajícího / cílového stavu opatření ISMS dle PoA (kap.4.4);
- analyzoval informační toky a způsob manipulace s informacemi / dokumenty (kap. 4.5.2, kap. 4.5.3, obrázek 15 a 16, tabulka 2);
- navrhnul možný postup provedení analýzy rizik v mikropodniku (kap. 4.8);
- navrhnul minimální rozsah dokumentace ISMS v mikropodniku (kap. 4.9.6):
    - „Politika ISMS“ (příloha 13);
    - „Prohlášení o aplikovatelnosti“ (příloha 12);
    - „Politika bezpečnosti IS“ (kap. 4.9.5);
    - „Plán kontinuity IS“ (příloha 14)
    - „Směrnice uživatele IS“ (příloha 15).

V IS ambulance všeobecného praktického lékaře byly identifikovány primární aktiva:

- zdravotní péče (služba);
- zdravotnická dokumentace (informace);

- účtování zdravotních služeb (informace);
- aplikační IS (informace).

Opatření k nastavení ochrany těchto aktiv v mikropodniku byla zavedena pomocí navrhnuté metodiky bezpečnosti IS.

Finanční náklady na zavedená opatření ISMS jsou uvedena v příloze 16, kde celkové počáteční náklady na zavedení navržených opatření jsou ve výši 263.214 Kč. Pro udržování zavedených opatření je nutné v rozpočtu mikropodniku, každý rok vyčlenit finanční prostředky a to 86.966Kč. Roční náklady tvoří cca 2 % obratu a jsou jednatelem schváleny jako přijatelné. Nejvíce finančních prostředků je nutné vyčlenit na licenční poplatky a aktualizace aplikačního SW SmartMedix 25.875Kč a zabezpečení dostupnosti smluvního správce IS 24.000Kč. Další náklady souvisí s platbami za připojení k internetu, on-line službu ochrany objektu EZS, pravidelná školení atd. V návrhu metodiky bezpečnosti IS je řada opatření, například – přijatelné použití aktiv (ISO 27002, kap. 8.1.3), čistý stůl a čistý displej (ISO 27002, kap. 11.2.9) a opatření k přenosu informací (ISO 27002, kap. 13.2.1), která nevyžadují finanční náklady na zavedení.

Předpokládaným přínosem realizovaného návrhu metodiky bezpečnosti IS pro mikropodnik je schopnost:

Předcházet:

- finančním ztrátám za pozastavení činnosti;
- finančním nákladům na obnovení, instalaci a konfiguraci IS;
- legislativním důsledkům dopadu porušení bezpečnosti informací;
- nedostupnosti potřebných informací v IS, porušení důvěrnosti seznámení se neoprávněnou osobou a narušení integrity pozměním dat.

Zabezpečit:

- dokumentovaný proces hlavních aktiv mikropodniku;
- zavedení normovaného standartu zpracování informací;
- řízení bezpečnosti informací v mikropodniku dle ISO/IEC 27001;
- předpoklad pro splnění požadavků kybernetické bezpečnosti v ambulanci VPL.

Poskytovat:

- přehled o HW, SW a technické vybavení mikropodniku;
- nastavený způsob výměny dat v komunikačním prostředí;

- usnadňuje implementaci změn v legislativě a bezpečnostních standardech;
- kontinuální řízení rizik a reakce na možné události a incidenty.

Konkurenční výhoda:

- umožnění přechodu vedení dokumentace na výhradně elektronickou podobu;
- optimalizace nákladů na životní cyklus informačního systému a podpůrných aktiv;
- zveřejněním politiky ISMS poskytuje občanům, veřejné správě a obchodním partnerům důvěru o bezpečném zpracování informací a dodržování GDPR.

Identifikované problémy v zavedeném ISMS:

- pacienti užívají nesprávného způsobu manipulace, sdílení zdravotnických informací v listinné podobě formou obyčejné listovní zásilky či vhození lékařské správy do poštovní schránky ambulance bez obálky nebo adresace příjemce;
- státní orgány, veřejná správa a poskytovatelé zdravotních služeb neužívají plně možností elektronické komunikace např. pomocí datové schránky pro jednoznačnou identifikaci odesílatele a příjemce pro vyžadování zdravotnických informací – registrace pacienta, zaslání výpisu se zdravotní dokumentace, zdravotního posudku, vyjádření lékaře k zdravotnímu stavu pacienta pro policii / soud aj.;
- komunikace s „třetí osobou“ vyžadující vystavení preskripce a případné sdělení výsledku vyšetření pacienta, o kterého daná „třetí osoba“ pečuje;
- nemožnost užití ZKB normovaného postupu zavedení bezpečnosti IS pro mikropodniky (odůvodnění kap. 3.2.4).

Obtížně aplikovatelná opatření ISMS:

- vyžadovaní ověřování identity pacientů při komunikaci po telefonu nebo emailem, souhlas (GDPR) s poskytováním informací na telefonní číslo a užitím komunikačního hesla se jeví jako elementární opatření k identifikaci oprávněné osoby, které se s ohledem na vyšší věk pacientů obtížně vynucuje;
- stanovení bezpečnostních rolí pro ISMS, kdy mikropodnik (ambulance VPL) má limitované finanční a lidské zdroje, nemá ve své organizační struktuře zaměstnance, odborný personál k posuzování, zavádění a udržování opatření bezpečnosti IS.

6 Závěr

Bezpečnost informací, ochrana soukromí a vlastní identita v informačních systémech patří k netriviálním problémům. V organizacích, které užívají IS k zpracování osobních údajů a informací o zdravotním stavu pacientů, musí být přijata vhodná opatření k ochraně informací. Autor v kapitole 4.9 navrhnul metodiku bezpečnosti IS podle ISO/IEC 27000 jako vhodný postup pro nastavení ISMS v zájmovém mikropodniku.

Jednatel ambulance VPL vnímá zavádění bezpečnosti IS jako kontrolovaný proces, kdy může předcházet úniku informací a neoprávněné manipulaci se zdravotnickou dokumentací pacientů. V mikropodniku je nastaveno auditování událostí s cílem zlepšovaní a příjímání nových opatření k udržení sytému řízení bezpečnosti informací. Aktuálně jednatel ambulance neusiluje o certifikaci ISMS.

Přínosem diplomové práce pro mikropodniku je:

- identifikovaný legislativní prostor ISMS;
- identifikovaná aktiva, přehled manipulace zpracovávaných informací (GDPR);
- návrh postupu komparace stavu opatření ISMS dle PoA;
- návrh postupu analýzy rizik podle ISO/IEC 27005;
- návrh minimálního rozsahu dokumentace ISMS pro IS;
- aplikovatelná opatření ISMS podle navrhnuté metodiky bezpečnosti IS.

Proces zavedení bezpečnosti IS v mikropodniku standardizoval zpracování osobních údajů a zdravotnických informací, podpořil bezpečný způsob sdílení informací pomocí datové schránky, užívání kvalifikovaného certifikátu umožnilo autentizaci elektronického dokumentu a zjednodušilo komunikaci se státními orgány a veřejnou správou. Aplikovaná opatření informační bezpečnosti zvýšila odolnost informačního systému proti identifikovaným hrozbám a zranitelnostem pomocí navrhnutých opatření uvedených v metodice bezpečnosti IS. Návrh metodiky je obecně vhodný pro implementaci v libovolném mikropodniku, ale není dogmatem, jak řešit potřebu nastavení informační bezpečnosti v organizacích s malým počtem zaměstnanců. Tato práce je základní analýzou možností splnění podmínek kybernetické bezpečnosti v reálném prostředí, kdy mikropodnik s udržovaným a certifikovaným ISMS v IS může následně garantovat:

- důvěrnost – informace je uchovávána a sdělena pouze oprávněné osobě;
- integritu – informace není bez vědomí oprávněné osoby změněna;
- dostupnost – informace je přístupná po identifikaci oprávněné osoby.

7 Seznam použitých zdrojů

BEZOUŠKA, T. 2020. *Metodický pokyn poskytovatelům zdravotních služeb ke kybernetické bezpečnosti, Příloha č. 9 - Metodika analýzy a řízení rizik (vzor)* [online]. (DOCX) Ministerstvo zdravotnictví ČR, 28 s. [cit. 2022-11-02]. Dostupné z: https://ncez.mzcr.cz/sites/default/files/Attachment/Metodika_analýzy_a_řízení_rizik_1.docx

BEZOUŠKA, T. 2022. *Metodický pokyn poskytovatelům zdravotních služeb ke kybernetické bezpečnosti, Příloha č. 8 - Metodika identifikace a správy informačních aktiv (vzor)* [online]. (DOCX). Ministerstvo zdravotnictví ČR [cit. 2022-08-07]. Dostupné z: https://ncez.mzcr.cz/sites/default/files/Attachment/Metodika-identifikace_a_správy_ informačních_aktiv.docx

BEZOUŠKA, T., BOREJ,J. 2019. *Metodický pokyn poskytovatelům zdravotních služeb k problematice kybernetické bezpečnosti* [online].(DOCX). Ministerstvo zdravotnictví ČR, 17 s. [cit. 2022-08-07]. Dostupné z: https://ncez.mzcr.cz/sites/default/files/Attachment/Metodický _pokyn_poskytovatelům_zdravotních_služeb_k_problematice_kybernetické_bezpečnosti.docx

BRUCKNER, T. 2012. *Tvorba informačních systémů: principy, metodiky, architektury*. 1. vyd. Praha: Grada. Management v informační společnosti. ISBN 978-80-247-4153-6.

BUCHALCEVOVÁ, A. 2008. Zlepšování softwarových procesů ve velmi malých podnicích. Liberec 06.11.2008 – 07.11.2008. In: Liberecké informatické fórum. Liberec : TU, 2008, s. 12–19. ISBN 978-80-7372-408-5. Dostupné také z: https://nb.vse.cz/~buchalc/clanky/procesy.pdf

BUCHALCEVOVÁ, A. 2016. Analysis of the management of business informatics framework from the green ICT viewpoint. International Journal of Information Technology and Management [online]. 2016, roč. 15, č. 1, s. 41–58. ISSN 1461-4111. DOI: 10.1504/IJITM.2016.073913 Dostupné také z: https://nb.vse.cz/~buchalc/clanky/ijitm2016.pdf

DANBY, S. 2023. The ITIL 4 Service Value System Explained. ITSM TOOLS. [Online] 2023. [cit. 2023-09-23]. Dostupné z: https://itsm.tools/the-itil-4-service-value-system-explained/

ET.AL, Yeni Kusumaningrum. 2021. Adoption of COBIT 5 Framework in Risk Management for Startup Company. Online. Turkish Journal of Computer and Mathematics Education (TURCOMAT). 2021, roč. 12, č. 3, s. 1446-1452. ISSN 1309-4653. Dostupné z: https://doi.org/10.17762/turcomat.v12i3.942. [cit. 2023-10-29].

GÁLA, L., POUR, J., ŠEDIVÁ, Z. 2009. *Podniková informatika*. 2., přeprac. a aktualiz. vyd. Praha: Grada Publishing. Expert. ISBN 978-80-247-2615-1.

GÁLA, L., POUR, J., ŠEDIVÁ, Z. 2015. *Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi*. 3., aktualiz. vyd. Praha: Grada Publishing. Management v informační společnosti. ISBN 978-80-247-5457-4.

GOGELA, R. 2011. *Standardy a definice pojmů ISMS*: Sborník příspěvků z bezpečnostního semináře Policejní akademie a evropského vedení AFCEA konaného dne 22. září 2011 na Policejní akademii České republiky v Praze. Vyd. 1. Praha: Policejní akademie České republiky. [cit. 2022-07-29] ISBN 978-80-7251-356-7. Dostupné také z: https://cybersecurity.cz/ data/Gogela.pdf

GOLL, J. 2023. *Zákon o kybernetické bezpečnosti versus ISO 27001 aneb jak vyhovět oběma normám: aneb jak vyhovět oběma normám* [online]. [cit. 2023-02-04]. Dostupné z: https://www.systemonline.cz/sprava-it/zakon-o-kyberneticke-bezpecnosti-versus-iso-27001.htm

HALBICH, Č., VOSTROVSKÝ, V., TYRYCHTR, J. 2015. Systems Theory and Model of Diversification in Building of Information Systems. *In: Moreno-Díaz, R., Pichler, F., Quesada-Arencibia, A. (eds) Computer Aided Systems Theory – EUROCAST 2015*. EUROCAST 2015. Lecture Notes in Computer Science, vol 9520. Springer, Cham. [cit. 2023-11-15]. Dostupné z: https://doi.org/10.1007/978-3-319-27340-2_3

ISACA. 2018. Introducing COBIT 2019. In: *Isaca.org*, [online]. (COBIT 2019 Executive Summary_v1.1.pdf) [cit. 2023-09-16]. Dostupné z: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/cobit-2019-toolkit.zip

ISO 27000. 2018. *ČSN ISO/IEC 27000 (369790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ISO 27001. 2014. *ČSN ISO/IEC 27001 (36 9797) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ISO 27002. 2014. *ČSN ISO/IEC 27002 (36 9798) Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Druhé vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ISO 27003. 2018. *ČSN ISO/IEC 27003 (36 9790) Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Pokyny*. 1. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ISO 27005. 2019. *ČSN ISO/IEC 27005 (36 9790) Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. 3. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ISO 27799. 2019. *ČSN EN ISO 27799 (98 2021) Zdravotnická informatika – Systémy řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002*. 2. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

ISO 31000. 2018. *ČSN ISO 31000 (505890) - Management rizik – Směrnice.* 1.vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.

JIRÁSEK, P., NOVÁK, L., POŽÁR, J. 2015. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze. [cit. 2022-07-30]. ISBN 978-80-7251-436-6. Dostupné také z: http://www.cybersecurity.cz/data/slovnik_v310.pdf

KOFRÁNEK, J., FELIX O., POLÁK J., BOREJ J. 2017. Napojení zdravotnických systémů na základní registry veřejné správy: ochrana a kontrolované sdílení osobních dat. *In: Medsoft 2017: Sborník příspěvků*. Praha: Creative Connections, 2017. s. 104-116. ISBN 978-80-86742-47-2. ISSN 1803-8115. Dostupné tak z: https://www.creativeconnections.cz/medsoft/2017/Medsoft_2017_Kofranek2.pdf

MAMRILLA, F., TOMAN, Š. 2021. *Kybernetická bezpečnost ve zdravotnictví* [online]. [cit. 2022-10-07]. Dostupné z: https://www.epravo.cz/top/clanky/kyberneticka-bezpecnost-ve-zdravotnictvi-112849.html

MZČR, 2022. *Metodika kybernetické bezpečnosti*. [online]. In: *Ministerstvo zdravotnictví ČR*. [cit. 2022-11-21]. Dostupné z: https://ncez.mzcr.cz/cs/kyberneticka-bezpecnost/metodika-kyberneticke-bezpecnosti.

NBÚ, 2013. *Návrh zákona o kybernetické bezpečnosti byl předložen vládě České republiky*, 8.7.2013. In: *NBÚ* [online]. [cit. 2023-02-03]. Dostupné z: https://www.nbu.cz/cs/aktualne/731-1398-navrh-zakona-o-kyberneticke-bezpecnosti-byl-predlozen-vlade-ceske-republiky/

NEZMAR, L. 2017. GDPR: praktický průvodce implementací. Online. Právo pro praxi. Praha: Grada Publishing, 2017. [cit. 2023-10-04]. ISBN 978-80-271-0668-4. Dostupné z: https://www.grada.cz/gdpr-prakticky-pruvodce-implementaci-9889/

NOVÁK, L., POŽÁR, J. 2011. *Systém řízení informační bezpečnosti: Sborník příspěvků z bezpečnostního semináře Policejní akademie a evropského vedení AFCEA konaného 22. září 2011 na Policejní akademii České republiky v Praze*. Vyd. 1. Praha: Policejní akademie České republiky. [cit. 2022-08-29]. ISBN 978-80-7251-356-7. Dostupné také z: https://www.cybersecurity.cz/data/SRIB.pdf

NÚKIB. 2020a. *Hrozba rozsáhlých kybernetických útoků na české zdravotnictví a další oblasti klesla na běžnou úroveň.* [online]. In: *NÚKIB.* [cit. 2023-11-21]. Dostupné z: https://nukib.cz/cs/infoservis/aktuality/1553-hrozba-rozsahlych-kybernetickych-utoku-na-ceske-zdravotnictvi-a-dalsi-oblasti-klesla-na-beznou-uroven/

NÚKIB. 2020b. *Doporučená bezpečnostní opatření k varování k varování ze dne 16.dubna 2020.* [online]. In: NÚKIB. (PDF). [cit. 2023-11-21]. Dostupný z: https://nukib.cz/download/archiv/ Doporuceni-k-varovani-2020-04-17.pdf

NÚKIB. 2022a. *Systém a rozsah ISMS*. In: NÚKIB [online]. (PDF). [cit. 2022-11-28]. Dostupné z: https://www.nukib.cz/download/publikace/podpurne_materialy/ odpurny_material _system _a_rozsah_ISMS_v1.0.pdf

NÚKIB. 2022b. *Průvodce řízení aktiv a rizik dle vyhlášky o kybernetické bezpečnosti*. In: *NÚKIB* [online]. (PDF). [cit. 2022-12-21]. Dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/Prvodce zenm aktiv a rizik dle vyhlky o kybernetick bezpenosti.pdf

NÚKIB. 2022c. *Příloha 4 - Struktura podpůrných aktiv*. In: *NÚKIB* [online]. (PDF). [cit. 2023-02-06]. Dostupné z: https://nukib.cz/download/publikace/podpurne_materialy/ Ploha 4 - Struktura podprnch aktiv.pdf

PostSignum, Kvalifikované certifikáty. In: Česká pošta [online] 2023. [cit. 2023-10-17]. Dostupné z: https://www.postsignum.cz/kvalifikovane_certifikaty.html

POUR, J. 2012. Business intelligence řešení v modelu MBI. In: *SYSTÉMOVÁ INTEGRACE 2/2012* [online]. 2.2.2012. Praha, 13 s. [cit. 2022-07-29]. ISSN 1210-9479. Dostupné z: https://scholar.archive.org/work/ildtpuw27vbyzcv6q5pz2svnhm

RAIN, T., ŠVARCOVÁ, I. 2010. Internet and seniors, In: *Journal on Efficiency and Responsibility in Education and Science, Vol. 3, No. 2, pp. 79-85, 31 December 2010*. ISSN 1803-1617, [on-line]. [cit 2023-11-19]. Dostupné z: www.eriesjournal.com/_papers/article_110.pdf

RANCE, S. 2019. The 7 Guiding Principles of ITIL 4: Practical Advice to Help You Make Decisions. SYSAID. [Online] 2023. [cit. 2023-09-23]. Dostupné z: https://www.sysaid.com/ blog/itil/the-7-guiding-principles-of-itil-4-practical-advice-to-help-you-make-decisions

ŠKRABÁNEK, J. 2020. ITIL 4 aneb Jak lépe řídit IT. In: *SystemOnLine 2023* [online]. [cit. 2023-09-20]. Dostupné z: https://www.systemonline.cz/sprava-it/itil-4-procesy-praktiky-a-ctyri-dimenze-rizeni-it.htm?mobilelayout=false. ISSN 1802-615X.

Tayllorcox: *ISMS FAQ: Co znamená zkratka ISMS*. In: *TayllorCox* [online]. 2022. [cit. 2023-08-16]. Dostupné z: https://www.tx.cz/isms/faq
Tayllorcox: Co je ITIL. In: *TayllorCox* [online]. 2023. [cit. 2023-02-24]. Dostupné z: https://www.tx.cz/ itil/metodika

TĚŠITELOVÁ, V., POLICAR, R., DUŠEK, L. 2018. Jak implementovat v ambulantní sféře nařízení Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) do resortu zdravotnictví. In: MZČR [online]. Praha: Ministerstvo zdravotnictví ČR, s. 110. [cit. 2023-01-28]. ISBN 978-80-85047-57-8. Dostupné z: https://www.mzcr.cz/ wpcontent/uploads/wepub/15782/34328/gdpr_AMBUL_20180509__metodika_implement ace_ambulantni_sfera.pdf

THOMAS, M., 2021. Using ITIL and COBIT 2019 for an integrated I&T framework. Online. 7.7.2021. [cit. 2023-09-29]. Dostupné z: https://www.axelos.com/resource-hub/white-paper/using-itil-cobit-2019-create-integrated-environment

TYRYCHTR, J. 2015. *Provozní a analytické databáze – Teoretické základy.* Praha : ČSVIZ. ISBN 978-80-87968-02-4. Dostupné také z: https://books.google.cz [cit. 2023-11-20].

Uživatelská příručka k definici malých a středních podniků [online], 2019. Lucenburk: Úřad pro publikace Evropské unie [cit. 2023-03-29]. ET-01-17-660-CS-N. PDF ISBN 978-92-79-69931-3. Dostupné z: doi:10.2873/117802

VITOUŠ, M. 2013. COBIT 5 v malých a středních firmách. SystemOnLine. [Online] 2023. [cit.: 2023-09-20]. Dostupné z: https://www.systemonline.cz/sprava-it/cobit-5-v-malych-a-strednich-firmach.htm. ISSN 1802-615X.

VOŘÍŠEK, J., BUCHALCEVOVÁ, A. 2015. Management of Business Informatics Model – Principles and Practices. In: *E a M: Ekonomie a Management [online]*. Liberec, ČR: Ekonomická fakulta, Technická univerzita v Liberci, s. 160-173. Roč. 18: č. 3. ISSN 1212-3609. Dostupné z: doi:10.15240/tul/001/2015-3-014

VŠE, 2015. *MBI – koncepce a návod k použití.* [online]. In: *Vysoká škola ekonomická.* (PPTX). 2015. [cit. 2022-08-09]. Dostupné z: https://mbi.vse.cz/mbi/files/help.pptx

Vyhláška č.82/2018 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), 2018. In: *Sbírka zákonů*. Částka č. 43/2018 Sb. [cit. 2023-03-28]. Dostupné také z: https://www.nukib.cz/download/publikace/legislativa/vkb_82-2018sb.pdf

Vyhláška č.317/2014 Sb., Vyhláška o významných informačních systémech a jejich určujících kritériích, 2014. In: *Sbírka zákonů*. Částka č. 127/2014 Sb. [cit. 2023-09-21]. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-317

Vyhláška č.437/2017 Sb., Vyhláška o kritériích pro určení provozovatele základní služby, 2017. In: *Sbírka zákonů*. Částka č. 157/2017 Sb. [cit. 2023-02-21]. Dostupné také z: https://www.zakonyprolidi.cz/cs/2017-437

Zákon č.110/2019 Sb., Zákon o zpracování osobních údajů, 2019. In: *Sbírka zákonů*. Částka č.47/2014 Sb. [cit. 2023-01-19]. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

Zákon č.181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), 2022. In: *Sbírka zákonů*. Částka č.75/2014 Sb. [cit. 2022-07-19]. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-365?text=181

Zákon č. 365/2000 Sb., Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů, 2000. In: *Sbírka zákonů*. Částka č.99/2000 Sb. [cit. 2023-05-25]. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-365/zneni-20230401

Zákon č. 372/2011 Sb., Zákon o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách), 2011. In*: Sbírka zákonů*. Částka č.131/2011 Sb. [cit. 2023-02-10]. Dostupné také z: https://www.zakonyprolidi.cz/cs/2011-372

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

Obrázek 1 Vnímání podniku jako systému....15
Obrázek 2 Komponenty informačního systému....16
Obrázek 3 Typická struktura současného IS....17
Obrázek 4 Rozsah ISMS varianta A, B, C....21
Obrázek 5 PDCA....23
Obrázek 6 Přiměřená úroveň nákladů na ISMS....25
Obrázek 7 Prostor ISMS....29
Obrázek 8 Ilustrace procesu řízení rizik bezpečnosti informací....37
Obrázek 9 Tříúrovňová hierarchie modelu MBI....43
Obrázek 10 Přehled objektů a jejich hierarchická struktura a vazby....44
Obrázek 11 Datový model pro analýzu rizik....46
Obrázek 12 Právní rámec poskytování zdravotní péče....49
Obrázek 13 Organizační struktura mikropodniku....52
Obrázek 14 EPC model zdravotní péče v ambulanci praktického lékaře....60
Obrázek 15 Schéma platformy IS mikropodniku....62
Obrázek 16 Informační tok v IS....63
Obrázek 17 Use case (lékař – pacient)....64
Obrázek 18 Primárních aktiva a jejich souvislost....76
Obrázek 19 Řízení rizik v mikropodniku....81
Obrázek 20 Návrh metodiky bezpečnosti IS v mikropodniku....93

8.2 Seznam tabulek

Tabulka 1 SWOT analýza....56
Tabulka 2 Manipulace (operace) s informacemi v ambulanci VPL....66
Tabulka 3 Ukázka zpracování „Prohlášení o aplikovatelnosti ISMS“....67
Tabulka 4 Role ISMS návrh části RACI matice....70
Tabulka 5 Přehled souvislostí primárních a podpůrných aktiv....77
Tabulka 6 Registr primárních aktiv ambulance VPL....78
Tabulka 7 Ukázka katalogu identifikovaných hrozeb....82
Tabulka 8 Ukázka katalogu zranitelností....83
Tabulka 9 Matice rizik pro primární aktivum PA s dopadem DO = 4....84
Tabulka 10 Registr rizik pro potřeby DP....86
Tabulka 11 Míra rizika účinků hrozby působící na aktiva....92

8.3 Seznam grafů

Graf 1 Počáteční stav plnění opatření ISMS....57
Graf 2 GAP analýza – porovnání počátečního stav ISMS k cílovému stavu PoA....58

8.4 Seznam použitých zkratek

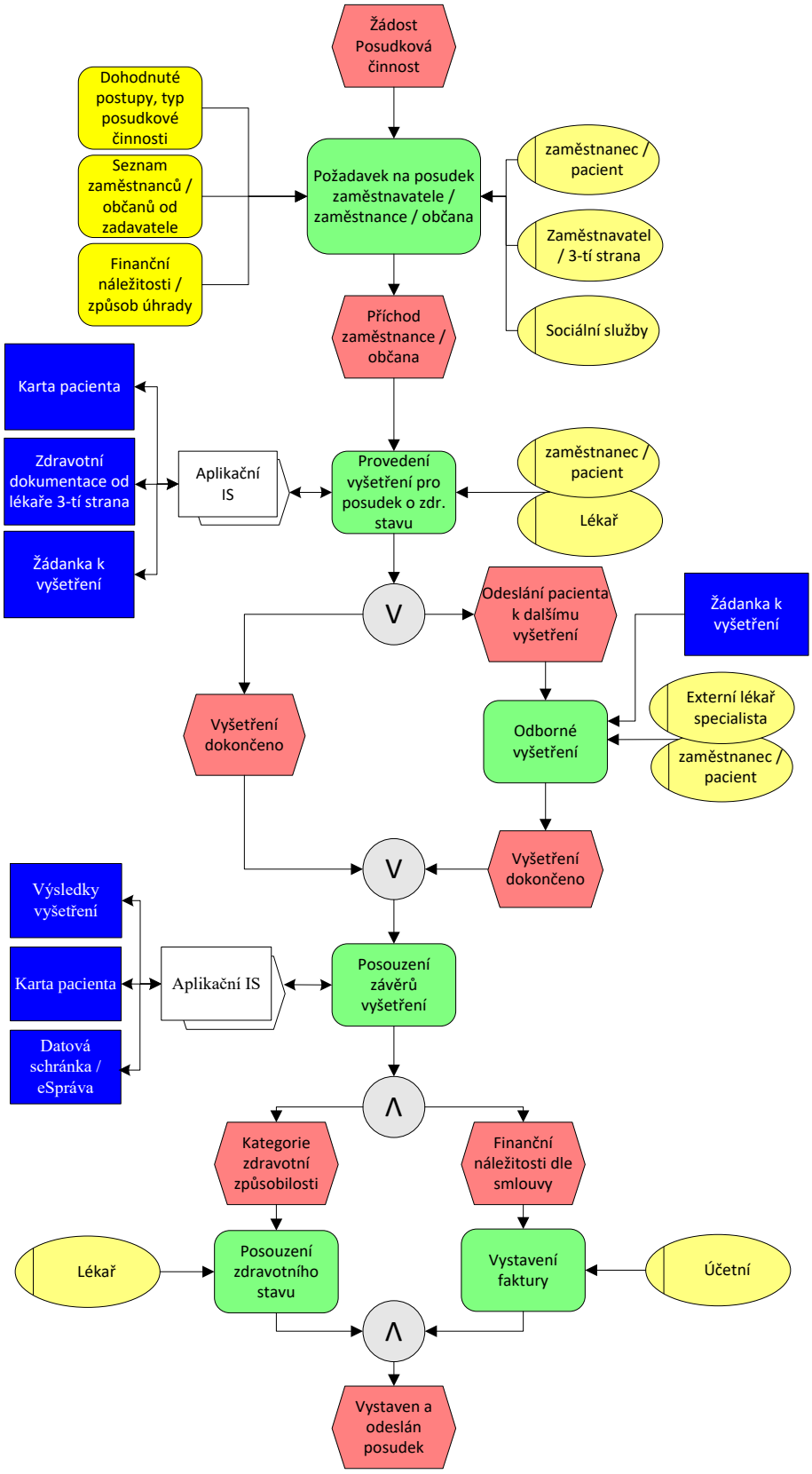
B2A	obchodní vztah business to administration
B2B	obchodní vztah business to business
B2C	obchodní vztah business to consumer
B2G	obchodní vztah business to goverment
BI	bezpečnost informací
BOZP	bezpečnost a ochrana zdraví při práci
CIA	Confidentiality, Integrity, Availability
COBIT	metodika Control Objectives for Information and related Technology
ČLK	Česká lékařská komora.
ČR	Česká republika
ČSN	chráněné označení českých technických norem
ČSSZ	Česká správa sociálního zabezpečení
ČZU	Česká zemědělská univerzita
DO	Míra dopadu
EPC	Event-driven Process Chain
EU	Evropská unie
EZS	elektronický zabezpečovací systém
GDPR	obecné nařízení o ochraně osobních údajů
HW	hardware
Hx	x-tá hrozba
ICT	informační a komunikační technologie
IS	informační systém
ISMS	systém řízení bezpečnosti informací
ISO	International Organization for Standardization
ISO/IEC	ČSN EN ISO/IEC
IT	informační technologie
ITIL	metodika Information Technology Infrastructure Library
KB	kybernetická bezpečnost
KII	kritická informační infrastruktura
LAN	Local Area Network – lokální počítačová síť
MBI	Management Byznys Informatiky

MZČR	Ministerstvo zdravotnictví České republiky
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OS	operační systém
PA	primární aktivum
PDCA	Plan, Do, Check a Act
PO	požární opatření
POA	podpůrné aktivum
PoA	prohlášení o aplikovatelnosti
RACI	matice zodpovědnosti
Rx	x-té riziko
SPL	společnost praktických lékařů
SVL	společnost všeobecného lékařství
SW	software
SWOT	analýza Strengths – Weaknesses – Opportunities – Threats
UPS	Uninterruptible Power Supply – záložní zdroj napájení
ÚZIS	Ústav zdravotnických informací a statistiky ČR
VDSL	Very High Speed DSL
VIS	významný informační systém
VKB, VoKB	vyhláška o zákoně kybernetické bezpečnosti, Vyhláška č.82/2018 Sb.
VPN	virtual private network
VPL	všeobecný praktický lékař
VŠE	Vysoká škola ekonomická
WLAN	Wireless Local Area Network
WPA2	pokročilý standard pro zabezpečení bezdrátových sítí
ZKB, ZoKB	zákon o kybernetické bezpečnosti, Zákon č.181/2014 Sb.
Zx	x-tá zranitelnost

Přílohy

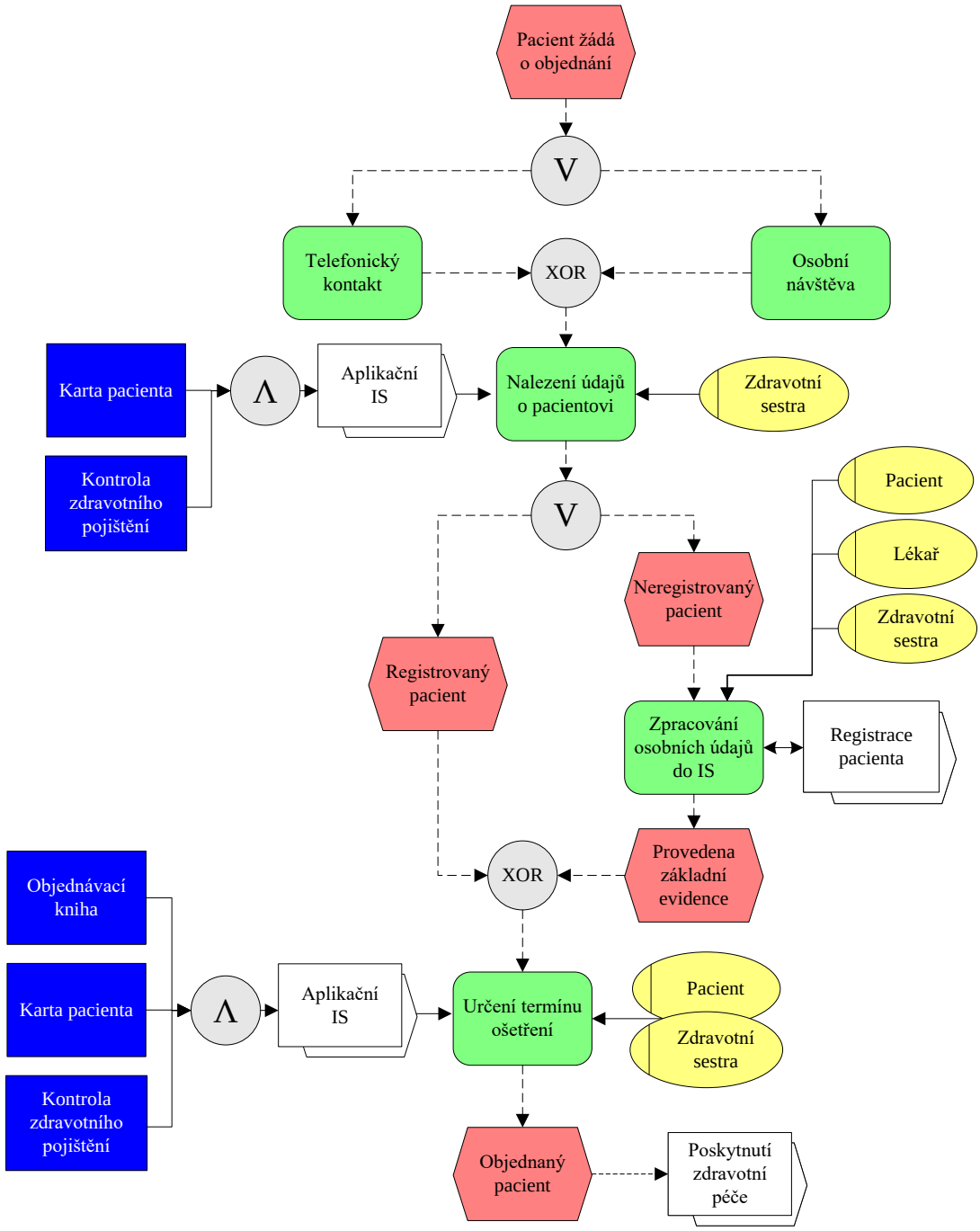
Příloha 1 - EPC model posudková činnost 116
Příloha 2 - EPC model objednání pacienta 117
Příloha 3 - EPC model zpracování osobních informací při registraci pacienta 118
Příloha 4 - Identifikovaná vybraná podpůrná aktiva. 119
Příloha 5 - Stupnice pro hodnocení aktiv důvěrnosti, integrity a dostupnosti. 120
Příloha 6 - Stupnice hodnocení hrozeb a zranitelností 121
Příloha 7 - Katalog identifikovaných hrozeb 122
Příloha 8 - Katalog identifikovaných zranitelností 123
Příloha 9 - Matice souvislostí hrozeb využívajících zranitelností 124
Příloha 10 - Matice rizik pro primární aktiva s hodnocením CIA DO = 4 125
Příloha 11 - Matice rizik pro primární aktiva s hodnocením CIA DO = 3 126
Příloha 12 - PoA s popisem vlastních navrhnutých opatření 127
Příloha 13 - Návrh politiky ISMS 136
Příloha 14 - Plán kontinuity ISMS v mikropodniku 138
Příloha 15 - Návrh směrnice uživatele IS 141
Příloha 16 - Přehled nákladů užitých opatření 145

Příloha 1 - EPC model posudková činnost



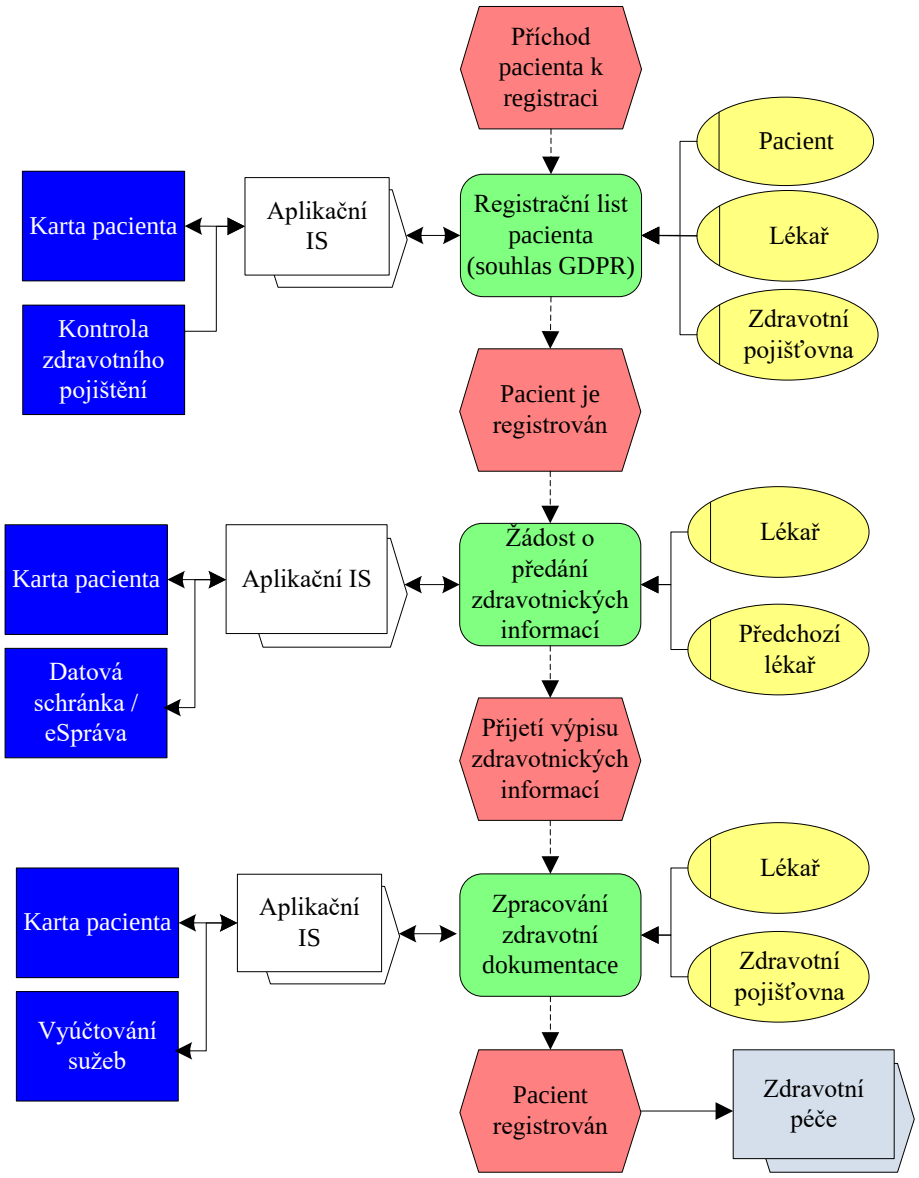
Zdroj: vlastní zpracování

Příloha 2 - EPC model objednání pacienta



Zdroj: vlastní zpracování

Příloha 3 - EPC model zpracování osobních informací při registraci pacienta



Zdroj: vlastní zpracování

Příloha 4 - Identifikovaná vybraná podpůrná aktiva.

Kategorie podpůrného aktiva	Skupina podpůrného aktiva	Typ podpůrného aktiva	Popis podpůrného aktiva	Váha vlivu	Váha kategorie
Diagnostické přístroje		EKG	Přístroj pro měření elektrické aktivity srdce - elektrokardiografie pacienta. Přenos dat přes USB port počítače do aplikačního SW.	3	**3**
		Tlakový Holter	Přístroj k ambulantní monitorování krevního tlaku pacienta. Přenos dat z přístroje do aplikačního SW.	2	
		Oxymetr	Přístroj k měření okysličení krve pacienta a přenosem do aplikačního SW.	2	
		POCT systém	K měření CRP, iFOB, SterpTest, INR pacienta a zaznameníní informací do aplikačního SW.	3	
		Měřič tlaků	Přístroj k měření kotníkových tlaků - screening ischemické choroby dolních končetin.	2	
		Teploměr laserový	Manuální měření teploty pacienta.	2	
		Váha	Měření hmotnosti pacientů s připojením do aplikačního SW.	2	
		Teploměr technický	Monitorování teploty fyzických prostorů ambulance praktického lékaře, uchovávání léčiv, očkovacích látek a zdravotnického materiálu.	3	
Komunikační prostředky	Komunikační sítě	internetové připojení	Mobilní:LTE, 5G. Bezdrátové: WIFI. Pevné:ADSL, ethernet, optika.	3	**2**
		Bezdrátová komunikace	Bluetooth, RFID.	2	
	Strukturovaná kabeláž	Síťové a telefonní kabely	Strukturovaná kabeláž se využívá k přenosu dat do zařízení, propojení v rámci lokáln sítě a telefonickým hovorům.zásuvky RJ45, RJ 11.	3	
		Propojovací kabely	Propojení mezi pracovní stanicí, notebokem a zásuvkou, monitorem, diagnostickým přístrojem či telefoním přístrojem a infarstrukturou.	2	
	Síťová zařízení	Směřovač (router)	Přesměrovává komunikaci do jiného segmentu stejného typu sítě.	2	
		Síťový most (bridge)	Spojuje dva fyzicky oddělené segmenty sítě.	2	
		HW/SW firewall	Zařízení pro ochranu provozu v sítích.	3	
Systémový SW	Uživatelský SW	Operační systém	Základní programové vybavení počítače. Zajišťuje komunikace mezi hardware a software a uživatelem.	3	**4**
		Integrační platforma	Software, který primárné slouží k výkon hlavní činnosti organizace, například aplikačním SW SMARTMEDIX.	4	
	Bezpečnostní SW	Antivir	Integrovaná funkcionalita MS WINDOWS nebo aplikace třetí strany pro ochranu malware.	3	
		Zálohovací SW	SW pro zálohování dat na externí paměťové zařízení nebo do cloudu pro obnovu funkcionality OS a aplikačního SW.	3	
	Firmware	Diagnostické přístroje	Upgrade firmware pro zlepšení schopostí přístroje, zabezpečení komunikačního rozhraní přístroje s počítačem.	3	
		Počítače	Upgrade BIOSu pracovní stanice, notebooku a firmware externích zařízení.	3	
		Síťová zařízení	Upgrade firmware, aktualizace funkcionality nových bezpečnostních a provozních funkcí síťového zařízení.	3	

Zdroj: vlastní zpracování, NÚKIB (2022c)

Příloha 5 - Stupnice pro hodnocení aktiv důvěrnosti, integrity a dostupnosti.

Stupnice pro hodnocení důvěrnosti

Úroveň		Popis
1	Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.
2	Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.
3	Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (např. obchodní tajemství, osobní údaje).
4	Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).

Stupnice pro hodnocení integrity

Úroveň		Popis
1	Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.
2	Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.
3	Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.
4	Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.

Stupnice pro hodnocení dostupnosti

Úroveň		Popis
1	Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).
2	Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.
3	Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována jako velmi důležitá.
4	Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována jako kritická.

Zdroj: vlastní zpracování, VKB (2018, příloha č.1)

Příloha 6 - Stupnice hodnocení hrozeb a zranitelností

Stupnice hodnocení hrozeb

Úroveň		Popis hrozby
1	Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
2	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
3	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
4	Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Stupnice hodnocení zranitelnosti

Úroveň		Popis zranitelnosti
1	Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
2	Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena.Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
3	Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována.Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4	Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Zdroj: vlastní zpracování, VKB (2018, příloha č.2)

Příloha 7 - Katalog identifikovaných hrozeb

Hx	Název hrozby	Hodnota Hx	Činnost, která hrozbu může naplnit
H01	Porušení bezpečnostní politiky IS.	3	Činnost uživatele a administrátora, která neodpovídá nastavenému způsobu užívání IS, operací s informací (manipulace se zdravotnickou dokumentací) a posyktování zdravotní péče. Provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administratorů.
H02	Poškození, selhání technického nebo HW vybavení.	3	Úmyslné, nezaviněné, náhodné selhání hardwarových součástí IS, diagnostických přístrojů (nevhodná manipulace, přepětí v el.síti, krádež a jiné).
H03	Poškození, selhání SW a OS.	3	Cílená snaha o narušení integrity SW, nevhodný update verze SW, chybná aktualizace OS nekompaktibilní s aplikačním SW (SmartMedix), Užívání SW třetích stran, které nejsou schváleny pro provoz v organizaci a nejsou uvedeny v bezpečnostní politice jako povolený SW může způsobit nedostupnost aplikačního IS.
H04	Zneužití identity jiné fyzické osoby.	3	Úmyslné/neúmyslné využití identity lékaře sestrou. Nesystémové nastavení opravnění jednotlivýh uživatelů IS. Neopravněná manipulace s dokumenty, vydáváním receptu, neschopenky, noprávněné zastupování v identifikováných činnostech při manipulaci s informacemi.
H05	Kybernetický útok z vnější komunikační sítě.	4	Útok hackera z cílem narušit aplikační IS - dostupnost připojení k internetu, integritu IS a důvěrnost informací v síti.
H06	Škodlivý kód.	4	Selhání antivirové ochrany, nevhodné chování uživatele v prostředí internetu a emailové komunikaci, užívání neprověřených externích nosičů dat. Škodlivý kód - malware, spyware, aj.
H07	Nedostupnost služby poskytované aplikačním IS.	3	Nefunkční přenos informací z diagnostických přístrojů. Nefunkční tisk, skenování, manipulace s informacemi. Narušení integrity a dostupnosti služeb poskytující citlivé a důvěrné zdravotnické informace.
H08	Nedostupnost komunikačních služeb.	2	Nedostupnost, narušení integrity a důvěrnosti připojení do komunikačího prostředí sítě internet, přerušení pevné linky telekomunikačních služeb.
H09	Neoprávněná modifikace informací v aplikačním IS.	2	Porušení důvěrnosti, integrity a dostupnosti zdravotnických informací v IS. V daném případě se jedná modifikaci informací v SW SmartMedix.
H10	Ztráta, zneužití certifikátu s heslem.	2	Stráta kontontroly nad kvalifikovaným a komerčním certifikátem způsobená manipulací při ukládání certifikátu na veřejném nezabezpečeném úložišti, uložení na přenosné médium, které nemám pod stálou kontrolou.
H11	Zneužití, porucha přenosných nosičů dat.	3	Krádež po narušení fyzické bezpečnosti objektu, přepětí v elektrické síti, škodlivý kód, ztráta mimo objekt organizace, předání nosiče dat neoprávněné osobě.
H12	Nedostupnost technické a softwarové pomoci dodavatelů.	2	Omezená pracovní doba dodavatelů, chybějící / nevhodný / nedostatečný smluvní vztah o poskytování služeb. Vysoké finanční náklady, které nejsou akcepotvatelné.
H13	Nedostupnost agendních IS.	3	Porucha připojení IS k externí síti (internet), Porucha informačních sytémů eNeschopenka, eRecept, ePortál ČSSZ, WebLIMS, MEX, eSpráva aj.
H14	Ztráta, poškození, odcizení elektronické zdravotní dokumentace.	4	Manipulace s elektronickou zdravotní kartou (dokumentací) pacienta, kdy může dojít vrámci činnosti ambulance k odeslání / přijetí / přenášení nezabezpečeným způsobem, zneužití identity jiné osoby k průniku do aplikačního IS, kopírováním dat neoprávněnou osobou z nezabezpečeného nosiče dat.
H15	Ztráta, poškození, odcizení papírové zdravotní dokumentace.	4	Manipulace s papírovou zdravotní kartou (dokumentací) pacienta nestandartním způsobem. Zaslání dokumentace posudkovému / reviznímu lékaři nezabezpečeným způsobem (obyčejný dopis). Havárie technických podpůrných zdrojů, požár. Narušení fyzické ochrany objektu - krádež.
H16	Neprovedení revize technických a diagnostických zařízení .	2	Včasnost a periodicita provádění pravidelných revizí elektrických přístrojů, technického vybavení, HW a kalibrace nasmlouvaných diagnostických zdravotnických přístrojů a techniky.
H17	Manipulace / operace s zdravotnickou dokumentací.	3	Neoprávněné sdělení o zdravotním stavu pacienta po telefonu neověřené /nepověřené osobě. Jiný pacien v ambulaci nahlíží do zdravotní dokumentace pacienta.
H18	Narušení fyzické bezpečnosti.	3	Nedostatečné zabezpečení okeních a vstupních otvorů, nefunkční / nevhodný elektronický zabezpečovací systém. Havárie technických podpůrných zdrojů, požár.
H19	Nedostupnost služeb zdravotní pojišťovny.	2	Neuzavřená smlouva o poskytování zdravotních služeb, neautorizované doplňky smluv, nenasmlouvané zdravotnické výkony a diagnostické přístroje.
H20	Porucha či nedostupnost tiskových a skenovacích zařízení.	3	Výpadek elektrické energie, nedotatek toneru, chyba na komunikačním portu zařízení, nenainstalované/odinstalované zařízení z aplikačního IS.
H21	Porucha dodávek elektrické energie,vody, vytápění.	2	Havárie zdrojů, přerušení smluvních dodávek, požár.
H22	Nedostupnost replikace databáze aplikačního IS.	3	Nedostupnost muže být zapříčiněna souvislostí s výpadkem elektrické energie, komunikačního prostředí, pokytovatele outsorcingových služeb. Porucha SW a HW aplikačního IS.
H23	Neposkytování zdravotní péče	4	Onemocnění lékaře, sestry. Ukončení pracovní smlouvy s personálem. Chybějící role odborného garanta zdravotní péče.

Zdroj: vlastní zpracování

Příloha 8 - Katalog identifikovaných zranitelností

Zx	Název zranitelnosti	Hodnota Zx
Z01	Nedostatečné provádění a vyhodnocování auditů, preventivních a servisních kontrol.	2
Z02	Nedostatečné stanovení bezpečnostních pravidel, práv a povinností uživatelů, administrátorů a bezpečnostních rolí.	3
Z03	Nevhodné nastavení přístupových oprávnění.	3
Z04	Nedostatečná ochrana a správa aktiv.	3
Z05	Přístupnost papírové dokumentace na pracovišti.	3
Z06	Nedostatek identifikace a autentizace odesílatele a příjemce informací.	4
Z07	Nedostatečná ochrana vnějšího perimetru.	3
Z08	Nevhodná fyzická ochrana budovy, prostorů ambulance, kontroly vstupů osob.	2
Z09	Nedostatek kontroly aktiv mimo objekt.	2
Z10	Nedostatek procesu účtování výkonů zdravotní péče.	2
Z11	Nedostatek při manipulaci s informacemi plynoucí z činnosti organizace.	4
Z12	Nedostatek odborného personálu.	4
Z13	Nedostatečné nastavení, správa a ochrana uživatelských hesel.	2
Z14	Neodhlášení uživatele z aplikačního IS při opuštění pracovní stanice.	3
Z15	Nedostatečné školení z informační bezpečsnoti zaměstnanců.	2
Z16	Nedostatek právní formulace uzavření dodavatelské smlouvy.	2

Zdroj: vlastní zpracování

Příloha 9 - Matice souvislostí hrozeb využívajících zranitelností

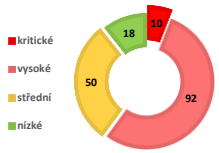
MATICE suvislostí hrozba / zranitelnost		ID	Z01	Z02	Z03	Z04	Z05	Z06	Z07	Z08	Z09	Z10	Z11	Z12	Z13	Z14	Z15	Z16
		Kategorie zranitelnosti	Nedostatečné provádění a vyhodnocování auditů, preventivních a servisních kontrol.	Nedostatečné stanovení bezpečnostních pravidel, práv a povinností uživatelů, administrátorů a bezpečnostních rolí.	Nevhodné nastavení přístupových oprávnění.	Nedostatečná ochrana a správa aktiv.	Přístupnost papírové dokumentace na pracovišti.	Nedostatek identifikace a autentizace odesílatele a příjemce informací.	Nedostatečná ochrana vnějšího perimetru.	Nevhodná fyzická ochrana budovy, prostorů ambulance, kontroly vstupů osob.	Nedostatek kontroly aktiv mimo objekt	Nedostatek procesu účtování výkonů zdravotní péče.	Nedostatek při manipulaci s informacemi plynoucí z činnosti organizace.	Nedostatek odborného personálu.	Nedostatečné nastavení, správa a ochrana uživatelských hesel.	Neodhlášení uživatele z aplikačního IS při opuštění pracovní stanice.	Nedostatečné školení z informační bezpečnosti zaměstnanců.	Nedostatek právní formulace uzavření dodavatelské smlouvy.
ID	Kategorie hrozeb	Hx /Zx	2	3	3	3	3	4	3	2	2	2	4	4	2	3	2	2
H01	Porušení bezpečnostní politiky IS.	3	A	A	A	A	A	A	A	A	A	A	A		A	A	A	
H02	Poškození, selhání technického nebo HW vybavení.	3	A	A		A			A	A	A	A	A				A	
H03	Poškození, selhání SW a OS.	3	A	A	A	A		A	A		A	A	A		A	A	A	
H04	Zneužití identity jiné fyzické osoby.	3		A	A	A	A	A					A			A	A	
H05	Kybernetický útok z vnější komunikační sítě.	4	A	A	A	A		A	A		A	A	A	A	A		A	A
H06	Škodlivý kód.	4	A			A			A		A		A		A		A	
H07	Nedostupnost služby poskytované aplikačním IS.	3	A		A							A	A					A
H08	Nedostupnost komunikačních služeb.	2	A			A			A	A		A	A					A
H09	Neoprávněná modifikace informací v aplikačním IS.	2		A	A	A					A	A	A		A	A	A	
H10	Ztráta, zneužití certifikátu s heslem.	2			A	A		A			A		A		A		A	A
H11	Zneužití, porucha přenosných nosičů dat.	3			A	A				A	A		A			A	A	
H12	Nedostupnost technické a softwarové pomoci dodavatelů.	2					A		A					A				A
H13	Nedostupnost agendních IS.	3						A				A	A					A
H14	Ztráta, poškození, odcizení elektronické zdravotní dokumentace.	4	A	A	A	A		A	A		A	A	A		A	A	A	A
H15	Ztráta, poškození, odcizení papírové zdravotní dokumentace.	4	A			A	A	A	A	A	A	A	A				A	
H16	Neprovedení revize technických a diagnostických zařízení .	2	A				A							A				A
H17	Manipulace / operace s zdravotnickou dokumentací.	3			A	A	A	A			A		A			A	A	
H18	Narušení fyzické bezpečnosti.	3	A		A		A			A					A		A	
H19	Nedostupnost služeb zdravotní pojišťovny.	2			A			A				A		A				A
H20	Porucha či nedostupnost tiskových a skenovacích zařízení.	3	A				A					A	A					
H21	Porucha dodávek elektrické energie,vody, vytápění.	2				A			A									A
H22	Nedostupnost replikace databáze aplikačního IS.	3	A			A					A							A
H23	Neposkytování zdravotní péče	4				A	A	A				A		A				A

Zdroj: vlastní zpracování

Příloha 10 - Matice rizik pro primární aktiva s hodnocením CIA DO = 4

MATICE RIZIK PAx pro DO = 4

ROZLOŽENÍ HODNOCENÍ RIZIK



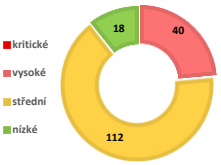
ID	Kategorie hrozeb	Hx /Zx	Z01 Nedostatečné provádění a vyhodnocování auditů, prevenčních a servisních kontrol.	Z02 Nedostatečné stanovení bezpečnostních pravidel, práv a povinností uživatelů, administrátorů a bezpečnostních rolí.	Z03 Nevhodné nastavení přístupových oprávnění.	Z04 Nedostatečná ochrana a správa aktiv.	Z05 Přístupnost papírové dokumentace na pracovišti.	Z06 Nedostatek identifikace a autentizace odesílatele a příjemce informací.	Z07 Nedostatečná ochrana vnějšího perimetru.	Z08 Nevhodná fyzická ochrana budovy, prostorů ambulancí, kontroly vstupu osob.	Z09 Nedostatek kontroly aktiv mimo objekt.	Z10 Nedostatek procesu účtování výkonů zdravotní péče.	Z11 Nedostatek při manipulaci s informacemi plynoucí z činnosti organizace.	Z12 Nedostatek odborného personálu.	Z13 Nedostatečné nastavení, správa a ochrana uživatelských hesel.	Z14 Neodhlášení uživatele z aplikačního IS při opuštění pracovní stanice.	Z15 Nedostatečné školení z informační bezpečnosti zaměstnanců.	Z16 Nedostatek právní formulace uzavření dodavatelské smlouvy.	Počet rizik s mírou hodnocení VYSOKÉ a KRITICKÉ
			2	3	3	3	3	4	3	2	2	2	4	4	2	3	2	2	102
H01	Porušení bezpečnostní politiky IS.	3	24	36	36	36	36	48	36	24	24	24	48		24	36	24		8
H02	Poškození, selhání technického nebo HW vybavení.	3	24	36		36			36	24	24	24	48				24		4
H03	Poškození, selhání SW a OS.	3	24	36	36	36		48	36		24	24	48		24	36	24		7
H04	Zneužití identity jiné fyzické osoby.	3		36	36	36	36	48					48			36	24		7
H05	Kybernetický útok z vnější komunikační sítě.	4	32	48	48	48		64	48		32	32	64	64	32		32	32	13
H06	Škodlivý kód.	4	32			48			48		32		64		32		32		7
H07	Nedostupnost služby poskytované aplikačním IS.	3	24		36							24	48					24	2
H08	Nedostupnost komunikačních služeb.	2	16			24			24	16		16	32					16	1
H09	Neoprávněná modifikace informací v aplikačním IS.	2		24	24	24					16	16	32		16	24	16		1
H10	Ztráta, zneužití certifikátu s heslem.	2			24	24		32			16		32		16		16	16	2
H11	Zneužití, porucha přenosných nosičů dat.	3			36	36				24	24		48			36	24		4
H12	Nedostupnost technické a softwarové pomoci dodavatelů.	2					24		24					32				16	1
H13	Nedostupnost agendních IS.	3						48				24	48					24	2
H14	Ztráta, poškození, odcizení elektronické zdravotní dokumentace.	4	32	48	48	48		64	48		32	32	64		32	48	32	32	13
H15	Ztráta, poškození, odcizení papírové zdravotní dokumentace.	4	32			48	48	64	48	32	32	32	64				32		10
H16	Neprovedení revize technických a diagnostických zařízení .	2	16				24							32				16	1
H17	Manipulace / operace s zdravotnickou dokumentací.	3			36	36	36	48			24		48			36	24		6
H18	Narušení fyzické bezpečnosti.	3	24		36		36			24					24		24		2
H19	Nedostupnost služeb zdravotní pojišťovny.	2			24			32				16		32				16	2
H20	Porucha či nedostupnost tiskových a skenovacích zařízení.	3	24				36					24	48						2
H21	Porucha dodávek elektrické energie,vody, vytápění.	2				24			24									16	0
H22	Nedostupnost replikace databáze aplikačního IS.	3	24			36					24							24	1
H23	Neposkytování zdravotní péče	4				48	48	64				32		64				32	6

Zdroj: vlastní zpracování

Příloha 11 - Matice rizik pro primární aktiva s hodnocením CIA DO = 3

MATICE RIZIK PAx pro DO = 3

ROZLOŽENÍ HODNOCENÍ RIZIK



ID	Kategorie hrozeb	Hx /Zx	Z01 Nedostatečné provádění a vyhodnocování auditů, preventivních a servisních kontrol.	Z02 Nedostatečné stanovení bezpečnostních pravidel, práv a povinností uživatelů, administrátorů a bezpečnostních rolí.	Z03 Nevhodné nastavení přístupových oprávnění	Z04 Nedostatečná ochrana a správa aktiv.	Z05 Přístupnost papírové dokumentace na pracovišti.	Z06 Nedostatek identifikace a autentizace odesílatele a příjemce informací.	Z07 Nedostatečná ochrana vnějšího perimetru.	Z08 Nevhodná fyzická ochrana budovy, prostorů ambulance, kontroly vstupů osob.	Z09 Nedostatek kontroly aktiv mimo objekt.	Z10 Nedostatek procesu účtování výkonů zdravotní péče.	Z11 Nedostatek při manipulaci s informacemi plynoucí z činnosti organizace.	Z12 Nedostatek odborného personálu.	Z13 Nedostatečné nastavení, správa a ochrana uživatelských hesel.	Z14 Nevdělkání uživatele z aplikačního IS při opuštění pracovní stanice.	Z15 Nedostatečné školení z informační bezpečnosti zaměstnanců.	Z16 Nedostatek právní formulace uzavření dodavatelské smlouvy.	Počet rizik s mírou hodnocení VYSOKÉ a KRITICKÉ
		Kategorie zranitelnosti	2	3	3	3	3	4	3	2	2	2	3	4	2	3	2	2	40
H01	Porušení bezpečnostní politiky IS.	3	18	27	27	27	27	**36**	27	18	18	18	**36**		18	27	18		2
H02	Poškození, selhání technického nebo HW vybavení.	3	18	27		27			27	18	18	18	**36**				18		1
H03	Poškození, selhání SW a OS.	3	18	27	27	27		**36**	27		18	18	**36**		18	27	18		2
H04	Zneužití identity jiné fyzické osoby.	3		27	27	27	27	**36**					**36**			27	18		2
H05	Kybernetický útok z vnější komunikační sítě.	4	24	**36**	**36**	**36**		**48**	**36**		24	24	**48**	**48**	24		24	24	7
H06	Škodlivý kód.	4	24			**36**			**36**		24		**48**		24		24		3
H07	Nedostupnost služby poskytované aplikačním IS.	3	18		27							18	**36**					18	1
H08	Nedostupnost komunikačních služeb.	2	12			18			18	12		12	24					12	0
H09	Neoprávněná modifikace informací v aplikačním IS.	2		18	18	18					12	12	24		12	18	12		0
H10	Ztráta, zneužití certifikátu s heslem.	2			18	18		24			12		24		12		12	12	0
H11	Zneužití, porucha přenosných nosičů dat.	3			27	27				18	18		**36**			27	18		1
H12	Nedostupnost technické a softwarové pomoci dodavatelů.	2					18		18					24				12	0
H13	Nedostupnost agendních IS.	3						**36**				18	**36**					18	2
H14	Ztráta, poškození, odcizení elektronické zdravotní dokumentace.	4	24	**36**	**36**	**36**		**48**	**36**		24	24	**48**		24	**36**	24	24	7
H15	Ztráta, poškození, odcizení papírové zdravotní dokumentace.	4	24			**36**	**36**	**48**	**36**	24	24	24	**48**				24		5
H16	Neprovedení revize technických a diagnostických zařízení .	2	12				18							24				12	0
H17	Manipulace / operace s zdravotnickou dokumentací.	3			27	27	27	**36**			18		**36**			27	18		2
H18	Narušení fyzické bezpečnosti.	3	18		27		27			18					18		18		0
H19	Nedostupnost služeb zdravotní pojišťovny.	2			18			24				12		24				12	0
H20	Porucha či nedostupnost tiskových a skenovacích zařízení.	3	18				27					18	**36**						1
H21	Porucha dodávek elektrické energie,vody, vytápění.	2				18			18									12	0
H22	Nedostupnost replikace databáze aplikačního IS.	3	18			27					18							18	0
H23	Neposkytování zdravotní péče	4				**36**	**36**	**48**				24		**48**				24	4

Zdroj: vlastní zpracování

Příloha 12 - PoA s popisem vlastních navrhnutých opatření

Kapitola normy	Cíle opatření	Aplikova-telnost	Vlastní opatření k splnění cíle	Počáteční stav
A.5	**Politiky bezpečnosti informací**			
A.5.1	**Směřování bezpečnosti informací vedením organizace**			
Cíl: Určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky týkající se činnosti organizace, příslušnými zákony a směrnicemi.				
A.5.1.1	Politiky pro bezpečnost informací	Ano	Vytvoření politiky ISMS (příloha 13), politiky bezpečnosti IS(DP kap.4.9.5)	částečně
A.5.1.2	Přezkoumání politik pro bezpečnost informací	Ano	Hodnocení aktuálního stavu dle navrhnuté politiky ISMS a PoA pomocí GAP analýzy (DP kap. 4.4)	částečně
A.6	**Organizace bezpečnosti informací**			
A.6.1	**Interní organizace**			
Cíl: Ustavit rámec pro zahájení a řízení implementace a provozování informační bezpečnosti v organizaci.				
A.6.1.1	Role a odpovědnosti bezpečnosti informací	Ano	Stanovení bezpečnostní správu dle ISO 27002. Role jsou rozdělné na interní a externí dle návrhu v DP kap. 4.6.4.	částečně
A.6.1.2	Princip oddělení povinností	Ano	Výkon bezpečnostních rolí by měl být neslučitelný. Snížení rizika zneužití aktiv organizace. Administrátor IS je určen jednatelem organizace.	neužívá
A.6.1.3	Kontakt s příslušnými orgány a autoritami	Ano	Jedná se především o dodavatele, zdravotní pojišťovny, ČSSZ, ÚZIS, komunikace s agendními IS kvalifikovaným certifikátem, aj.	užívá
A.6.1.4	Kontakt se zájmovými skupinami	Ano	Lékař má povinnost být členem ČLK – Česká lékařská komora. Nepovinné členství – SPL sdružení praktických lékařů, SVL – společnost všeobecných lékařů. Smluvní kontakt s ZP.	užívá
A.6.1.5	Bezpečnost informací v řízení projektů	NE	Organizace neorganizuje.	neorganizuje
A.6.2	**Mobilní zařízení a práce na dálku**			
Cíl: Zajistit bezpečnost při použití mobilních zařízení a pro práci na dálku.				
A.6.2.1	Politika mobilních zařízení	Ano	Lékař užívá SW SmartMedix na notebooku i mimo objekt organizace. Politika účtů na OS Windows a řízený přístup do aplikačního prostředí, replikace databáze, automatické zálohování informací, antivirová ochrana.	částečně
A.6.2.2	Práce na dálku	Ano	Databáze aplikačního SW užívá replikace. Elektronické soubory jsou zálohovány na cloud. Instalovaný SW TeamViewer pro vzdálený přístup do PC pro administrátora aplikačního SW – outsourcing za přítomnosti administrátora IS organizace.	částečně
A.7	**Bezpečnost lidských zdrojů**			
A.7.1	**Před vznikem pracovního vztahu**			
Cíl: Zajistit, aby zaměstnanci a smluvní strany byli srozuměni se svými povinnostmi a aby pro jednotlivé role byli vybráni vhodní kandidáti.				
A.7.1.1	Prověřování	Ano	Výpis z rejstříku trestů, vzdělání, životopis, potřebné certifikáty kvalifikace, informace od předchozího zaměstnavatele, pohovor.	užívá
A.7.1.2	Podmínky pracovního vztahu	Ano	Pracovní smlouva, Souhlas s pracovní řádem, BOZP, GDPR, vzdělání zaměstnance a jiné.	užívá

A.7.2	**Během pracovního vztahu**			
Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi a plnili si svoje povinnosti v oblasti bezpečnosti informací.				
A.7.2.1	Odpovědnosti vedení organizace	Ano	Jednatel vyžaduje nastavení ISMS/GDPR v organizaci a požaduje od dodavatelů.	částečně
A.7.2.2	Povědomí, vzdělání a školení bezpečnosti informací	Ano	Každoroční školení založené na znalosti IS, aktiv organizace, informační bezpečnosti – školení z provozní bezpečnosti IS, GDPR.	částečně
A.7.2.3	Disciplinární řízení	Ano	Nastaveno v pracovní smlouvě.	užívá
A.7.3	**Ukončení a změna pracovního vztahu**			
Cíl: Chránit zájmy organizace v procesu změny nebo ukončení pracovního vztahu.				
A.7.3.1	Odpovědnosti při ukončení nebo změně pracovního vztahu	Ano	Proces nastaven politikou bezpečnosti IS.	neužívá
A.8	**Řízení aktiv**			
A.8.1	**Odpovědnost za aktiva**			
Cíl: Identifikovat aktiva organizace a definovat odpovědnosti k jejich přiměřené ochraně.				
A.8.1.1	Seznam aktiv	Ano	Aktiva identifikována v registru primární a podpůrných aktiv.	neužívá
A.8.1.2	Vlastnictví aktiv	Ano	Vlastnictví nastaveno pro administrátora, uživatele (lékař, sestra).	částečně
A.8.1.3	Přípustné použití aktiv	Ano	Především se jedná o důvěrnou zdravotní dokumentaci, interní a externí citlivé informace smluvních vztahů, osobní informace a veřejné dokumenty opatření DP kap. 4.5.3. Užívání PA a POA k určeným účelům.	užívá
A.8.1.4	Navrácení aktiv	Ano	Zápůjčka zdravotnické dokumentace (listinná podoba) revizním a posudkovým lékařům dle zákona.	užívá
A.8.2	**Klasifikace informací**			
Cíl: Zajistit, aby informace získaly odpovídající úroveň ochrany v souladu s jejich důležitostí pro organizaci.				
A.8.2.1	Klasifikace informací	Ano	Klasifikace informací je klasifikována na veřejné, citlivé, důvěrné. DP kap. 4.5.3.	částečně
A.8.2.2	Označování informací	NE	Není plněno.	neorganizuje
A.8.2.3	Manipulace s aktivy	Ano	Nastaven proces na základě informačních toků a manipulace s informacemi dle DP kap.4.5.3.	užívá
A.8.3	**Manipulace s médii**			
Cíl: Předcházet neoprávněnému vyzrazení, modifikaci, odstranění nebo zničení informací uložených na médiích.				
A.8.3.1	Správa výměnných médií	Ano	Není řešeno. Jednateli org. navrhnuto pořízení SW pro správu přístupu vyměnitelných médií a zavedení evidence médií. Obsahuje také zálohovací paměťová média.	neužívá
A.8.3.2	Likvidace médií	Ano	Proces bude nastaven v bezpečnostní směrnici. V současné době žádná vyměnitelná média se v organizaci neužívají. Datová media instalovaná v pracovní stanici a notebooku, která budou podléhat bezpečnému výmazu.	neužívá
A.8.3.3	Přeprava fyzických médií	Ano	Papírovou zdravotní dokumentaci přepravovat osobně, kurýrem nebo doporučenou listovní zásilkou. Data na USB flash šifrovaně.	částečně

A.9	Řízení přístupu			
A.9.1	**Požadavky organizace na řízení přístupu**			
Cíl: Omezit přístup k informacím a vybavení pro zpracování informací.				
A.9.1.1	Politika řízení přístupu	Ano	Je ukotvena v politice ISMS a politice bezpečnosti IS. Souvisí s řízením přístupu dle A.9.2. Návrh zpracován v DP kap. 4.9.	užívá
A.9.1.2	Přístup k sítím a síťovým službám	Ano	Přístup je řízen aplikačním IS dle potřeb užívaní přístupu k software, diagnostickým přístrojům a portálům. Dle schéma IS v DP obrázek 15.	užívá
A.9.2	**Řízení přístupu uživatelů**			
Cíl: Zajistit oprávněný přístup k informacím a předcházet neoprávněnému přístupu k systémům a službám.				
A.9.2.1	Registrace a zrušení registrace uživatele	Ano	Účet uživatele je vytvořen na základě podepsané pracovní smlouvy a poučení užívání aplikačního IS a proškolení ze směrnice bezpečnosti IS.	částečně
A.9.2.2	Správa uživatelských přístupů	Ano	Administrátor IS v organizaci řídí správu uživatelských přístupů - v systému Windows, SMARTMEDIX, webové portály (Medila, UZIS, Zdravotní pojišťovny, aj.).	užívá
A.9.2.3	Správa privilegovaných přístupových práv	Ano	Je řízeno jednatelem organizace. Především rozdělení rolí lékař a sestra.	užívá
A.9.2.4	Správa tajných autentizačních informací uživatelů	NE	Neprovádí se.	neorganizuje
A.9.2.5	Přezkoumání přístupových práv uživatelů	Ano	Souvisí s požadavky na provoz a nastavením aplikačního SW. Politika bezpečnosti IS.	užívá
A.9.2.6	Odebrání nebo úprava přístupových práv	Ano	Provádí administrátor určený za oblast IS. (pověřený zaměstnanec jednatelem organizace).	užívá
A.9.3	**Odpovědnosti uživatelů**			
Cíl: Učinit uživatele odpovědné za ochranu jejich autentizačních informací.				
A.9.3.1	Používání tajných autentizačních informací	NE	Neprovádí se.	neorganizuje
A.9.4	**Řízení přístupu k systému a aplikacím**			
Cíl: Předcházet neautorizovanému přístupu k systémům a aplikacím.				
A.9.4.1	Omezení přístupu k informacím	Ano	V elektronické formě nastaveno politikou účtů z úrovní administrátor, uživatel (lékař, sestra, administrativní pracovník), v hlasové a dokumentové (papírové) formě se řídí dle pravidel GDPR. Citlivé (důvěrné) interní informace o řízení, know-how, smluvní a finanční toky pouze jednatel.	částečně
A.9.4.2	Bezpečné postupy přihlášení	Ano	Nastavena silná hesla (OS, SMARTMEDIX), dvoufaktorové ověření, užívání digitálních certifikátů a identit k přístupu k agendními IS, portálům ZP, klientům poskytující výměnu dat.	užívá
A.9.4.3	Systém správy hesel	Ano	Hesla a certifikáty uloženy mimo organizaci.	částečně
A.9.4.4	Používání privilegovaných programových nástrojů	Ano	Omezeno, zakázáno bootování USB zařízení, povoleno bootování pouze systémového disku. BIOS chráněn heslem.	neužívá
A.9.4.5	Řízení přístupu ke zdrojovým kódům programů	Ano	Neaplikuje se, organizace užívá licencovaný SW, který je outsourcingován s podporou a updaty. Organizace neprovádí vývoj vlastního SW.	užívá

A.10	**Kryptografie**			
A.10.1	**Kryptografická opatření**			
Cíl: Zajistit řádné a efektivní užívání kryptografie k ochraně důvěrnosti, autentičnosti a / nebo integrity informací.				
A.10.1.1	Politika používání kryptografických opatření	Ano	Kryptografické šifrování obsahu disků pomocí BitLocker, užívání šifrování databáze zdravotní dokumentace v souvislosti s replikaci v MS Azure. Šifrování disků a externích USB disků dle MBS NUKIB 2020.	částečně
A.10.1.2	Správa klíčů	Ano	Správa klíčů jednatele – digitální podpis, certifikáty a uložení klíčů od šifrovaných disků.	částečně
A.11	**Fyzická bezpečnost a bezpečnost prostředí**			
A.11.1	**Bezpečné oblasti**			
Cíl: Předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace.				
A.11.1.1	Fyzický bezpečnostní perimetr	Ano	Projekt fyzické bezpečnosti – interní neveřejný dokument (nákres bezpečnostního perimetru a oblastí ukládání informací, přehled informačních aktiv, technické řešení a nastavení EZS, smlouva o ochraně objektu online ochrana fa. Jablotron).	částečně
A.11.1.2	Fyzické kontroly vstupu	Ano	EZS – elektronický systém zabezpečení uzamčeného objektu.	užívá
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	Ano	Uzamykatelné kartotéky se zdravotnickou dokumentací, uzamykání místností, aktivní EZS.	užívá
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	Ano	Zabezpečení okenních otvorů mřížemi, doplnění čidel EZS, protipožární čidla, přidělení kódu EZS pro každého zaměstnance zvlášť, EZS napojena na pult centrální ochrany, zásah bezpečnostní agenturou a součinnosti s Policií ČR.	částečně
A.11.1.5	Práce v bezpečných oblastech	NE	Neužívá.	neorganizuje
A.11.1.6	Oblasti pro nakládku a vykládku	NE	Oblast není součástí objektu organizace.	neorganizuje
A.11.2	**Zařízení**			
Cíl: Předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činnosti organizace.				
A.11.2.1	Umístění zařízení a jeho ochrana	Ano	Aplikovaná opatření A.5 - A.11snižující rizika hrozeb k zvýšení bezpečnosti ochrany zařízení.	částečně
A.11.2.2	Podpůrné služby	Ano	Instalace UPS k ochraně před selháním napájení v souvislosti zachováním dostupnosti a integrity IS a primárních aktiv organizace.	neužívá
A.11.2.3	Bezpečnost kabelových rozvodů	Ano	Provedení rekonstrukce silových a síťových rozvodů, pro napájení aktiv a pro přenos dat k zajištění CIA dle standardu ČSN EN 50174-2.	neužívá
A.11.2.4	Údržba zařízení	Ano	Provádění pravidelných servisních činností, revizí a kalibrací zařízení k zajištění dostupnosti a integrity.	užívá
A.11.2.5	Přemístění aktiv	Ano	Manipulace s aktivy a informacemi podléhá politice bezpečnostní IS a nesmí být s nimi manipulováno mimo objekt bez předchozího schválení odpovědné osoby aktiva.	užívá
A.11.2.6	Bezpečnost zařízení a aktiv mimo prostory organizace	Ano	Přenášení NB lékaře, přístup do systému otiskem prstu/heslem, HDD šifrován, data jsou v cloudu, replikace databáze mezi počítači v ambulanci a mimo ambulanci dle politiky bezpečnosti IS.	částečně
A.11.2.7	Bezpečná likvidace nebo opakované použití zařízení	Ano	Všechna záznamová a paměťová média, diagnostické přístroje musí být před jejich likvidací či předání mimo organizaci bezpečně vymazány nebo odstraněna.	částečně

A.11.2.8	Uživatelská zařízení bez obsluhy	Ano	V přítomnosti třetí osoby nesmí být zařízení ponechána bez kontroly povinné osoby.	užívá
A.11.2.9	Zásada prázdného stolu a prázdné obrazovky monitoru	Ano	Edukace personálu v rámci pravidelných školení. Schválená politika bezpečnosti IS. Musí být přijaty opatření s ohledem na volně dostupné dokumenty a paměťová média a informace zobrazená na monitoru.	částečně
A.12	**Bezpečnost provozu**			
A.12.1	**Provozní postupy a odpovědnosti**			
Cíl: Zajistit správný a bezpečný provoz vybavení pro zpracování informací.				
A.12.1.1	Dokumentované provozní postupy	Ano	Dokumentované provozní postupy a činností organizace v souvislosti identifikací manipulace s aktivy a informacemi. Metodika bezpečnosti IS.	neužívá
A.12.1.2	Řízení změn	Ano	Nastavení systému řízení změn informační bezpečnosti na základě změnového hodnocení dopadů rizik při změně výkonu činnosti organizace a procesů.	neužívá
A.12.1.3	Řízení kapacit	Ano	Zajištění dostatečné kapacity pro ukládání a zpracování elektronické a listinné zdravotnické dokumentace. Aktualizace SW, rozsahu paměťového úložiště, kapacity kartoték.	užívá
A.12.1.4	Princip oddělení prostředí vývoje, testování a provozu	NE	Zabezpečeno outsoucingem dodavatele SW.	neorganizuje
A.12.2	**Ochrana proti malwaru**			
Cíl: Zajistit, aby informace a vybavení pro zpracování informací byly chráněny proti malwaru.				
A.12.2.1	Opatření proti malwaru	Ano	Vynucení užívání antivirové ochrany na všech zařízeních na platformě IOS, Windows a Android a edukace personálu vedoucí k odpovídajícím bezpečnostním návykům uživatelů IS.	užívá
A.12.3	**Zálohování**			
Cíl: Chránit proti ztrátě dat.				
A.12.3.1	Zálohování informací	Ano	Nastavené automatické zálohování elektronických dokumentů v cloudu, databáze zdravotnických informací formou replikace databáze pomocí MS Azure Backup, archivace listinné zdravotní dokumentace pacientů.	částečně
A.12.4	**Zaznamenávání formou logů a monitorování**			
Cíl: Zaznamenávat události a vytvářet záznamy.				
A.12.4.1	Zaznamenávání událostí formou logů	Ano	Události v aplikačním SW jsou logovány (identifikace uživatele. kdo a jaké informace zpracovával) V OS Windows jsou logovány události v Computer management, Windows Event Viewer, Windows logy (Application, Security, Setup, System).	částečně
A.12.4.2	Ochrana logů	Ano	Logy jsou stahovány každé 3 měsíce, ukládány na určené záznamové médium a vyhodnocovány v případě nestandartní události v IS.	neužívá
A.12.4.3	Logy o činnosti administrátorů a operátorů	Ano	Shodné opatření s A.12.4.1.	neužívá
A.12.4.4	Synchronizace hodin	Ano	Automatická synchronizace času je zabezpečena službou OS Windows 10 funkcí "Nastavovat čas automaticky".	užívá

A.12.5	**Správa provozního software**			
Cíl: Zajistit integritu provozních systémů.				
A.12.5.1	Instalace software na provozní systémy	Ano	Software, firmware, ovladače zařízení a jejich update je na základě prověření bezpečnosti obsahu na počítače instalován administrátorem.	částečně
A.12.6	**Řízení technických zranitelností**			
Cíl: Zabránit využívání technických zranitelností.				
A.12.6.1	Řízení technických zranitelností	Ano	Nastavení pravidelných revizí a kalibrací diagnostických zařízení, elektrických spotřebičů a servis počítačů. Řízený upgrade sw a firmware technických zařízení.	částečně
A.12.6.2	Omezení instalace softwaru	Ano	Uživatel nemá právo instalace SW. Provádí administrátor.	užívá
A.12.7	**Hlediska auditu informačních systémů**			
Cíl: Minimalizovat dopady auditních činností na provozní systémy.				
A.12.7.1	Opatření k auditu informačních systémů	Ano	Auditování se provádí po ambulantní době, minimálně 1x měsíčně. Audit síťových prvků, audit počítačů, audit tiskáren.	neužívá
A.13	**Bezpečnost komunikací**			
A.13.1	**Správa bezpečnosti sítě**			
Cíl: Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací.				
A.13.1.1	Opatření v sítích	Ano	Nastavení systému správy, kontroly a řízení nasazením aktivních prvků umožňující bezpečnostní opatřeni. Security gateway – pokročilá správa firewall, VPN, správa VLAN, DDoS, malware ochrana, blokování nebezpečných www. Intranet – sdílení informací.	částečně
A.13.1.2	Bezpečnost síťových služeb	Ano	Nastavení šifrování a užívání elektronických certifikátů pro přístup do registrů, přístup na portály veřejné správy a pojišťoven.	částečně
A.13.1.3	Princip oddělení v sítích	Ano	Nastaven oddělený provoz interní a externí sítě LAN (VLAN). Jsou stanoveny principy sdílení informací ve vnitřní sítí formou komunikace v intranetu a při externím zpracovávání informací v databázi aplikačního IS, probíhá výměna dat přes zabezpečenou šifrovanou replikaci dat v prostředí internet (MS AZURE).	částečně
A.13.2	**Přenos informací**			
Cíl: Zajistit bezpečnost informací při jejich přenosu v rámci organizace a s externími subjekty.				
A.13.2.1	Politiky a postupy při přenosu informací	Ano	Řídit se navrhnutou politikou ISMS, metodikou bezpečnosti IS a opatřeními v politice bezpečnosti IS. DP 4.9.	částečně
A.13.2.2	Dohody o přenosu informací	Ano	Podepsané smlouvy o sdílení informací (zdravotnických dat) - užívání kvalifikovaného a komerčního certifikátu. Služba WebLIMS, eSpráva, Datová schránka, SMARTMEDIX, ČSSZ, eNeschopenka, eRecept, ÚZIS, zdravotní pojišťovny.	částečně

A.13.2.3	Elektronické předávání zpráv	Ano	Forma klientů – stahování informací z uložišť jednotlivých poskytovatelů viz. Dohody o přenosu informací. A.13.2.3.	částečně
A.13.2.4	Dohody o utajení nebo o mlčenlivosti	Ano	Opatření k GDPR, zaměstnanecká smlouva.	užívá
A.14	**Akvizice, vývoj a údržba informačních systémů**			
A.14.1	**Bezpečnostní požadavky informačních systémů**			
Cíl: Zajistit, aby se bezpečnost informací stala nedílnou součástí informačních systémů v jejich celém životním cyklu. To zahrnuje i požadavky na informační systémy, které poskytují služby ve veřejných sítích.				
A.14.1.1	Analýza a specifikace požadavků bezpečnosti informací	Ano	Opatření jsou rozvedena v analýze DP kap.4. užít SWOT, GAP analýzu a popsat hlavní procesy organizace, toky informací a IS.	neužívá
A.14.1.2	Zabezpečení aplikačních služeb na veřejných sítích	Ano	Identifikace pro komunikaci pomocí elektronického certifikátu organizace, šifrování, VPN.	částečně
A.14.1.3	Ochrana transakcí informačních služeb	Ano	Hlavní opatření je užívání VPN, šifrování vlastního obsahu komunikace, užívání certifikátů a důvěryhodnosti koncových uzlů, smluvní vztah.	částečně
A.14.2	**Bezpečnost v procesech vývoje a podpory**			
Cíl: Zajistit, aby bezpečnost informací byla navrhována a implementována v životním cyklu vývoje informačních systémů.				
A.14.2.1	Politika bezpečného vývoje	Ano	Outsourcing MEDAX pro SMARTMEDIX	neorganizuje
A.14.2.2	Postupy řízení změn systémů	Ano	Outsourcing MEDAX pro SMARTMEDIX	neorganizuje
A.14.2.3	Technické přezkoumání aplikací po změnách provozní platformy	Ano	Outsourcing MEDAX pro SMARTMEDIX	neorganizuje
A.14.2.4	Omezení změn softwarových balíků	Ano	Outsourcing MEDAX pro SMARTMEDIX	neorganizuje
A.14.2.5	Principy budování bezpečných systémů	Ano	Outsourcing MEDAX pro SMARTMEDIX	neorganizuje
A.14.2.6	Prostředí bezpečného vývoje	Ano	Outsourcing MEDAX pro SMARTMEDIX	neorganizuje
A.14.2.7	Outsourcovaný vývoj	Ano	Outsourcing MEDAX pro SMARTMEDIX	neorganizuje
A.14.2.8	Testování bezpečnosti systémů	Ano	Outsourcing MEDAX pro SMARTMEDIX	neorganizuje
A.14.2.9	Testování akceptace systémů	Ano	Outsourcing MEDAX pro SMARTMEDIX	neorganizuje
A.14.3	**Data pro testování**			
Cíl: Zajistit ochranu dat používaných pro testování.				
A.14.3.1	Ochrana dat pro testování	Ano	Outsourcing MEDAX pro SMARTMEDIX	neorganizuje
A.15	**Dodavatelské vztahy**			
A.15.1	**Bezpečnost informací v dodavatelských vztazích**			
Cíl: Zajistit ochranu aktiv organizace, ke kterým mají dodavatelé přístup.				
A.15.1.1	Politika bezpečnosti informací pro dodavatelské vztahy	Ano	Uzavřená smlouva o poskytnutí licencí software SMARTMEDIX, online podpory, helpdesku, o aktualizacích aplikačního SW a poskytování replikací databáze v prostředí MS Azure. Součástí dohod je stanovení pravidel GDPR a dohoda o mlčenlivosti, ochraně informací a zákazu jejich zneužití.	částečně
A.15.1.2	Bezpečnostní požadavky v dohodách s dodavateli	Ano	Souhlas s bezpečností informací v souvislosti A.15.1.1.	částečně
A.15.1.3	Dodavatelský řetězec informačních a komunikačních technologií	Ano	Dodávky jsou uskutečněny formou dodaného HW, SW, technologii, komunikačních sítí, kdy konfigurace se provádí až v organizaci a přístupové údaje k administraci jsou výhradně pod kontrolou organizace.	užívá

A.15.2	**Řízení dodávek služeb dodavatelů**			
Cíl: Udržovat dohodnutou úroveň bezpečnosti informací a dodávky služeb ve shodě s dodavatelskými dohodami.				
A.15.2.1	Monitorování a přezkoumání služeb dodavatelů	Ano	Monitorování a přezkoumání je prováděno za přítomnosti administrátora IS organizace při fyzickém zásahu do aplikačního SW dodavatelem. Administrátor má plnou kontrolu nad správou účtů.	užívá
A.15.2.2	Řízení změn ve službách dodavatelů	Ano	Update programového kódů aplikace je oddělen od přístup k informacím v databázi, je prováděn na základě dodavatelské smlouvy, a to v souvislosti s legislativními změnami nebo funkčními změnami v SW.	užívá
A.16	**Řízení incidentů bezpečnosti informací**			
A.16.1	**Řízení incidentů bezpečnosti informací a zlepšování**			
Cíl: Zajistit odpovídající a efektivní přístup ke zvládání incidentů bezpečnosti informací, zahrnující komunikaci ohledně bezpečnostních událostí a slabých míst.				
A.16.1.1	Odpovědnosti a postupy	Ano	Stanoveny role v bezpečnostní politice IS (interní – ADM, USER, vlastník aktiv; externí – manažer a architekt KB). Nastaven proces řízení rizik IS v ISMS.	neužívá
A.16.1.2	Hlášení událostí bezpečnosti informací	Ano	Dojde-li k podezření nebo uskutečnění incidentu ISMS, organizace identifikuje incident, na základě řízení rizik vyhodnotí závažnost a újmu a aplikuje opatření v souvislosti typem hrozby a "oslabené" zranitelnosti.	neužívá
A.16.1.3	Hlášení slabých míst bezpečnosti informací	Ano	Při nalezení "slabých míst" bezpečnosti informací informovat administrátora IS organizace, dodavatele aplikačního SW, technologií a diagnostických přístrojů.	neužívá
A.16.1.4	Posouzení a rozhodnutí o událostech bezpečnosti informací	Ano	V souvislosti s A.16.1.1 a A.16.1.2 rozhodnout v rámci nastaveného systémů řízení rizik o klasifikaci incidentu, pokud k němu došlo. Politika bezpečnosti IS.	neužívá
A.16.1.5	Reakce na incidenty bezpečnosti informací	Ano	Přijetí opatřeni dle dokumentovaných postupů, přijetí opatření dle analýzy rizik, návrh nových opatřen pro minimalizaci zranitelností vůči působící hrozbě.	částečně
A.16.1.6	Ponaučení z incidentů bezpečnosti informací	Ano	Znalosti z analýzy a řešení incidentu využít ke snížení pravděpodobnosti dalšího incident, kdy znalost zapracovat do ISMS a provést edukaci personálu.	částečně
A.16.1.7	Shromažďování důkazů	Ano	Identifikovat, získat a uchovat informace o incidentu jako důkaz o události v ISMS.	neužívá
A.17	**Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací**			
A.17.1	**Kontinuita informační bezpečnosti**			
Cíl: Kontinuita bezpečnosti informací musí být součástí systémů řízení kontinuity činnosti organizace.				
A.17.1.1	Plánování kontinuity bezpečnosti informací	Ano	Zdravotnická dokumentace je redundantně vedena v dokumentové podobě a k záznamu informací může být užito psacích potřeb či psacího stroje. Rozsah poskytování zdravotní péče je ovlivněn dostupností zdroje el. energie pro diagnostické přístroje a užívání aplikačního IS. Plán kontinuity IS vzor DP kap.4.9.	částečně
A.17.1.2	Implementace kontinuity bezpečnosti informací	Ano	V souvislosti s A.17.1.1 a politikou bezpečnosti IS je řešením vytvoření Plánu kontinuity IS v souvislosti s ISMS organizace.	částečně
A.17.1.3	Verifikace, přezkoumání a vyhodnocování kontinuity bezpečnosti informací	Ano	Provádět min.1x za rok verifikaci implementovaných opatření ISMS k řízení kontinuity činnosti organizace.	neužívá

A.17.2	**Redundance**			
Cíl: Zajistit dostupnost vybavení pro zpracování informací.				
A.17.2.1	Dostupnost vybavení pro zpracování informací	Ano	Dostupnost a integrita zdravotnických informací o pacientech v rámci hlavního aktiva "zdravotní péče" je zabezpečena redundancí elektronické dokumentace (replikací dbf.) a listinou (dokumentovou). Redundance podpůrných aktiv souvisí s aplikovanými opatřeními k snížení rizik (systém řízení rizik). Nastavení redundance HW a technických prostředků.	částečně
A.18	**Soulad s požadavky**			
A.18.1	**Soulad s právními a smluvními požadavky**			
Cíl: Vyvarovat se porušení zákonných, předpisových nebo smluvních povinností týkající se bezpečnosti informací a na jakýchkoliv bezpečnostních požadavků.				
A.18.1.1	Identifikace odpovídající legislativy a smluvních požadavků	Ano	Je stanoven legislativní rámec poskytování zdravotní péče, a v souvislosti s ISO/IEC 2700x, ZKB, VKB, metodiky GDPR. Politikou ISMS organizace je definován prostor pro systém řízení informační bezpečnosti. DP kap. 3.3, 4.1, 4.2. a příloha 13.	částečně
A.18.1.2	Ochrana duševního vlastnictví	Ano	Právo duševního vlastnictví při tvůrčí činnosti/ netvůrčí obchodní činnosti nebo činnosti, jejímž výsledkem je nehmotný statek. Příkladem je know-how organizace nebo užívání legálních licencí software.	užívá
A.18.1.3	Ochrana záznamů	Ano	Je nastavena ochrana primárních a podpůrná aktiv zachování důvěrnosti, integrity, dostupnosti a spolehlivosti v souladu s požadavky v A.18.1.1.	částečně
A.18.1.4	Soukromí a ochrana osobních údajů	Ano	Splnění nařízení EU 679/2016 k GDPR. Užití ISMS k zavedení GDPR. Edukace personálu dodržování A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru a nesdělování informací osobě neoprávněné. Ve smlouvách s interními a externími zaměstnanci vyžadovat dohodu o mlčenlivosti, ochraně informací a zákazu jejich zneužití	užívá
A.18.1.5	Regulace kryptografických opatření	Ano	Užívání elektronických certifikátů osobou oprávněnou.	užívá
A.18.2	**Přezkoumání informační bezpečnosti**			
Cíl: Zajistit, že bezpečnost informací je implementována a provozována v souladu s politikami a postupy organizace.				
A.18.2.1	Nezávislé přezkoumání bezpečnosti informací	Ano	Stanovený přístup organizace k ISMS a v případě, že dojde ke změnám v bezpečnosti informací (změna legislativy), by měl být proveden nezávislý audit.	neužívá
A.18.2.2	Shoda s bezpečnostními politikami a normami	Ano	Stav ISMS v organizaci se porovnává se schváleným legislativním rámcem, politikou ISMS, politikou bezpečnosti IS a PoA.	neužívá
A.18.2.3	Přezkoumání technické shody	Ano	Auditování informačního systému v souvislosti s opatřením A.18.2.2.	neužívá

Zdroj: vlastní zpracování, ISO 27001 (2014)

Příloha 13 - Návrh politiky ISMS

Politika ISMS

Ambulance praktického lékaře

Cílem realizace ISMS ve zdravotnickém zařízení je implementovat informační bezpečnost v souladu ISO/IEC 27000 a získat kontrolu nad bezpečností informací v elektronické, tištěné a myšlenkové podobě.

Hlavním cílem bezpečnostní politiky mikropodniku je:

- zajistit princip důvěrnosti, integrity a dostupnosti zpracovávaných informací;
- chránit identifikovaná informační aktiva organizace;
- aplikovat nutná opatření k řízení rizik (hrozba/zranitelnost)
- zlepšovat princip řízení bezpečnosti informací ISMS;
- zachovat dostupnost procesu poskytování zdravotní služby;
- být v souladu s platnou legislativou;
- je závazná pro všechny zaměstnance mikropodniku.

Závazná legislativa ISMS pro poskytování zdravotní péče v mikropodniku:

- ISO/IEC 27000 - systémy řízení bezpečnosti informací;
- ISO/IEC 27799 – pokyny k implementace ISO/IEC 27002 ve zdravotnictví;
- GDPR – Nařízení Evropského parlamentu a Rady (EU) 2016/679;
- zákon č. 372/2011 Sb., Zákon o zdravotních službách a podmínkách jejich poskytování;
- vyhláška č. 98/2012 Sb., o zdravotnické dokumentaci.

Rozsah a hranice ISMS mikropodniku je stanoven:

- fyzický prostor podnikání a zaměstnanci – provozovna ambulance praktického lékaře;
- právní rámec zdravotní péče ve zdravotnickém zařízení s přenesením výkonu státní správy (MZ ČR – ZP – poskytovatel zdravotní péče);
- zdravotní dokumentace v analogové (listinné) a elektronické (digitální) formě;
- smlouvy s dodavateli a odběrateli; organizační směrnice (dokumenty), účetní výkazy a personální dokumenty mikropodniku;
- prostředí aplikačního IS mikropodniku (primární a podpůrná aktiva).

Postupy a opatření k řízení ISMS:

- implementovat a budovat bezpečnost informací na vlastních aktivech mikropodniku;
- průběžně sledovat portál NÚKIB o aktuálních možných kybernetických hrozbách;
- aktualizovat, auditovat, monitorovat a průběžně vyhodnocovat provoz IS;

- nastavit nezbytnou míru informační bezpečnosti pro každý incident k jeho ošetření;
- udržovat dokumentaci ISMS (nejméně 1x ročně aktualizovat);
- sestavit havarijní plán provozu, zálohování a obnovy IS;
- provádět pravidelná školení zaměstnanců z informační bezpečnosti provozovaného IS;
- zabezpečit ICT podporu pro provoz informačního systému mikropodniku.

V Pardubicích dne . června 2023 jednatel

Zdroj: vlastní zpracování

Příloha 14 - Plán kontinuity ISMS v mikropodniku

Incident č.1

Přerušení dodávek elektrické energie, které má za následek porušení dostupnosti připojení do internetu a komunikace s agendními systémy a přerušení poskytování zdravotní péče.

Hrozba

H21 – **Porucha dodávek elektrické energie**, vody, vytápění.

- Úroveň rizika STŘEDNÍ.

Inicializuje:

H07 – Nedostupnost služby poskytované aplikačním IS.

H08 – Nedostupnost komunikačních služeb.

H13 – Nedostupnost agendních IS.

Dopad

- omezení poskytování zdravotních služeb;
- omezení provozu aplikačního IS, nedostupnost připojení k internetu, přístup IS k agendním systémům je off-line.

Porušení dostupnosti služeb aplikačního IS – lékař není schopen vystavit receptu (eRecept), vystavení pracovní neschopnosti (eNeschopenka) a poukaz na léčebnou a ortopedickou pomůcku (ePoukaz)**.**

Opatření

Činnost při incidentu

Lékař může vystavit recept, neschopenku a poukaz písemnou formou na standardizovaný formulář nebo vytisknout na tiskárnu (funkční UPS) v off-line režimu IS. Následně po obnovení dodávek elektrické energie a zprovoznění konektivity do internetu, systém odešle elektronickou podobu požadavků. Informuje pacienty o přerušení poskytování zdravotní péče, uzavře ambulanci do obnovení dodávek elektrické energie. Uživatelé ukončí práci na počítačích a provedou bezpečné vypnutí.

Ošetření zranitelnosti k snížení rizika

- mít řádně uzavřenou smlouvu s dodavatelem elektrické energie;
- instalace záložních zdrojů UPS pro aktivní prvky, počítače, tiskárny a diagnostické přístroje.
- provádět pravidelnou technickou revizi rozvodů elektrické energie a UPS;

- nastavit způsob zálohování a replikace dat;
- nastavit alternativní způsob vystavení preskripce;
- při výluce poskytování zdravotní péče mít dohodu o ošetření pacientů jiným poskytovatelem.

Obnovení kontinuity

- uživatelé provedou uložení elektronických dokumentů a ukončí práci v aplikačním SW, provedou bezpečné vypnutí počítače, aktivních prvků, tiskáren a diagnostických přístrojů;
- zaměstnanci prověří přívod elektrické energie v rozvaděči organizace;
- kontaktovat dodavatele elektrické energie a informují se o události;
- informovat pacienty v čekárně a objednaným pacientům oznámí výluku služeb;
- po obnovení přívodu elektrické energie, provedou kontrolu zapnutí UPS, zpuštění routeru, počítačů, tiskáren a diagnostických zařízení;
- uživatelé se přihlásí do aplikačního SW – po ověření funkcionality je provoz obnoven.

Doba obnovení kontinuity ISMS: **závisí na obnovení dodávek elektrické energie.**

Incident č.2

Nefunkčnost počítač, poškození operačního systému, aplikačního software na PC – narušení integrity a dostupnosti systémového disku, nefunkčnost jednoho replikačního uzlu.

Hrozba

H02 – Poškození, selhání technického nebo HW vybavení.

H03 – Poškození, selhání SW a OS.

- Úroveň rizika VYSOKÉ.

Inicializuje:

H01 – Porušení bezpečnostní politiky IS.

H06 – Škodlivý kód.

H09 – Neoprávněná modifikace informací v aplikačním IS.

H12 – Nedostupnost technické a softwarové pomoci dodavatelů.

H14 – Ztráta, poškození, odcizení elektronické zdravotní dokumentace.

H22 – Nedostupnost replikace databáze aplikačního IS.

Dopad

- omezení poskytování zdravotních služeb;

- omezení dostupnosti zdravotní dokumentace;
- omezení provozu aplikačního IS

Porušení dostupnosti a integrity informací v IS, které nebyly replikovány z poškozeného počítače. Porušení integrity hardware počítače má vliv na dostupnosti software.

Opatření

Činnost při incidentu

Počítač vypnout, odpojit od napájení a kontaktovat správce IS, případně podporu aplikačního SW. Lékař může pracovat na druhém dostupné počítači. Nefunkční počítač předá správci IS.

Ošetření zranitelnosti k snížení rizika

- mít řádně uzavřenou smlouvu s dodavatelem aplikačního SW a správcem IS;
- nastavit životní cyklus počítače pro obměnu 3 - 5let, dle způsobu užívání a délce provozu – omezit riziko selhání HW komponent;
- nastavit způsob zálohování a replikace dat;
- nastavit a prověřit způsob instalace počítače a obnovy dat v aplikačním IS s obnovením replikace uzlu;
- při výluce poskytování zdravotní péče mít dohodu o ošetření pacientů jiným poskytovatelem.

Obnovení kontinuity

- správce IS provede kontrolu konfigurace a zabezpečení přístupového bodu do internetu;
- při selhání OS nebo aplikačního SW provede kontrolu CIA spuštění OS a SW;
- pří napadení počítače malware provést kontrolu disků na samostatném počítači s aktualizovanou antivirovou ochranou;
- při selhání HW na nefunkčním PC provést testy funkčnosti HW a nastaveni BIOS;
- provedení nové instalace počítače zařazeného do IS podle doporučeného postupu politiky bezpečnosti IS s obnovou dat, elektronických dokumentů z cloudu a obnově databáze dat aplikačního IS replikovaného uzlu;
- Po ověření instalace, nastavení uživatelských účtů a verifikaci přístupů potřebných pro zabezpečení do jednotlivých portálů je provoz obnoven.

Doba obnovení kontinuity ISMS: **do 48 hodin od zahájení řešení.**

Zdroj: vlastní zpracování

Příloha 15 - Návrh směrnice uživatele IS

Směrnice uživatele IS

GDPR

Seznámit se s dokumentací GDPR v ambulanci VPL a rozsahem zpracovávaných informací podléhajících ochraně osobních údajů a znát způsob manipulace (distribuce, přístup, použití, ukládání, řízení změn, uchování, likvidace) dokumentovaných informací v informačním systému a objektu ambulance.

Pro nově registrované pacienty požadovat „Souhlas se zpracováváním osobních údajů a zdravotnické dokumentace, GDPR“, formulář je dostupný v elektronické kartě pacienta.

Manipulace a sdílení informací

Pro zpracování interních informací organizace, osobních údajů a zdravotnické dokumentace (elektronické, listinné, hlasové) užívat výhradně informačního systému na přiděleném počítači zdravotní sestry a lékaře.

Sdílet informace užíváním datové schránky, klientů pro výměnu informací (eSpráva, WebLIMS (užívat výhradně datové schránky k přijímání a odesílání elektronických dokumentů obsahující zdravotnické informace při komunikaci s ostatními poskytovateli zdravotní péče a veřejnou správou);

Při hlasové telefonní komunikaci, výhradně užívat telefonních přístrojů a čísel organizace, dbát na identifikaci pacienta pomocí smluveného hesla pro komunikaci (Souhlas se zpracováváním osobních údajů a zdravotnické dokumentace, GDPR).

Zdravotní kartu pacienta užívat v objektu ambulance VPL pro potřeby ošetřujícího lékaře či náhledu pacientem a pořizovat kopie zdravotní dokumentace se souhlasem lékaře.

Přístup do IS

Pravidlo vytváření hesel uživatelský účtů – délka hesla min. 10 znaků, musí obsahovat velké, malé, alfanumerické a speciální znaky (příklad: Inj3k*cE78).

Pro přístup do operačního systému, aplikačního SW a ostatních komponent IS výhradně užívat vlastní uživatelský účet se zásadou „každý systém, jedinečné heslo“.

Přihlášení do agendních a externích IS upřednostnit přihlášení pomocí digitálního klíče, certifikátu nebo pomocí dvoufaktorové ověření uživatele, pokud to IS umožnuje.

Fyzická bezpečnost

Mít kontrolu nad přístupem k listinné zdravotnické dokumentaci v kartotéce, na pracovní stole a v objektu ambulance v přítomnosti pacientů. Řídit fyzický vstup osob do archivu zdravotních karet ambulance.

Po ukončení pracovní doby listinné dokumenty (zdravotní karty pacientů) uložit do kartotéky a uzamknout. Uzavřít okenní otvory a uzamknout dveře a prostory objektu ambulance. Při odchodu zabezpečit zastřežení objektu užitím EZS. Každý zaměstnanec má osobní kód k EZS objektu.

Počítačová bezpečnost

Každý uživatel IS má vlastní uživatelský účet vytvořený správcem IS.

Uživateli je zakázáno spouštět programové vybavení, které není součástí IS

Uživatel je při přerušení práce na počítači povinen provést uzamknutí nebo odhlášení uživatele z OS případně s aplikačního SW (SmartMEDIX).

Zaměstnanci mají povoleno užívat určená externí záznamová media na PC k tomu určených.

Pro práci mimo objekt ambulance je určen přenosný počítač lékaře s instalovaným aplikačním SW SmartMEDIX, s nastavenou replikací databáze s PC v ambulanci zabezpečenou aplikačním SW SmartMEDIX. Počítače jsou chráněny antivirovým SW, v prostředí internetu užívají VPN, certifikáty pro komunikaci a šifrováním informací na pevném disku pomocí BitLocker. PC a notebook je pravidelně zálohován.

Komunikační bezpečnost

Uživatel pro potřebu interní a externí komunikace (přenosu informací) potřebujeme znát „o čem, kdy, s kým, kdo musí/může komunikovat a způsob realizace komunikace – ústní, písemná, elektronická“.

Pro bezpečnost informací v komunikačním prostředí internetu (zabezpečení důvěrnosti, integrity, dostupnosti a autenticity) IS užívá VPN, šifrováním dokumentů a certifikátů.

V organizaci jsou nastaveny procesy k přenosu informací, užíváním doporučeného dopisu, kurýra, datové schránky PO, agendních systémů (eRecept, eNeschopenka) a klientů (eSpráva, WebLIMS, EUC);

Bezpečnostní událost / incident IS

Přerušení připojení k internetu – v případě výpadku připojení do internetu dojde k přerušení spojení s agendními a externími IS, kdy ambulance dále pracuje v intranetu organizace

(ostrovní režim) a je zachováno spojení s diagnostickými přístroji a tiskárnou. Nelze odeslat vystavené žádanky, eRecept, eNeschopenka atd. Prověřit dostupnost služeb u poskytovatele internetu, kontaktovat administrátora IS. Po obnovení připojení do internetu dojde k automatické synchronizaci odesílaných a přijímaných dat.

Výpadek elektrického proudu – při přerušení dodávek elektrické energie, dojde k přepnutí na záložní zdroj UPC. Záložní zdroj poskytuje cca 20 minut práce. Práci následně v aplikačním SW ukončete a počítač vypněte, pokud nedojde k obnovení dodávek elektřiny.

Nefunkční počítač – počítač nelze zapnout, po zapnutí počítače PC nereaguje, nestartuje, došlo k pádu operačního systému nebo neočekávanému vypnutí. Počítač odpojte a připojte do elektrické zásuvky a následně zapněte. Pokud nedojde k automatickému obnovení funkcionality volejte správce IS.

Nemohu se přihlásit do IS – po opakované pokusu přihlášení do operačního systému, agendních / externích IS, aplikačního SW se nelze přihlásit, přístup byl zamítnut. Zkontrolujte způsob zadávání přihlašovacích údajů, platnost elektronického certifikátu, připojení k internetu. Zjištěnou závadu řešte s odpovědnou osobou, případně ze správce IS.

Nalezení škodlivého kódu (malware) – antivirový program nalezl v souborech počítače, elektronické poště nebo na vyměnitelném paměťovém médiu škodlivý kód (virus, podezřelí soubor). Poznačte si informace o události, podezřelí soubor na základě doporučení antivirového programu vyřešte nebo volejte správce IS.

Podezření na ransomware – v případě zachycení podezřelých emailů, souborů a adresářů v IS s kterými nelze pracovat, hlásit správci IS. Může se jednat právě o zachycení činnosti související s ransomware. Uživatel této události může předcházet: neotvíráním emailových příloh a nespouštěním odkazů od neznámých odesilatelů, všímat si obsahu emailu s chybnou diakritikou českého jazyka.

Přijetí zdravotní dokumentace pacienta od jiného poskytovatele zdravotní péče jiným než doručeným způsobem (GDPR) – informovat původce informací o nevhodném způsobu doručení informací a nastavit nový způsob manipulace – přijímání informací.

Nefunkční agendní systémy eNeschopenka, eRecept – nedošlo k vystavení neschopenky nebo receptu pacienta. V aplikačním IS prověřit připojení do internetu, spojení s agendními systémy a platnost certifikátu, případně informovat správce IS. V případě, že tato služba je nedostupná u poskytovatele, budou vystavené dokumenty odeslány následně po obnovení služeb agendních systémů.

Základní opatření:

Dodržovat zásadu čistý stůl a čistý displej:

- nezanechávat na pracovním stole otevřenou zdravotní kartu (dokumentaci) jiného pacienta, který není aktuálně ošetřován, aby nedošlo k neoprávněnému seznámení se s informacemi;
- dbát na minimalizaci pracovního okna aplikačního software (SmartMedix) v přítomnosti jiné osoby, aby nedošlo k neoprávněnému seznámení se s informacemi, případně odhlášení uživatele z dané aplikace či OS při nepřítomnosti uživatele;
- při přerušení práce na počítači provést uzamknutí/odhlášení uživatele.

Absolvovat školení pro zaměstnance (min. 1xročně) v rozsahu:

- být seznámen s aktivy mikropodniku a s činnostmi, kdy dochází k manipulaci s informacemi;
- znát bezpečné postupy přenosu a sdílení informací v elektronické/analogové podobě;
- být seznámen s hrozbami, rozpoznat je a aktivně jim předcházet v procesu poskytování zdravotní péče;
- formovat návyky (nesdílení účtů v IS, odhlašování z IS, princip čistého stolu).

Zdroj: vlastní zpracování

Příloha 16 - Přehled nákladů užitých opatření

Popis opatření	Opatření dle PoA	Počáteční investice	Roční náklady
Nákup stolního a přenosného PC	A.6.2, A.8.1, A.15.1.3, A.17.2.1	45 690 Kč	bez nákladů
Nákup multifukční tiskárny A4	A.8.1.3, A.8.2.3,A.12.3.1, A.15.1.3	10 290 Kč	5 000 Kč
3x záložní zdroj UPS APC Power Saving Back-UPS Pro 900VA	A.11.1.4, A11.2.2	19 200 Kč	bez nákladů
Rekonstrukce LAN infrasturktury a síťových prvků (router)	A.11.2.3, A.13.1	20 000 Kč	bez nákladů
SW SmartMEDIX pro 2PC, replikace DB a SW podpora	A.6.2:2, A.7.1.2, A.8, A.9, A.10.1.1, 14.2	32 000 Kč	25 875 Kč
Digitální certifikáty kvalifikovaný a komerční certifikát	A.8.2, A.10, A.13.2	836 Kč	500 Kč
Antivirový program ESET Smart Security Premium 1-4 PC	A.11.2.1, A.12.2.1	bez nákladů	1 615 Kč
Připojení do internetu (optika) a telefonní linka (záložní VDSL připojení, telefon)	A.9.4, A.12.1.3	1 998 Kč	12 576 Kč
Nákup Microsoft 365 Business Basic s OneDrive (zálohování dokumentů)	A.6.2.1, A.11.2.2, A.12.3.1	bez nákladů	1 680 Kč
Nákup externího HDD 2TB pro off-line zálohování	A.11.2.3, A.12.3.1	3 000 Kč	bez nákladů
Zavedení EZS s dohledem na pult ochrany objektu + hlásiče (požár, plyn, voda)	A.11.1	30 000 Kč	6 720 Kč
Instalace - nastavení BIOS, OS a programového vybavení 2xPC	A.9, A.12.5.1	7 200 Kč	bez nákladů
Implementace GDPR a vypracování dokumentace v AVPL	A.8, A.9,A.12.1.1, A.13.2, A.18.1.4	25 000 Kč	2 000 Kč
Uzamykatelná kartotéka (2000 karet)	A.8.1.3, A.11.1.3	60 000 Kč	bez nákladů
Školení (prvotní, 1x za rok) zaměstnanců BOZP, ISMS (GDPR)	A.7.1.2, A.7.2, A.8	3 000 Kč	2 000 Kč
Revize elektrický spotřebičů a kalibrace diagnostických zdravotnických přístrojů	A.11.2.4, A.12.6.1	5 000 Kč	5 000 Kč
Smlouva o podpoře a údržbě IS	A.6.1.2, A.7.1.2, A.12.5.1, A.12.6.1, A12.7.1, A.17.1	bez nákladů	24 000 Kč
Celkové náklady		263 214 Kč	86 966 Kč

Zdroj: vlastní zpracování